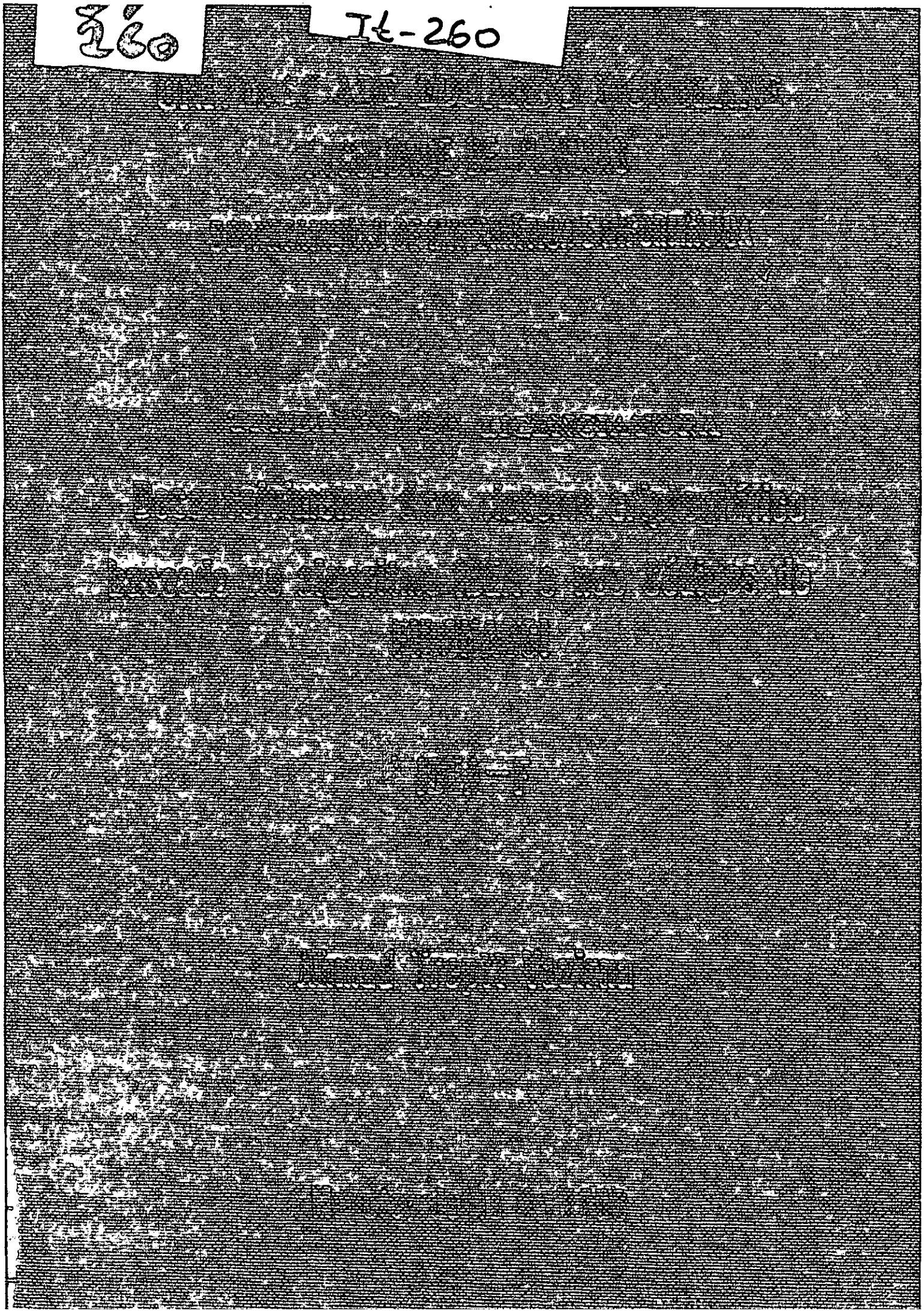


UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS

Departamento de Matemática e Informática

TRABALHO DE LICENCIATURA

Desenvolvimento dum sistema criptográfico baseado no algoritmo IDEA e nos Códigos de Fibonacci

IDEA-F

Ahmad Treptt Vazirna

Maputo, Julho de 2006

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS

Departamento de Matemática e Informática

TRABALHO DE LICENCIATURA

Desenvolvimento dum sistema criptográfico baseado no algoritmo IDEA e nos Códigos de Fibonacci

IDEA-F

Autor: Ahmad Treptt Vazirna

Supervisor: Prof. Doutor Yuri Petrossiuk

Maputo, Julho de 2006

DEDICATÓRIA

Dedico este trabalho a minha família, em especial, ao meu Pai, Emir Vazirna, pelo apoio moral e financeiro que me deu ao longo da minha formação académica.

Às minhas irmãs, Yasmien e Zoarina, pela paciência e amizade que demonstraram ao longo da minha vida.

A minha namorada, Jacqueline, por ter estado ao meu lado tanto nos bons como nos maus momentos.

AGRADECIMENTOS

Agradeço, em especial, o meu supervisor o Prof. Doutor Yuri Petrossuik, pela disposição e paciência que teve para me mostrar o caminho a seguir para a realização deste trabalho, pelas suas criticas que me permitiram aprimorar o mesmo e pelo apoio prestado ao longo de toda investigação.

A todos meus familiares que de forma directa ou indirecta me apoiaram na minha formação académica.

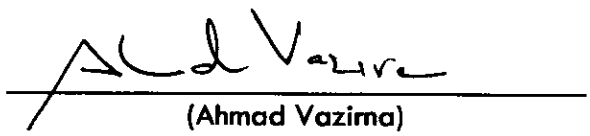
Aos meus amigos, pela compreensão e dedicação que demonstraram ao longo da minha vida, principalmente quando não pude estar com eles por causa das minhas responsabilidades académicas.

Agradeço, também, aos meus colegas de curso, que ao longo do mesmo me apoiaram e com os quais ultrapassei as grandes dificuldades que surgiram ao longo do curso.

Aos docentes e funcionários do DMI, vai um abraço pela paciência que tiveram para comigo ao longo do Curso.

DECLARAÇÃO SOB COMPROMISSO DE HONRA

Declaro por minha honra, que este trabalho é resultado da minha investigação e que nunca foi usado para a obtenção de nenhum outro grau académico que não seja o indicado – **Licenciatura em Informática**, da Faculdade de Ciências da Universidade Eduardo Mondlane (UEM).



(Ahmad Vazirna)

Índice

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E ACRÓNIMOS

DES – Data Encryption Standard

FTP – File Transfer Protocol

IDEA – International Data Encryption Algorithm

IP – Internet Protocol

ISDN – Integrated Service Digital Network

ISO – International Organization for Standarization

ISP – Internet Service Provider

LAN – Local Area Network

MAN – Metropolitan Area Network

MIME – Multi-Purpose Internet Mail Extension

MD5 – Message Digest, Version 5

PGP – Pretty Good Privacy

RDIS – Rede Digital com Integração de Serviços

RSA – Rivest-Shamir-Adelmar

S/MIME – Secure MIME

SSL – Secure Sockets Layer

SI – Sistema de Informação

TCP – Transmission Control Protocol

TIC – Tecnologias de Informação e Comunicação

VLSI – Very-Large-Scale Integration

VSAT – Very Small Aperture Terminal

WAN – Wide Area Network

GLOSSÁRIO

Algoritmo – é uma sequência finita e não ambígua de instruções para solucionar um problema.

Algoritmo RSA – é um algoritmo de encriptação de Chave Pública baseado na exponenciação da aritmética modular.

Aplicação – em Informática, é um programa que executa tarefas de interesse prático que justificam a utilização dos computadores pelos indivíduos e pelas empresas. Ver *Software*.

Arquitecturas de computadores – são as diferenças na forma de fabricação dos computadores. Com a popularização dos computadores houve a necessidade de se interagir um equipamento com outro, surge, assim, a necessidade de se criar um padrão. As mais populares são o PC (*Personal Computer*) da IBM e o Macintosh da Apple.

Assinatura digital – é um mecanismo de autenticação que permite ao emissor duma mensagem anexar um código que actua como uma assinatura. A assinatura garante a origem e a integridade da mensagem.

Autenticação – é um processo usado para verificar a integridade dos dados transmitidos.

Autenticador – é a informação adicional adicionada a mensagem para permitir que o receptor verifique que a mensagem é autêntica.

Bactéria – é um programa que consome os recursos computacionais através da sua replicação.

Biometria [*bio* (vida) + *metria* (medida)] – é o estudo estatístico das características físicas ou comportamentais dos seres vivos. Recentemente este termo também foi associado a medida de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente.

Bit – é a mais pequena parcela de informação que pode ser representada num computador. Fisicamente, pode ser materializado em qualquer dispositivo capaz de assumir dois estados diferentes. Logicamente, usam-se os símbolos "0" (zero) e "1" (um) para representar cada um dos dois estados. Bit significa *Binary Digit*.

Bitwise operation (Lógica binária) – é a base de todo o cálculo computacional. Na verdade, são estas operações mais básicas que constituem todo o poderio dos computadores. Qualquer operação, por mais complexa que pareça, é traduzida internamente pelo processador para estas operações.

Bridge (Ponte) – é o termo utilizado em informática para designar um dispositivo que liga duas redes informáticas que usam protocolos distintos, ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo *ethernet* ou *token ring*.

BSAFE, JSAFE e S/MAIL – é um conjunto de componentes de segurança que permite a inserção de funcionalidades de troca de dados em aplicações de comunicação e E-Commerce.

Bug – é qualquer falha em um programa de computador que o impede de funcionar como esperado. Um *bug* pode ser:

- De ordem **sintáctica**: o uso no programa, de um código inexistente na linguagem de programação;
- De ordem **excepcional**: um erro que produz uma operação lógica ou matemática impossível (como uma divisão por zero);
- De ordem **lógica**: o uso no programa, de um código da forma incorrecta, esperando produzir um resultado.

Byte – é um conjunto de oito bits e constitui a unidade de armazenamento básica da memória e de outros dispositivos de armazenamentos externos, como os discos magnéticos, as disquetes e os CD-ROM.

Câmara Escura – é, basicamente, uma caixa com um buraco em uma das paredes. Com uma abertura pequena o suficiente, a luz de apenas uma parte da cena pode acertar qualquer parte

específica da parede de trás; quanto menor o buraco, mais definida a imagem no lado de trás.

Cerâmica – é a arte de fabricar vasos ou outros objectos de barro ou outra substância congénere.

Cifra – é um algoritmo para encriptação e decriptação. Uma cifra substitui uma peça de informação (um elemento do texto em claro) por outro objecto, com, a intenção de ocultar o seu significado. Geralmente, a regra de substituição é controlada por uma chave secreta.

Cifra de Bloco – é um algoritmo de Encriptação Simétrica em que uma grande quantidade de bits do texto em claro é transformada como um todo em bloco de texto cifrado do mesmo tamanho.

Cifra de Fluxo – é um algoritmo de Encriptação Simétrico em que o texto cifrado é produzido bit-por-bit ou byte-por-byte dum fluxo do texto em claro.

Chave Pública – é uma das duas chaves usadas num sistema de Encriptação Assimétrica. Para uma comunicação segura, a chave privada deve ser conhecida apenas pelo seu dono.

Chave Secreta – é a chave usada num sistema de Encriptação Simétrico. Ambos participantes devem partilhar a mesma chave, e esta chave deve ser mantida em segredo para garantir a segurança da comunicação.

Clientes e Servidores – Numa rede, os computadores partilham serviços e recursos. Quando um computador solicita serviços ou utilização de recursos a outro computador, actua como cliente. O computador que fornece o serviço ou recurso actua como servidor.

Clock – todo processador possui um Clock, que é responsável por indicar a rapidez de processamento de dados do processador. Pode-se encontrar processadores de 2GHz (GigaHertz) o que significa que ele pode efectuar 2 Biliões de processamentos num Segundo (a cada ciclo do relógio).

Computador – é um equipamento electrónico, já quase considerado um electrodoméstico, geralmente associado a um monitor, um teclado e um *mouse*. Por outro lado, é qualquer equipamento ou dispositivo capaz de armazenar e manipular, lógica e matematicamente, quantidades numéricas representadas fisicamente. Exemplos de computadores: ábaco, calculadora, computador analógico, computador digital.

Computador quântico – é um dispositivo que executa cálculos fazendo uso directo de propriedades da mecânica quântica, tais como sobreposição e emaranhamento. Teoricamente, computadores quânticos podem ser implementados e o mais desenvolvido actualmente trabalha com poucos qubits (bit quântico) de informação. O principal ganho desses computadores é a possibilidade de resolver em tempo eficiente, alguns problemas que na computação clássica levariam tempo impraticável, como por exemplo: factorização, busca de informação em bancos não ordenados, etc.; pois possuem a capacidade de realizar cálculos simultâneos.

Comunicação – é o intercâmbio de informação entre sujeitos ou objectos. Deste ponto de vista, a comunicação inclui temas técnicos (por exemplo, a telecomunicação), biológicos (por exemplo, fisiologia, função e evolução) e sociais (por exemplo, jornalismo, relações públicas, publicidade, audiovisual e meios de comunicação de massa).

Confusão – é uma técnica criptográfica que procura tornar a relação entre a estatística do Texto Cifrado e o valor da Chave de encriptação o mais complexo possível. Isto alcança-se pelo emprego dum complexo algoritmo que depende da chave e da entrada.

Criptoanálise – é a parte da Criptologia que se preocupa com a quebra duma Cifra para recuperar a informação, ou forçar informação encriptada que será aceite como autentica.

Criptoanálise Diferencial – é uma técnica em que textos em claro escolhidos com diferenças padrões XOR específicos são encriptados. As diferenças dos padrões do texto cifrado resultante providenciam informação que pode ser usada para deduzir a Chave de encriptação.

Criptografia – é a parte da Criptologia que trata do desenho de algoritmos para encriptação e

decriptação, com o objectivo de garantir a segurança e/ou autenticidade duma mensagem.

Criptografia Quântica – é um método de criptografia mais antigo que à descoberta da criptografia de Chave Pública, a pode ser usada para unir duas mensagens em uma única transmissão quântica na qual o receptor poderia decodificar cada uma das mensagens porém nunca as duas simultaneamente. A Criptografia Quântica utiliza princípios físicos da matéria para permitir criar uma chave secreta que não pode ser quebrada (nem por um computador quântico). Ao basear-se nos princípios da Mecânica Quântica este método garante assim a segurança.

Criptologia – é o estudo da segurança das comunicações, o que inclui ambas Criptografia e Criptoanálise.

Dados – constituem a informação que descreve os objectos, os factos e os fenómenos do mundo real. Por vezes, usa-se a designação dados para se referir o *input* que é introduzido no computador, antes de ser processado. O resultado do processamento é denominado Informação. Deste modo, os dados podem ser considerados como a "matéria-prima" a partir da qual se cria a Informação. Esta classificação é, no entanto, relativa e arbitrária, porque aquilo que em determinado contexto constitui informação poderá funcionar como dado ou "matéria-prima" num outro processo de tratamento de dados. Uma outra classificação, também usada com frequência, distingue dados e programas. Neste caso, os dados constituem a informação, e os programas são as rotinas que actuam sobre esses dados, transformando-os ou apresentando-os sob outra forma.

Decriptação – é a translação dum texto ou dado encriptado (denominado Texto Cifrado) para o texto ou dado original (denominado texto em claro). É também denominado *Decifração*.

Difusão – é uma técnica criptográfica que procura ocultar a estrutura estatística do texto em claro através da dispersão da influência de cada dígito do texto em claro sobre muitos dígitos do texto cifrado.

Digrama – é uma sequência de duas letras. Em Inglês ou outras línguas, a frequência relativa de vários digramas no texto em claro podem ser usado na criptoanálise de algumas Cifras. Também conhecido por *Dígrafo*.

Download – é a transferência dum ficheiro dum servidor da Internet para um computador local.

E-Commerce – é o mesmo que comércio electrónico, também conhecido como E-Business.

E-mail – é a abreviatura de *electronic mail*. Esta expressão designa o correio electrónico, através do qual os utilizadores podem trocar mensagens constituídas por texto, imagens, vídeo e som.

Efeito Avalanche – é a característica dum algoritmo criptográfico em que uma pequena alteração no texto em claro e na chave resulta numa grande mudança no texto cifrado.

Encriptação – é o processo de conversão do texto em claro ou dado em uma forma incompreensível usando uma translação reversível, baseado numa tabela ou algoritmo de translação. Também é denominada *Encifração*.

Encriptação Assimétrica – é um tipo de criptosistema em que a encriptação e decriptação são efectuadas usando duas chaves diferentes, uma denominada Chave Pública e outra Chave Privada. Também é denominada *Encriptação de Chave Pública*.

Encriptação da Chave Pública – é o mesmo que *Encriptação Assimétrica*.

Encriptação Convencional – é o mesmo que Encriptação Simétrica.

Encriptação Múltipla – é o uso repetido duma função de encriptação, com chaves diferentes, para produzir um mapeamento mais complexo de texto em claro para cifrado.

Encriptação Simétrica – é um tipo de criptosistema em que a encriptação e decriptação são executados usando a mesma chave. Também é conhecida como *Encriptação Convencional*.

Esteganografia – é a arte de escrever em cifras ou em sinais convencionais.

Ethernet – é uma tecnologia de interconexão para LAN'S baseada no envio de pacotes.

Firewall – é um programa desenvolvido por empresas de software, com o objectivo de evitar os "Blended Threats" (códigos maliciosos que se espalham pela Internet sem que o utilizador do computador que infecta/está a infectar saiba) e os ataques de programas espiões. Falando da sua função relacionada com os vírus, este programa vigia as "portas" (as portas são aquelas que deixam passar a informação da Internet/computador, conforme o protocolo.

FTP – é um protocolo usado na Internet para a transferência de ficheiros entre computadores.

Gateway – é um dispositivo que executa uma conversão da camada do aplicativo de informações de uma pilha de protocolos para outra.

Hardware – é o termo usado para designar todos os componentes físicos do computador quer seja de natureza electrónica, mecânica ou magnética.

Homófonos – são palavras que possuem uma grafia diferente mas que tem o mesmo som e se pronunciam da mesma maneira.

Host – é qualquer máquina ou computador conectado a uma rede. Os hosts variam de computadores pessoais a super-computadores, dentre outros equipamentos, como roteadores.

Hub – é o aparelho que interliga diversos. O Hub é indicado para redes com poucos terminais de rede, pois o mesmo não comporta um grande volume de informações passando por ele ao mesmo tempo.

Informação – é um termo que pode assumir muitos significados dependendo do contexto, em Informática relaciona-se com o processamento de dados brutos. A informação representa o dado interpretado, contextualizado ou útil para alguém.

Informática – é o conjunto de ciência e técnica que tem por objecto o tratamento de dados relativos à informação por processos racionais e automáticos, que implicam a utilização de um computador e aparelhos complementares deste.

Input (Entrada) – é o processo através do qual os dados são introduzidos num computador, para processamento ou armazenamento. O input pode ser manual ou automático. O input manual é aquele que é efectuado pelo utilizador, geralmente através do teclado e do rato. O input automático é aquele que é feito por outro dispositivo. Por exemplo, o envio de dados do disco duro para a memória é um processo de input automático. Esquematicamente, considera-se input todo o processo de envio de dados para memória e para o processador.

Intaglio – é uma técnica de impressão na qual uma imagem é inserida numa superfície. Normalmente, cobre ou pratos de zinco são usados como superfície.

Internet – é a maior rede de computadores existente na Terra. O termo Internet pode ser usado para designar um sistema de redes de computadores interligadas.

Internet-Café (Cyber café) – é um local que, além de funcionar como bar ou pastelaria, oferece a seus clientes acesso à *Internet* mediante o pagamento de uma taxa, usualmente cobrada por hora.

Intranet – é uma rede de computadores privativa que utiliza as mesmas tecnologias que são utilizadas na Internet. O protocolo de transmissão de dados de uma intranet é o TCP/IP e sobre ele podemos encontrar vários tipos de serviços de rede comuns na Internet, como por exemplo o e-mail, chat, grupo de notícias, HTTP, FTP entre outros.

Intruso – é qualquer indivíduo que obtêm, ou tenta obter, acesso não autorizado num sistema computarizado ou privilegio não autorizados num Sistema.

ISDN (RDIS) – é um protocolo de comunicação, oferecido por empresas de telefonia, que permite que redes de telefone transportem tráfegos de dados, voz e de outros tipos. O ISDN já existe a algum tempo, sendo consolidado nos anos de 1984 e 1986.

Kbyte – é um múltiplo do byte. Corresponde a 1024 bytes. Esta unidade é usada para medir a capacidade de dispositivos pequenos.

LAN – é um tipo de rede na qual os computadores participantes se encontram localizados dentro dum mesmo edifício.

Laser (Light Amplification by Stimulated Emission of Radiation) – é um dispositivo que produz radiação electromagnética com características muito especiais, isto é, ela é monocromática (possui frequência muito bem definida) e coerente (possui relações de fase bem definidas), além de ser colimada (propaga-se como um feixe).

Layout – é um esboço mostrando a distribuição física e tamanhos de elementos como texto, gráficos ou figuras num determinado espaço.

Licenças – é uma permissão de uso dum software, isto é, de que forma o tal programa pode ser usado, basicamente se você deve pagar para ter o direito de usá-lo (o exemplo mais famoso é o sistema operacional Windows), se você pode usá-lo gratuitamente (freeware, como muitos programas em sites de downloads, muitos acompanhados de spywares) e se você tem direito total sobre ele, o seu código fonte, podendo modificá-lo e vendê-lo se desejar, apenas com restrições quanto ao uso de marcas (o sistema operacional Linux e o navegador Firefox fazem parte desse grupo).

Link – é um canal de comunicação de rede que consiste em um caminho de circuito ou transmissão e em todos os equipamentos relacionados entre o emissor e o receptor. Mais frequentemente usado para se referir a uma conexão WAN.

Malware – é um software malicioso. Pode ser um vírus, uma bactéria, etc.

MAN – são redes ou ligações entre redes de computadores dentro da área geográfica de uma mesma cidade.

Microondas – são ondas electromagnéticas no intervalo de 1 a 30 GHz. As redes baseadas em microondas são uma tecnologia em evolução ganhando espaço devido à largura de banda alta e custo relativamente baixo.

MIME – é um protocolo usado para correio electrónico na *Internet*.

Mnemónica – é a arte de usar ou cultivar a memória.

Multimédia – é a combinação de dois ou mais meios (som, vídeo, animação e gráficos) numa aplicação. As grandes quantidades de informação que o ficheiro multimédia utiliza obrigam à utilização de dispositivos de armazenamento de alta capacidade.

Multiplexação – é uma técnica através da qual informações de canais lógicos múltiplos podem ser transmitidas através de um único canal físico.

Odómetro – é um instrumento que serve para medir as distâncias percorridas.

Online – é um termo Inglês usado para designar uma ligação electrónica com acesso permanente. Por outro lado, **offline** traduz-se na indisponibilidade da entidade perante o sistema.

Offline – ver *online*.

Output (Saída) – é o resultado dum processamento efectuado por um processador. Dependendo do tipo de processamento efectuado e do tipo de informação resultante, o output dum computador pode ser enviado para o ecrã, impressora, discos e disquetes do computador, colunas do som, ou mesmo para outros computadores e dispositivos que estejam acessíveis através da rede.

Packet switching – são caminhos full duplex estabelecidos, em que os pacotes somente transitarão por eles.

Paleografia – é a arte de decifrar escritos antigos.

Pasigrafia – é a escrita Universal para ser entendida por todos. Sistema de abreviaturas taquigráficas.

Pedra de Roseta – é um bloco de granito negro que proporcionou aos investigadores ler um mesmo texto escrito em egípcio demótico, grego e em hieróglifos egípcios. A pedra serviu de chave para a decifração dos hieróglifos.

Pedra Filosofal – é uma pedra que, segundo os alquimistas, devia efectuar a transmutação dos metais em ouro.

Performance – é uma locução estrangeira (Inglesa) que significa desempenho.

Pipeline – é uma técnica de hardware que permite que a CPU realize a busca de uma ou mais instruções além da próxima a ser executada. Estas instruções são colocadas em uma fila de memória (dentro da CPU) onde aguardam o momento de serem executadas.

PGP – é um programa de computador que utiliza criptografia para proteger a privacidade do E-mail e dos arquivos guardados no computador do usuário. PGP pode, ainda, ser utilizado como um sistema à prova de falsificações de assinaturas digitais, permitindo desta forma a comprovação de que arquivos ou e-mails não foram modificados.

Processamento – é o processo de transformação a que os dados são submetidos no interior do computador pelos programas. Como exemplos de processamento efectuados por programas de computador pode-se citar:

1. O acesso a uma base de dados para pesquisa de informação e elaboração de indicadores de Gestão;
2. A integração de imagens estáticas ou animadas num filme digitalizado;
3. A utilização de diversos tipos de caracteres e estilos num texto digitado pelo utilizador através do teclado.

Protocolo – é um conjunto de especificações e regras através dos quais duas camadas do mesmo nível da arquitectura de rede podem estabelecer uma comunicação virtual.

Proxy – é um software que faz de *cache* em redes de computadores. São máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.

PSN (Packet-switched network) – é uma rede de comutação de pacotes. É uma Rede que utiliza a tecnologia de comutação de pacotes para transferir dados.

Repetidor – é um dispositivo usado para estender a dimensão de uma rede. O repetidor gera os sinais da rede novamente e os retemporiza no nível do bit para que eles trafeguem em uma distância maior nos meios.

Rococó – é um género de ornamentação muito usado durante o reinado de Luís XV e princípios do de Luís XVI, de França. Serve para caracterizar um objecto antigo, ultrapassado ou de mau gosto.

Router (Roteador) – é um equipamento usado para fazer a comunicação entre diferentes redes de computadores. Este equipamento provê a comunicação entre computadores distantes entre si e até mesmo com protocolos de comunicação diferentes.

Satélite artificial – é qualquer corpo feito pela mão humana que orbita um planeta. Actualmente estão em órbita, para alem dos satélites do sistema GPS, satélites de comunicações, satélites científicos, satélites militares e uma grande quantidade de lixo espacial. Os satélites de comunicações são satélites que retransmitem sinais entre pontos distantes da Terra. Estes satélites servem para retransmitir sinais de televisão, rádio ou mesmo telefone. Os satélites científicos são utilizados para observar a Terra ou o espaço ou para realizar experiências em microgravidade.

Sinóptica – refere-se a uma obra ou tratado que apresenta em síntese o conjunto de uma ciência.

Sistema de Informação – é o termo utilizado para descrever um sistema automatizado ou manual, que abrange pessoas, máquinas, e/ou métodos organizados para colectar, processar, transmitir e disseminar dados que representam informação para o usuário.

Software – é o conjunto de programas que asseguram o funcionamento dum computador. Os componentes fundamentais do software de um computador são o BIOS, o sistema operativo e os programas de aplicação. Ver *Aplicação.*

Switch (Comutador) – é um dispositivo utilizado em redes de computadores para reencaminhar dados entre os diversos nós. Possuem diversas portas, assim como os hubs, e operam na camada acima dos hubs. A diferença é que segmenta a rede internamente, sendo que a cada porta corresponde um segmento diferente, o que significa que não haverá colisões entre tramas de segmentos

diferentes — ao contrário dos *hubs*, cujas portas partilham o mesmo domínio de colisão.

TCP/IP – é um o grupo de protocolos de comunicação que implementam a pilha de protocolos sobre a qual a *Internet* e a maioria das redes comerciais roda. Deriva das siglas TCP e IP.

Tecnologias de informação e comunicação – são o conjunto de meios tecnológicos que nos ajudam a adquirir, tratar ou processar, guardar e partilhar informação e conhecimento. Portanto, estas tecnologias incluem o computador, a rádio, a televisão, o telefone fixo e o móvel, a Internet, o correio electrónico, as máquinas ATM dos bancos, os faxes, os cartões bancários, os *walkman*, os leitores de CDs e DVDs, etc.

Texto Cifrado – é a saída dum algoritmo de encriptação. É a forma encriptada duma mensagem ou dados.

Texto em Claro – é a entrada duma função criptográfica ou a saída duma função de decriptação.

Tomografia – é uma imagem que deriva do tratamento informático dos dados obtidos numa série de projecções angulares de raios X.

Transponder – é um dispositivo que recebe, amplifica e retransmite um sinal em uma frequência diferente ou transmite uma mensagem pré-determinada em resposta a um sinal pré-definido anteriormente. O transponder é um dispositivo de rastreamento capaz de localizar diversos objectos em determinados lugares de acordo com a frequência pré-programada. O transponder é um dispositivo semelhante ao GPS, porém não é necessário ter-se um satélite, com isso seu custo é menor, mas a sua desvantagem em relação ao GPS é seu alcance, que é muito menor.

Trojans (Cavalos de Tróia) – é um programa que permite que um computador possa receber comandos externos, sem o conhecimento do usuário do mesmo. Desta forma o intruso pode ler, copiar, apagar, alterar dados do sistema e, em certos casos, roubar dados confidenciais do usuário, como senhas bancárias. Os trojans podem ser instalados através dum vírus ou quando um usuário faz um *download* e depois executa o arquivo.

Velocidade da Luz – simbolizada por c, é a velocidade da luz no vácuo e é igual a aproximadamente 300.000 Km/s.

Verme (Worm) – é um programa que apenas se replica, com o objectivo de causar graves danos ao sistema. Desta forma, seus autores visam tornar suas criações mais conhecidas na Internet. Os vermes não precisam infectar arquivos legítimos do sistema. Eles instalam um sistema completo para o seu funcionamento.

Vírus – é um programa malicioso desenvolvido por programadores que, como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios. A maioria das contaminações ocorrem pela acção do usuário executando o anexo de um e-mail. A segunda causa de contaminação é por Sistema Operacional desactualizado, sem a aplicação de correctivos que bloqueiam chamadas maliciosas nas portas do micro.

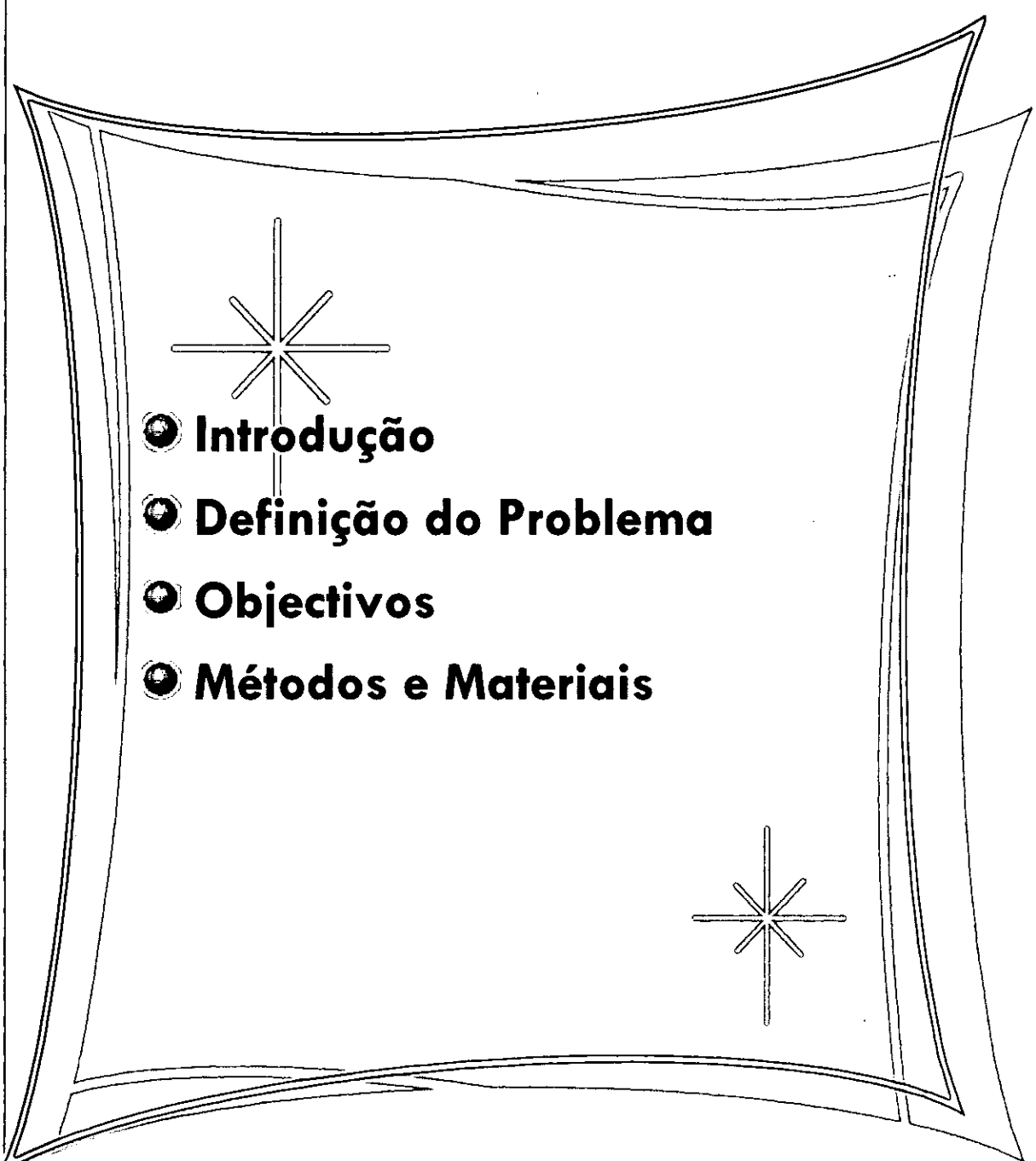
WAN – são as redes ou sistemas de ligação entre redes em maiores distâncias do que as MAN. Uma WAN pode interligar computadores e redes situados em diferentes continentes.

Wiring closet – é uma sala especialmente projectada e usada para cabear uma rede de dados ou de voz. "Wiring closets" servem como um ponto de junção central para o cabeamento e o equipamento de cabeamento que são usados para interconectar dispositivos.

WWW (World Wide Web) – é uma rede mundial de computadores. Grande rede de servidores da Internet que fornecem hipertexto e outros serviços aos terminais que executam aplicativos de clientes, como, por exemplo, um navegador da WWW.

CAPÍTULO I

INTRODUÇÃO



- Introdução
- Definição do Problema
- Objectivos
- Métodos e Materiais

1. INTRODUÇÃO

Desde o seu surgimento, acerca de 4 milhões de anos, que o Homem teve necessidades. Com a finalidade de as saciar este foi obrigado a raciocinar e procurar soluções, o que o fez evoluir. Deste modo, pode-se afirmar que a evolução do Homem esteve sempre ligada as suas necessidades [13].

Com o desenvolvimento das Sociedades, caracterizado por um crescimento Populacional, o Homem concluiu que para satisfazer as suas necessidades individuais e colectivas deveria cooperar com o seu semelhante, o que culminou com o surgimento das Organizações, que se dedicam a uma ou mais actividades económicas, tendo umas se dedicado ao fabrico de bens, outras a comercialização desses mesmos bens, outras com objectivos Políticos, outras com o objectivo de prestar serviços de vários tipos (Saúde, Educação, Transporte, etc.). Umas das principais características de qualquer actividade económica é que ela gera, ou melhor, trabalha com dados, o que fez com que um dos primeiros desafios das Organizações fosse o de definir mecanismos adequados para o processamento, captação e armazenamento destes dados. Pois é através dos dados que as Organizações obtêm informação que é usada para a tomada de decisão, coordenação da sua actividade, controlo, análise da sua expansão e resolução de conflitos. De maneira que, o tratamento dos dados deve ser objectivo, rápido e fiável, para que se produza informação útil, atempada e confiável.

Inicialmente a gestão dos dados estava confinada a processos manuais, como o recurso ao papel para o registo e tratamentos dos dados, o uso de ficheiros e armários para o armazenamento, este modelo de trabalho era muito limitado e caro. Por exemplo, o cálculo de transacções era efectuado por uma equipa numerosa de escriturários, o que acarretava custos e aumentava a probabilidade de ocorrência de erros, e em determinadas áreas como a ciência e a engenharia eram necessárias Tabelas de Números cada vez maiores [8].

Com o início da Revolução Industrial no século XVIII e a consequente expansão da mesma pelo mundo inteiro, as actividades económicas tornaram-se cada vez mais complexas, principalmente devido ao crescimento do volume de trabalho das Organizações provocado pelo aumento da Procura e Oferta de Bens e Serviços. Além da complexidade, a Revolução Industrial veio elevar o nível de concorrência entre Organizações que se dedicavam a uma mesma actividade. Estes dois factores fizeram

com que as Organizações procurassem alternativas a gestão manual dos dados, pois tinham necessidades de faze-lo de forma mais eficaz e eficiente, principalmente no que diz respeito a execução de operações aritméticas visto que o volume de dados aumentou consideravelmente, e que, também, lhes permitissem competir num mercado cada vez mais "agressivo" em que a capacidade de satisfazer o Cliente ditava o sucesso da Organização. Além disso, está Revolução, provocou uma mudança na forma como as Organizações faziam uso da sua Informação, o que fez com que a mesma passasse a ser considerada um Recurso da própria Organização, assim como as Instalações, Propriedades, Recursos Humanos e Capital. Esta procura de alternativas de processamento e a valorização da informação impulsionou o surgimento de grandes avanços científicos e tecnológicos na área da colecta, processamento, disseminação e armazenamento da informação, como foi o caso do computador durante o século XIX [8].

O Computador veio dinamizar o modo de trabalho Humano, permitindo a redução de custos da maior parte das operações das actividades económicas, como por exemplo, o processamento de salários de forma mais rápida e menos onerosa, a gestão de inventários das lojas muito mais eficazes, o controlo mais eficiente de processos industriais complexos como a refinação de petróleo, a laminagem do aço, a montagem na Industria Automóvel, etc. Com o passar do tempo, o computador foi ganhando popularidade passando a ser usado num simples processo de compra e venda dum estabelecimento Comercial e por fim, ao uso doméstico [8]. Para o caso concreto de Moçambique, prevê-se que em 2006 existam cerca de 600.000 Computadores, o que faz com que a proporção do número de Computadores/Habitantes seja de 3/100 [41].

Esta rápida expansão do computador, grandemente provocada pela necessidade de se processar dados de forma mais eficaz, fez com que este fosse considerado o invento mais inovador de sempre pois revolucionou a forma do Homem pensar e agir, tendo alterado, também, o modelo de Gestão das Organizações. Deste modo, a gestão da informação tornou-se na actividade mais complexa e dispendiosa de qualquer organização, pois os Gestores deram-se conta de que sem a informação a sua Organização não poderia continuar com a sua actividade e em certos casos entraria em falência; por outro lado, a boa Gestão da mesma permitiria a Organização se precaver de possíveis catástrofes naturais, incêndios, acções criminosas, etc. De maneira que, foram obrigados a definir políticas para proteger a *informação armazenada no computador* contra a perda, destruição e roubo. Esta Política tem como

objectivo principal, impedir o acesso ilegal tanto das instalações onde o Sistema de Informação actua, como dos próprios computadores onde a informação está armazenada, com o recurso a guardas, câmaras de vigilância, cofres, alarmes, o uso da biometria para o controle de acesso, etc.; além disso, produzir cópias periódicas dos dados e instaura-los num outro computador que se encontra geograficamente distante.

1.1. Definição do Problema

O aumento do número de computadores por instituição e a expansão dos chamados Sistemas de Informação criou nas Organizações a necessidade de partilhar recursos computacionais, correlacionar e trocar informação e disseminar a informação de forma rápida e para o usuário certo, é neste âmbito que surgem as redes de computadores, responsáveis por fazer com que todos recursos computacionais, como aplicações, base de dados, hardware, etc., estejam disponíveis para qualquer um numa Rede [18]. A implementação destas redes culminou com a invenção da *Internet* que veio facilitar, ainda mais, a troca de informação. Esta possibilidade contribuiu para que as Organizações expandissem as suas actividades além Fronteira, criando assim, a Sociedade Global de Informação; em que Homens, Sistemas e Organizações interagem à baixo custo e independentemente da sua localização geográfica, cultura, língua, Regime Político e Economia, permitindo que a informação esteja disponível a todos intervenientes da Organização. Contudo, esta troca faz com que a informação circule por um meio de transmissão o que a deixa vulnerável, este facto aliado a crescente valorização da Informação e consequente interesse pela mesma por parte de indivíduos e Organizações alheias a Organização, fez com que fosse necessário implementar medidas de segurança para a *rede de computadores* a que um computador pode pertencer, podendo ser a *Internet* ou uma intranet. Para este caso não se podem aplicar as mesmas medidas que as das instalações, pois os meios de transmissão estendem-se por milhares e milhares de quilómetros daí que não seria economicamente viável, por exemplo, colocar guardas em todos segmentos desse meio, em vez disso devem-se definir mecanismos, a baixo custo, que protejam a informação durante a sua transmissão. A solução mais eficaz para este problema é "mascarar" a informação, a ser enviada, produzindo um texto aparentemente confuso e sem sentido, para que mesmo tendo acesso a ele, um intruso não possa lê-lo; uma vez no destino este mesmo texto é "desmascarado" e torna-se novamente legível, esta ciência ficou conhecida como *Criptografia*, e consiste, basicamente no uso dum *algoritmo* e, por vezes, duma ou mais *chaves*. O sucesso desta técnica depende da

utilização dum algoritmo suficientemente forte e que dificulte qualquer tentativa ilegal de "desmascarar" a informação, ciência esta conhecida como *Criptoanálise*, e também em manter a ou as chaves secretas.

Por outro lado, as oportunidades de acesso as redes de computadores aumentaram com o acesso a *Internet*, o que facilitou a instalação ilícita de malwares nos computadores da Organização, por indivíduos com a intenção de lesar o funcionamento e os recursos dos mesmos [39]. Contudo, este tipo de ataques não é o que mais preocupa as Organizações pois existem mecanismos, como softwares apropriados, para detecta-los e em certos casos combate-los. Além disso, esta forma de ataque já foi bastante difundida, pois afectam drasticamente o funcionamento dos computadores, de maneira que, os gestores, mesmo em países em desenvolvimento, já se consciencializaram para a necessidade de definir medidas de segurança contra os mesmos.

Como se pode denotar, a segurança da informação durante a sua transmissão, tornou-se na grande preocupação dos gestores, principalmente em organizações de considerável magnitude, em que a informação circula por muitos locais, muitos dos quais estranhos a própria Organização.

Ao longo dos anos foram propostos vários algoritmos criptográficos e com eles foram aumentando as tentativas de quebra-los. Aliado a isto, esta o facto de que os SI vêm-se tornando mais complexos e requerem o uso dum algoritmo que não sobrecarregue o sistema, o que dificulta ainda mais a tomada de decisão no que concerne a: que medidas implementar? quais as mais eficazes? quanto devo gastar para proteger os meus dados? quanto valem os meus dados? a quem interessam os meus dados? E é sobre como responder a estas questões relacionadas com a transmissão da informação que este trabalho se debruça. Para tal, ele descreve aspectos ligados a segurança de SI e faz uma comparação entre os principais algoritmos criptográficos, propondo, também, um novo algoritmo, mais adequado às novas exigências dos SI's.

1.2. Objectivos

1.2.1. Objectivo Geral

- Desenvolver um sistema criptográfico baseado no algoritmo simétrico IDEA e nos Códigos de Fibonacci.

1.2.2. Objectivos específicos

- Identificar os principais problemas e ataques da segurança da informação que as organizações enfrentam;
- Consciencializar os gestores da informação e os próprios usuários das TI sobre os perigos que advêm da má utilização dos mecanismos de segurança;
- Fazer uma análise comparativa entre a Criptografia Simétrica e Assimétrica, identificando assim as vantagens e desvantagens de cada um;
- Motivar as organizações para o uso da criptografia como forma de tornar os seus sistemas de informação mais seguros;
- Comparar os algoritmos simétricos entre si, demonstrando assim as vantagens do IDEA;
- Analisar a adaptabilidade dos Códigos de Fibonacci em Sistemas Criptográficos, incorporando-os no IDEA;
- Disponibilizar uma bibliografia que retrate os princípios e práticas da criptografia e segurança de sistemas de tecnologias de informação e comunicação, e;
- Apresentar um resumo de todos os resultados dos testes como forma de fundamentar os objectivos deste estudo e tirar as devidas conclusões, produzindo, assim, um manual que servirá de suporte ao gestor para a tomada de decisão quanto a questões de segurança.

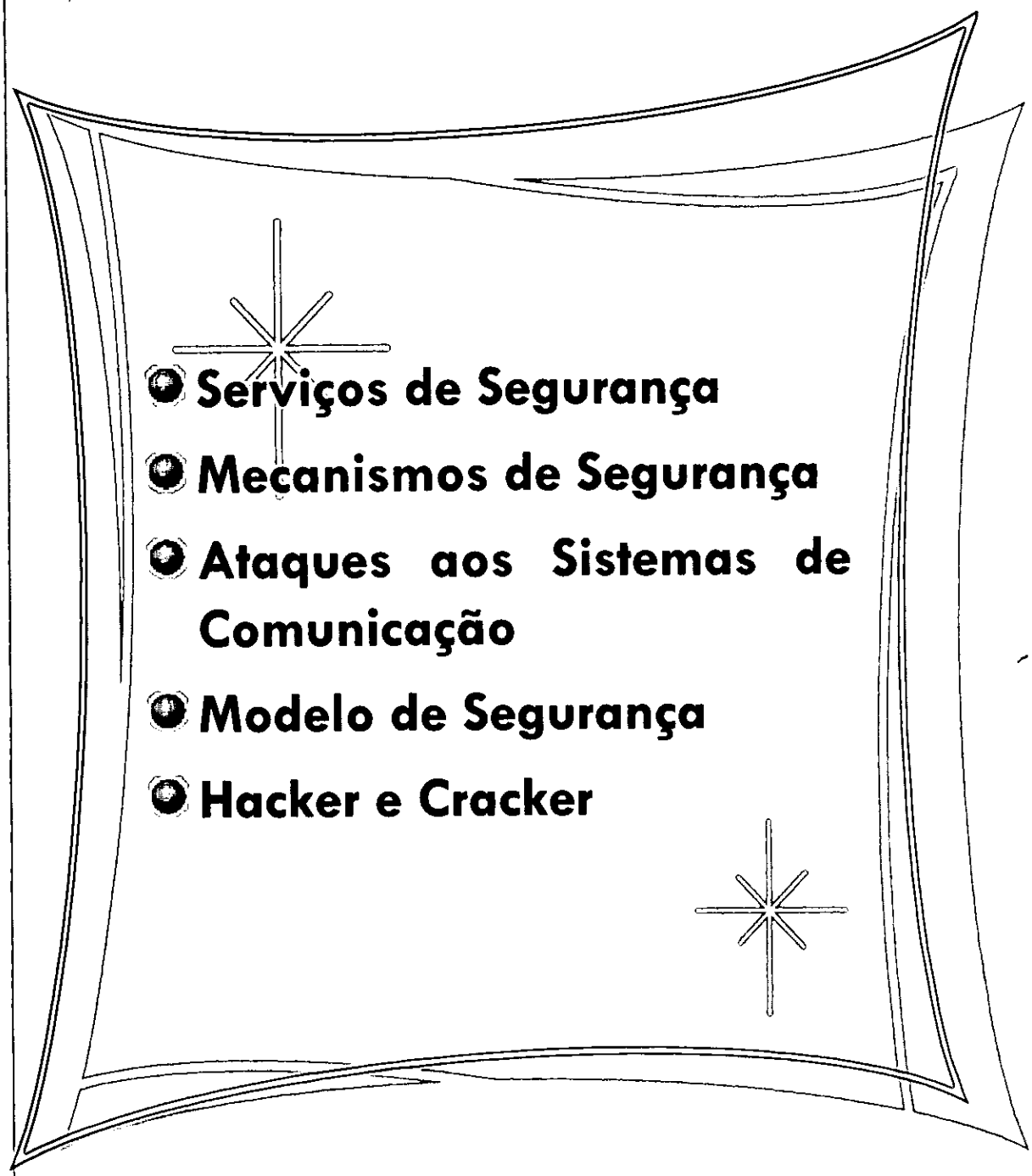
1.3. Métodos e Materiais

Para a realização deste trabalho investigativo estão previstas as seguintes etapas:

- Estudo teórico do tema que consistirá na pesquisa bibliográfica, pela Internet e pela consulta da bibliografia impressa disponível;
- Efectuar entrevistas junto aos gestores para ficar a par das suas necessidades e dos ataques mais comuns a sua segurança;
- Desenvolver uma aplicação, em Delphi, que gera os Códigos de Fibonacci, como forma de analisar o seu comportamento;
- Analisar o desempenho do algoritmo IDEA em termos de rapidez e segurança comparando-o aos restantes algoritmos simétricos, desenvolvendo, para o efeito, uma aplicação, em Delphi, que implemente todos estes algoritmos e testando-os numa pequena rede de três computadores baseada em Windows;
- Implementar o IDEA-F na aplicação acima mencionada e comparar o seu desempenho com os demais algoritmos, e;
- Simular a intercepção da informação na rede usando um software apropriado.

CAPÍTULO II

SEGURANÇA DA INFORMAÇÃO



- Serviços de Segurança
- Mecanismos de Segurança
- Ataques aos Sistemas de Comunicação
- Modelo de Segurança
- Hacker e Cracker

2. SEGURANÇA DA INFORMAÇÃO

Para se analisar as necessidades em termos de segurança duma Organização e se efectuar uma escolha sensata de Políticas e Ferramentas a adoptar, o Gestor de segurança deve ter em consideração os seguintes aspectos [16]:

- **Serviço de segurança:** é um serviço que eleva a segurança dos sistemas de processamento de dados e da transferência de informação duma Organização. Os serviços tem como objectivo conter os ataques de segurança, e eles fazem uso de um ou mais mecanismos de segurança para providenciar o serviço;
- **Mecanismo de segurança:** é um mecanismo que é desenvolvido para detectar, prevenir e recuperar dados em caso de ataques à segurança, poder ser, por exemplo, um sistema de Backup de dados;
- **Ataque à segurança:** interpreta-se como sendo qualquer acção que comprometa a segurança da informação pertencente a uma Organização.

Como exemplo de violação da segurança, pode-se citar casos como [15]:

- Um funcionário de uma organização "A" pretende enviar uma mensagem ao funcionário "B" fazendo uso da rede interna de dados, um outro funcionário "C" que não está autorizado a ler o conteúdo da mensagem pode facilmente, por pertencer a organização e consequentemente ter acesso a rede, monitorar a transmissão e capturar uma cópia da mensagem;
- Pior que interceptar uma mensagem, um funcionário "A" produz uma mensagem com instruções desejadas e transmite ao servidor do sistema fazendo-se passar pelo administrador, estas instruções podem ser para actualizar o ficheiro de autorizações dos usuários concebendo ao funcionário acesso total ao sistema;
- Quando um funcionário é despedido, o Gestor dos Recursos Humanos envia uma mensagem ao servidor com instruções para encerrar a conta do funcionário. Após o encerramento, o servidor insere uma nota no ficheiro dos funcionários confirmando assim a acção. O funcionário como ainda tem acesso a rede pode interceptar a mensagem e atrasa-la o suficiente para poder aceder uma ultima vez o sistema e retirar informação confidencial relativa a Organização. Depois a mensagem segue o seu curso e consequentemente a acção é executada e a nota inserida. O acesso do funcionário não irá ser detectado por um tempo considerável;

- Uma mensagem é enviada por um cliente para um armazenista com instruções para várias transacções. Por um acaso os produtos solicitados podem-se desvalorizar no mercado, diminuindo assim o seu preço de venda e consequentemente ser tabelado com um valor inferior ao da compra, por esta situação trazer prejuízos ao cliente este pode alegar que não efectuou nenhuma encomenda;
- Um intruso pode enviar uma mensagem contendo softwares maliciosos a um funcionário da organização, e enquanto este lê a mensagem o software é instalado no computador. Este software pode ser um vírus, trojan, bactéria, verme, etc. Destes softwares, o mais preocupante é o trojan, pois este dá acesso total do computador e consequentemente do sistema ao intruso, alem disso, uma das características mais importante deste software é a difícil detecção do mesmo pois ele age sem atrapalhar o trabalho do funcionário.

2.1. Serviços de Segurança

A maior parte das actividades humanas depende do uso do documento. Os documentos geralmente possuem assinaturas, datas, podem ser protegidos contra a leitura e divulgação não autorizada, alteração e mesmo destruição, podem ainda ser reconhecidos e autenticados, podem também ser copiados ou licenciados. Quanto mais as TIC's se expandem e se tornam imprescindíveis para a actividade humana mais a informação electrónica substitui a física, deste modo todos os atributos que o documento possuía devem agora ser implementados, mesmo que em diferente plataforma, na informação electrónica, pois analisando as medidas de segurança da informação física e comparando-as com a electrónica, nota-se que apesar dos demais avanços verificados na área das TIC's, a questão da segurança continua sendo um problema crónico quando se pretende armazenar e transmitir a informação em formato electrónico, isto é [15]:

- No formato físico é possível distinguir uma cópia do seu original, enquanto que no electrónico por ser uma sequência de bits é impossível fazer esta distinção;
- Qualquer alteração do conteúdo de um documento físico pode deixar evidências da mesma, como um borrão, o que não acontece num electrónico, em que se alteram apenas os bits, e;
- A proveniência ou até o autor de um documento físico podem ser, facilmente, reconhecidos através do uso de um timbre, assinatura, carimbo, e até tipo de letra do autor, o que é impossível num documento electrónico.

Analisando as diversas actividades em que são empregues os documentos, podemos concluir que a estes estão associados factores, como:

- Identificação;
- Autorização;
- Licença e ou certificação;
- Assinatura;
- Testemunhas;
- Consentimento;
- Responsabilidade;
- Recibos;
- Certificação da origem e do destinatário;
- Endosso;
- Acesso (egresso);
- Validação;
- Período de validação;
- Autenticidade;
- Voto;
- Proprietário;
- Registro;
- Aprovação/reprovação, e;
- Privacidade (secretismo).

Quando implementados em conjunto os factores acima descritos, estes ajudam a garantir a:

- Confidencialidade;
- Autenticação;
- Integridade;
- Não-Repudiação;
- Controlo de acesso, e;
- Disponibilidade.

2.2. Mecanismos de Segurança

Os mecanismos devem ser definidos tanto para a segurança física como para a lógica da informação, dai que um mecanismo só, não pode satisfazer todos os aspectos mencionados atrás, contudo existe um que se distingue dos restantes pela sua importância, que é a *criptografia*. Sistemas criptográficos são os mecanismos mais usados para providenciar uma melhor segurança, dado que são geralmente baratos, podem ser adaptados ou integrados na maior parte dos SI´s e não precisam muito da intervenção Humana, e por isso são muito usados para garantir a segurança da informação durante a sua transmissão.

2.3. Ataques aos Sistemas de Comunicação

Em SI onde a informação por si só não possui uma representação física, a segurança da informação se centra no facto de como prevenir uma intrusão ou, se isto falhar, detectar a intrusão e recuperar da mesma.

Para entender os ataques devemos entender porque somos atacados, os motivos dos intrusos são vários tentarei aqui mencionar alguns, nomeadamente [15]:

- Para ter acesso a informação;
- Impressionar um outro usuário ou mesmo para responsabilizar um outro usuário, por:
  - Originar informação fraudulenta;
  - Modificar informação legítima;
  - Usar identidade falsa para ter acesso a locais não autorizados;
  - Autorizar transacções fraudulentas ou para confirma-las;
- Negar a responsabilidade para informação que o intruso mesmo criou;
- Clamar que recebeu de um outro usuário a informação que o intruso criou;
- Dizer que enviou uma mensagem para um outro usuário a uma dada hora, informação essa que ele não enviou ou, se enviou, enviou num outro período;
- Clamar que não recebeu a mensagem enquanto recebeu ou indicar uma falsa hora de recepção;
- Tornar mais abrangente a licença dum software do intruso;
- Modificar a licença de outros;
- Ocultar a presença de alguma informação dentro de outra informação;
- Inserir-se no meio duma ligação entre dois usuários, sem ser detectado;
- Ver quem acede a qual informação e quando é que os acessos são efectuados, mesmo que a informação por si só se mantenha oculta;
- Impugnar um protocolo de integridade de informação de revelar informação que o intruso deseja manter secreta;
- Modificar o funcionamento dum software adicionando processos que favoreçam ao intruso;
- Fazer com que outros violem um protocolo introduzindo informação incorrecta;
- Destruir a confidencialidade de um protocolo causando uma aparente falha no sistema;
- Impedir a comunicação entre usuários, em particular, criando uma interferência que dê uma comunicação autorizada como não autorizada;

- Roubar informações confidenciais, para posterior venda a concorrentes ou outros fins;
- Danificar intencionalmente recursos da organização como forma de se vingar de uma represália ou demissão, por si, tida como injusta, e;
- Efectuar transacções ilegais ou acções prejudiciais a organização em nome de terceiros como forma de prejudicar os colegas ou encobrir suas falcatruas.

Um dos factores mais preocupantes na gestão da informação é que os ataques são maioritariamente, cerca de 70%, perpetuados pelo público interno, isto é, por funcionários da Organização [39]. Este público interno, por pertencer a Organização, conhece o SI, a Infra-estrutura de comunicação e, em certos casos as vulnerabilidades dos mecanismos de segurança, o que lhe dá vantagem em relação aos intrusos externos. A Criptografia ajuda, também, a ultrapassar esta dificuldade pois permite a definição de diferentes níveis de segurança, ou por outro lado podem ser definidas várias chaves quanto necessário.

2.3.1. Categorias de ataques

Os ataques ao Sistema de comunicação dum sistema computarizado ou da rede podem ser caracterizados pela *análise do fluxo de dados*, este fluxo pode advir de um ficheiro, usuário ou de uma área da memória para um destino que pode ser outro ficheiro ou usuário. Como se pode ver pela Figura 1, durante a comunicação, numa rede de dados, um fluxo de informação é emitido pelo emissor (origem) para um determinado receptor (destino).

Figura 1 – Fluxo de dados durante uma Comunicação.

Com a implementação das redes de computadores a informação tornou-se tão vulnerável quanto a comunicação por telefone, isto é susceptível a ataques como [16]:

- **Interrupção** ⇨ este ataque está ligado a destruição dum recurso do sistema, podendo ser o corte duma linha de comunicação, danificação propositada de uma peça de hardware, etc., estando por isso ligado a disponibilidade do sistema (veja Figura 2);

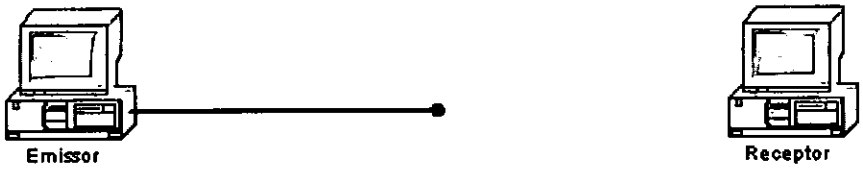


Figura 2 – Interrupção do fluxo de dados durante uma Comunicação.

- **Intercepção** ⇨ um computador, pessoa ou software não autorizado consegue penetrar na segurança da Organização, acedendo assim a qualquer recurso disponível, com o desejo de recolher informação ou programas confidenciais (veja Figura 3);

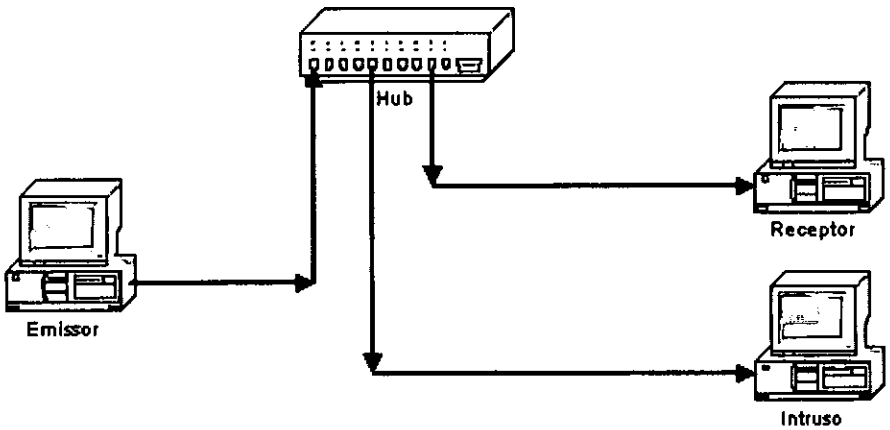


Figura 3 – Intercepção do fluxo de dados durante uma Comunicação.

- **Modificação** ⇨ este ataque esta ligado ao da intercepção, a diferença é que este não apenas recolhe informação como a modifica e se faz passar pelo Emissor, como exemplo disso podemos ter a mudança de informação de um ficheiro, a alteração de um programa para que este execute as suas rotinas de forma diferente favorecendo assim o atacante e desestabilizando o sistema da organização, e até modificar o conteúdo de uma mensagem que esta sendo transmitida na rede, este ataque lesa a integridade do sistema. A Figura 4 ilustra este tipo de ataque, em que no $Tempo_1$ (T_1) o emissor envia uma mensagem ao receptor e esta é interceptada pelo intruso que a modifica e reenvia a mesma no $Tempo_2$ (T_2);

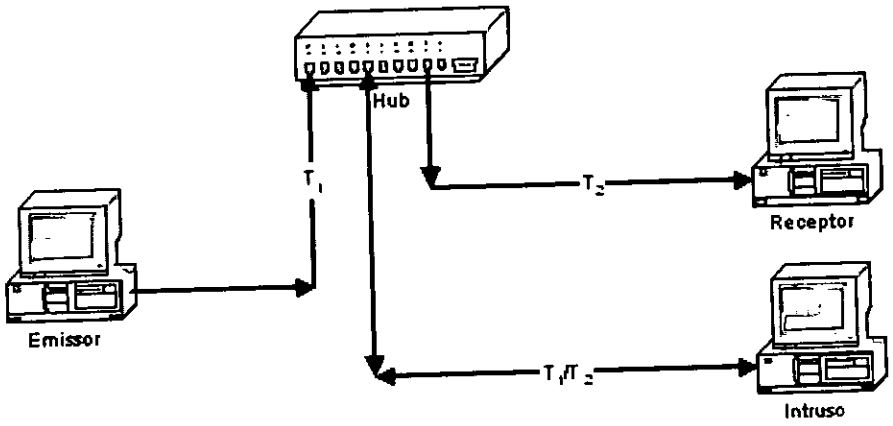


Figura 4 – Modificação do fluxo de dados durante uma Comunicação.

- **Fabricação** ⇨ um elemento não autorizado pode introduzir no sistema objectos prejudiciais ao mesmo, atingindo assim a autenticidade da informação, estes objectos podem ser registos inexistentes, instalar programas maliciosos, como vírus, worms, etc. (veja Figura 5).

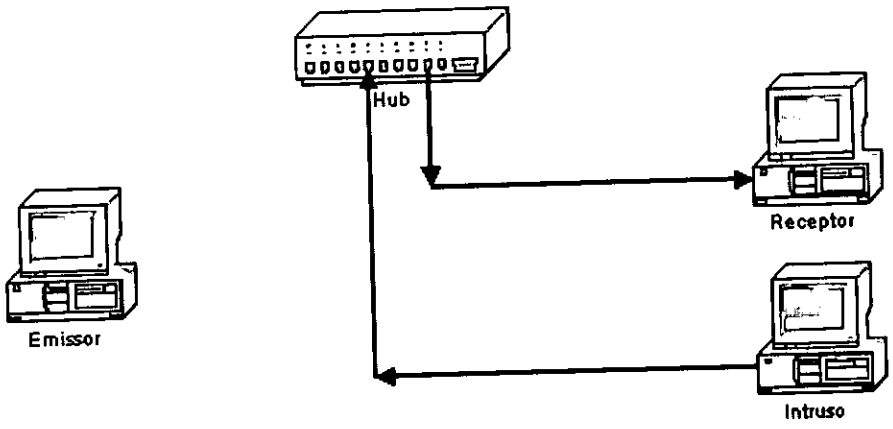


Figura 5 – Fabricação dum fluxo de dados.

2.3.2. Classificação dos ataques

Os ataques atrás descritos podem ser classificados como *passivos* e *activos* dependendo da sua interacção com a informação em circulação.

2.3.2.1. Ataques passivos

Estão relacionados com a auscultação ou monitorização da informação durante a transmissão. O objectivo destes ataques é de obter informação apenas.

Existem duas principais formas de ataques passivos [16]:

- **Captação do conteúdo da mensagem** – este ataque geralmente ocorre durante uma conversa telefónica, uma mensagem de E-mail ou outra forma de troca de informação em que esta possa interessar a terceiros;

- **Análise do fluxo de informação** – suponha que tenhamos uma forma de "mascarar" a informação antes de a transmitir, de modo que mesmo sendo capturada a mensagem, o intruso não consiga ler a informação nela contida, podendo apenas colher características como o padrão da mensagem, quem enviou e para quem enviou, a localização e identidade do *host* da comunicação, a frequência e o tamanho da informação. Este tipo de atributos, inerente nas mensagens, pode ser útil para deduzir a natureza da comunicação.

Os ataques passivos são de difícil detecção, pois eles não envolvem alteração da mensagem. Contudo, é possível prevenir este ataque, por isso para combate-los deve-se pensar na prevenção mais do que na detecção.

2.3.2.2. Ataques activos

Estes ataques consistem, principalmente, na modificação da mensagem e criação duma falsa mensagem, e geralmente caracterizam-se por [16]:

- **Ataque de falsa identidade:** implica a produção ou alteração duma mensagem e respectiva emissão da mesma pelo intruso fazendo-se passar por um outro usuário;
- **Modificação:** implica, como o próprio nome transparece, a alteração da mensagem original com o objectivo de produzir um efeito não autorizado;
- **Retenção:** envolve a captura duma informação e consequente retransmissão da mesma, mas num período conveniente ao intruso, atrasando assim a comunicação;
- **Encerramento dum serviço:** iniba o normal funcionamento dum serviço ou a Gestão do local de comunicações. Este ataque, geralmente, tem um alvo específico. Outra forma de encerrar um serviço é danificar o funcionamento da rede, isto pode ser efectuado destruindo todos ou alguns canais de comunicação ou enchendo a rede de mensagens inúteis de maneira a degradar a *performance* da mesma.

Os ataques activos apresentam características opostas aos passivos. Enquanto que os ataques passivos são difíceis de detectar e existem medidas que impeçam o seu sucesso, os ataques activos são difíceis de prevenir, pois para o fazer seria necessário proteger, permanentemente, todas as infra-estruturas de comunicação e caminhos por onde a informação circula, o que acarretaria custos elevados de instalação e manutenção. Em vez disso, é preferível detectar os ataques e recuperar dos mesmos.

2.4. Modelo de segurança

Depois de identificados os ataques, as Organizações devem decidir o nível de segurança a implementar para uma rede ou sistema e os recursos físicos e lógicos a serem protegidos. Ainda nesta fase, seleccionam-se as ferramentas a usar e quantificam-se os custos associados aos ataques e os dos mecanismos de protecção para minimizar a probabilidade de ocorrência dum ataque [16].

Os aspectos de segurança são implementados quando há necessidade de proteger a informação contra o acesso ilegal ou não autorizado dum intruso que pode apresentar uma ameaça a segurança da Informação [15].

2.4.1. Segurança Lógica

Na segurança lógica onde o elemento a proteger é a informação (no formato electrónico) devem ser definidos mecanismos de segurança que contemplem dois momentos, nomeadamente, o do armazenamento da informação no computador e o da circulação da mesma.

2.4.1.1. Transmissão

Quando uma mensagem está para ser transferida duma origem para um destino através de uma rede, como a *Internet*, as duas partes intervenientes, o emissor e o receptor, devem cooperar para que a troca de informação termine bem sucedida. Um canal lógico de informação é estabelecido pela definição duma rota pela Internet da origem ao destino e pela identificação de protocolos, como o TCP/IP ou similares, pelos dois intervenientes, veja a Figura 6 [16].

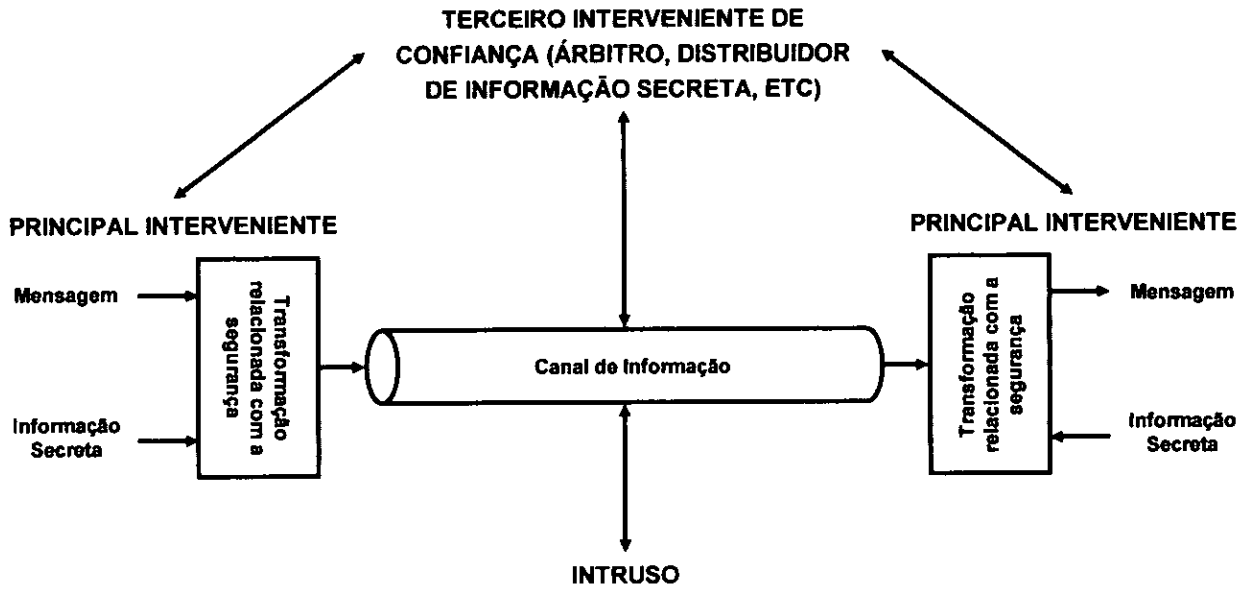


Figura 6 – Modelo de Segurança de Redes [16].

Todos mecanismos de segurança para a transmissão da informação tomam em consideração dois aspectos [16]:

- A segurança relacionada com a transformação da informação a ser enviada. Um exemplo disto é o uso da encriptação da informação, que impede que mesmo tendo acesso a ela o intruso seja incapaz de lê-la e que também pode ser usada para verificar a autenticidade do emissor.
- Uma informação secreta partilhada pelos dois intervenientes que se supõe ser desconhecida pelo intruso. Um exemplo disso é a chave de encriptação usada em conjunto com a transformação para "mascarar" a informação antes do envio e para "desmascarar" a mesma na recepção.

Como se pode ver na Figura 6, pode-se ainda incluir um terceiro interveniente que servirá para garantir a segurança da informação, podendo ser uma entidade que irá distribuir a chave de encriptação aos intervenientes, e poderá, também, arbitrar conflitos entre o emissor e o receptor relativamente a autenticidade da transmissão da informação.

No geral, um modelo de segurança da informação durante a transmissão, consiste em [16]:

- Desenvolver um algoritmo que execute uma transformação complexa suficiente para garantir a segurança;
- Criar uma função para a criação da chave a ser usada com a informação;

- Conceber métodos para a distribuição e partilha da informação secreta e das chaves, e;
- Especificar um protocolo para que dois elementos do sistema façam uso seguro do algoritmo e partilhem seguramente a informação secreta.

2.4.1.2. Armazenamento

Neste nível de segurança, encontra-se a instalação propositada de aplicativos maliciosos que tem a função de identificar e testar as vulnerabilidades do sistema e que podem afectar o funcionamento dos softwares de aplicação e de sistema. Deste género encontramos dois tipos [16]:

- **Ameaça de acesso à informação** – intercepta e modifica dados para um intruso que não deve ter acesso a informação;
- **Ameaça aos serviços** – impede o uso dos computadores pelos legítimos usuários, encerrando os seus aplicativos. Vírus e vermes são exemplos de ataques a softwares. Estes aplicativos são introduzidos no sistema por meios como uma disquete ou mesmo pela rede de dados.

O mecanismo de segurança para o acesso a informação do computador consiste em [12]:

- **Software de guarda**, como um *Firewall*, que inclua um procedimento de acesso através de uma senha que deverá impedir o acesso a todos usuários com excepção para aqueles que possuam autorização e uma outra função para detectar e rejeitar os vírus, vermes, e outros ataques do género.
- **Software de detecção e recuperação**, como um antivírus, para que quando o acesso for conseguido seja por um intruso ou software malicioso este se responsabilize por monitorar a actividade do computador e avaliar a informação armazenada, numa tentativa de detectar a presença destes e defender o computador contra os mesmos;
- **Sistemas Operativos**, como o Windows XP, que possuem:
  - **Controlos internos de acesso** – consiste, basicamente, no uso de senhas para autenticação do usuário;
  - **Protecção de ficheiros** – consiste em definir propriedades dos ficheiros como a proibição a escrita, leitura, modificação ou abertura dos ficheiros;
- **Protocolos de comunicação** – no conhecido protocolo TCP/IP, o IP actualmente em uso na Internet foi projectado para fornecer autenticação, integridade, controle de acesso e confiabilidade na camada de rede, e;

- **Routers** – são usados como filtros de endereços.

2.4.2. Segurança Física

A segurança física da informação aborda questões ligadas a medidas de prevenção tanto contra ataques às Infra-estruturas da Organização, como contra catástrofes naturais. O que pode incluir inundações, incêndios, terramotos, furacões, e outras calamidades naturais que ponham em causa a integridade dos computadores em que estão armazenados os dados. Este tipo de segurança comporta, também, a entrada ilegal dum intruso nas instalações da Organização, como forma de aceder mais facilmente os computadores e a rede à que estes pertencem.

Neste nível de segurança, podem ser usados mecanismos como [12]:

- Contratação de vigilantes (guardas);
- Instalação de câmaras de vigilância;
- Implementação de métodos de controlo de acessos, como:
  - Métodos Biométricos (envolve analises a retina, impressões digitais, etc.);
  - Cartões inteligentes;
- Alarmes contra intrusos e actividades naturais;
- Alarmes contra incêndios;
- Implementação de Sistemas de backup's (cópias de segurança) e redundância;
- Colocação de objectos valiosos em cofres, e;
- Etc.

O tipo de mecanismos a adoptar depende das dimensões de cada Organização e de quanto a mesma pretende gastar com o seu sistema de segurança.

Como se pode concluir, todo o sistema de segurança deve, basicamente, possuir mecanismos de detenção, prevenção e recuperação de ataques. Pelo que se viu acima, estes factores são mais infalíveis em documentos físicos, o que contribui negativamente para a disseminação dos sistemas informatizados, pois esta deficiência fomenta muita desconfiança no seio dos usuários, principalmente em países em vias de desenvolvimento, como é o caso de Moçambique, onde as TIC's são desconhecidas e não estão ao alcance da maior parte da população, devido a factores económicos, e em certos casos sócio-culturais.

2.5. Hacker e Cracker

As violações são genericamente perpetradas pelos chamados *Crackers* que tentam penetrar em sistemas acessados por uma rede de dados. A acção do *Cracker* é maliciosa e é motivada por orgulho, fama, vingança e dinheiro; e pode ser, por exemplo, um empregado desiludido com a organização e que deseja causar danos a mesma, ou até um criminoso que pretende penetrar no sistema com o objectivo de obter ganhos financeiros ou, ainda, para testar a sua capacidade de quebrar sistemas de segurança e entrar em um computador do sistema.

Por outro lado, existem os *Hackers* que apesar se serem muitas vezes confundidos com os *Crackers*, não são maléficos, muito pelo contrário, tentam ajudar a Organização, testando o seu SI em busca de vulnerabilidades ou possíveis falhas e por vezes testam, também, Softwares para detectar possíveis bugs. Uma vez, encontradas estas vulnerabilidades e bugs reportam-nos a Organização ou até ao Público em geral.

A forma recente de ataque à Sistemas é o recurso aos chamados *trojan* (Cavalos-de-Tróia) que são aplicativos que dão acesso ao computador da Organização a um aplicativo-mãe instalado no computador do Hacker, este género de Software permite ao *Hacker* comandar o computador remotamente, podendo ter acesso a todos ficheiros instaurados no computador, a definições do sistema, e podem penetrar o computador através dum E-mail, duma disquete, duma caneta, durante a navegação na Internet, etc. De salientar que, o *trojan* actua escondido, isto é, pode-se trabalhar no computador normalmente sem reparar que alguém esta entrando no mesmo, e por isso este tem ganhado popularidade, o já não é o caso dos vírus que alteram o funcionamento do computador e, assim, é facilmente detectável.

CAPÍTULO III

MEIOS DE TRANSMISSÃO

- Meios Magnéticos
- Par Trançado
- Cabo Coaxial
- Fibras Ópticas
- Transmissão em Linha de Visão
- Satélites de Comunicação

3. MEIOS DE TRANSMISSÃO

Nas Organizações, geralmente, os computadores pertencem à uma LAN. Tipicamente, um usuário pode aceder a outros computadores, servidores, *Host* da LAN ou em outras LAN's do mesmo edifício que estão conectadas com *routers* ou *bridges*. Este é o primeiro ponto de vulnerabilidade, neste caso a maior preocupação é um acto de espionagem por parte dum funcionário. O *wiring closet*, usado para interligar os cabos de Telefone e dados internos, é um ponto muito vulnerável. Se um intruso penetra no armário, pode espiar os fios e ver qual é usado para a transmissão dos dados, após isto, pode ligar um rádio-transmissor de baixa potência. Os sinais resultantes podem ser captados por uma localização próxima, como um carro, um edifício, etc. Por outro lado, o *wiring closet* pode ter uma ligação à uma antena de microondas, ou uma ligação de microondas ponto-por-ponto.

O *wiring closet* pode, também, ter uma ligação a um *packet switching network*, que pode ser uma linha *leased*, uma linha privada directa, ou uma conexão *switched* numa linha de telecomunicação pública como a ISDN. Dentro da rede, os dados passam por muitos nós e *links* até chegar ao destino [16].

Um ataque pode acontecer a qualquer meio de comunicação. Para ataques activos, o intruso precisa de controlo físico, duma porção do *link* e estar possibilitado a introduzir e captar a transmissão. Para um ataque passivo, o intruso precisa apenas de conseguir "observar" a transmissão. O *link* de comunicação pode ser por cabo (par trançado, cabo coaxial, fibra óptica) ou por ondas (microondas ou canais de satélite).

O par trançado e o cabo coaxial podem ser atacados com *invasive taps* e dispositivos indutores que monitoram a emissão electromagnética. *Invasive taps* permitem ataques tanto activos como passivos, e o *inductive taps* são úteis para ataques passivos. Nenhum dos tipos de escuta aplica a fibra óptica, que é uma das grandes vantagens deste meio [16].

A Fibra Óptica não emana ondas electromagnéticas, e por isso não é vulnerável a *inductive tap*. Fisicamente, quebrando o cabo decrementa a qualidade do sinal e por isso é detectável. A comunicação por microondas e satélite pode ser interceptada com pouco risco para o atacante, isto é principalmente efectuável para transmissões que cobrem áreas geograficamente distantes. Ataques activos são fazíveis em microondas e satélite, mas são difíceis e caros.

Como se pode concluir, nenhum meio, por si só, garante uma segurança eficaz o que nos leva a pensar que a Criptografia é a melhor forma de combater a intrusão.

O meio de transmissão é o caminho físico entre o transmissor e o receptor. O propósito da camada física é transportar um fluxo bruto de bits duma máquina para outra. Antes de se efectuar a transmissão deve-se decidir sobre qual dos meios implementar, e esta decisão depende do valor a ser gasto e da tecnologia que pretendemos usar. Vamos agora, analisar os mais frequentes.

3.1. Meios Magnéticos

Esta é uma das formas mais comuns de transportar dados, que consiste em escrevê-los em Canetas (Memória Flash) ou em Discos Flexíveis, e transportar fisicamente, a fita ou os discos até ao computador destino. Embora este método não seja muito sofisticado, é mais eficaz em termos de custos, mas, como é óbvio, é ineficaz em caso de longas distâncias e quando os dados são enviados ou solicitados por uma aplicação. Mas são úteis quando o custo do bit transportado é um factor importante [18].

3.2. Par Trançado

Este é o método mais barato e mais usado nos países em desenvolvimento, como é o caso de Moçambique. Apesar do método anterior ser considerado aceitável, tem o inconveniente de retardar a transmissão dado que a mesma é efectuada em minutos ou horas, e em sistemas *online* a transmissão deve ser feita em milissegundos.

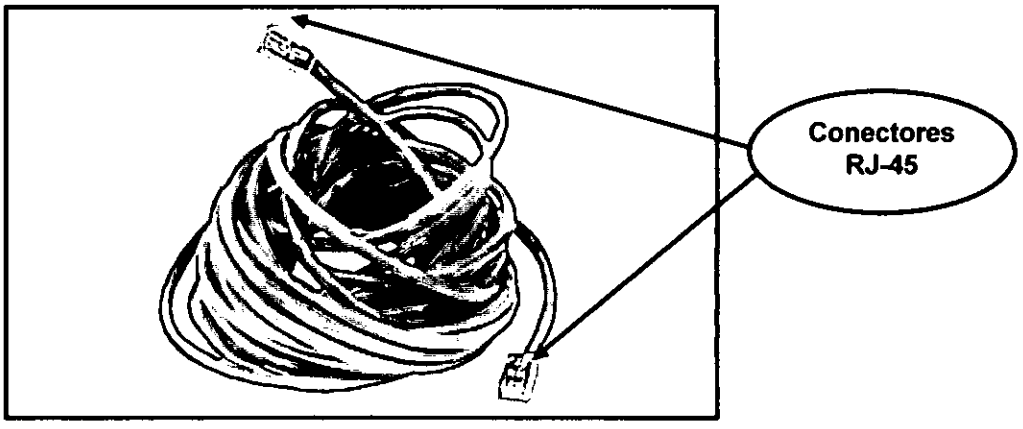


Figura 7 – Par Trançado do tipo UTP [5].

3.2.1. Características

O Par Trançado consiste em dois fios de cobre isolados (ver Figura 7), tipicamente com espessura de 1 mm, trançados entre si de forma helicoidal, como a molécula do ADN.

A forma trançada é usada para reduzir a interferência eléctrica de outros pares similares vizinhos, pois dois fios paralelos formam uma antena enquanto que um par trançado não.

Os pares trançados podem se estender por vários quilómetros sem amplificação, mas para distâncias maiores são necessários *repetidores*. Quando muitos pares trançados se estendem paralelamente, como os fios que saem dum edifício de apartamentos em direcção a central telefónica, eles são agrupados e envoltos em uma bainha protectora.

A taxa de transmissão para locais que se encontram próximos é de 100 Mbps e para longas distâncias é de 4 Mbps ou mais [7].

Os Pares trançados são usados tanto na transmissão digital como analógica. A banda passante depende da espessura do fio e da distância percorrida. Para sinais analógicos, amplificadores são necessários em cada 5 á 6 km. Para sinais digitais, amplificadores são necessários em cada 2 á 3 km.

Comparado a outros meios de comunicação como o cabo coaxial e a fibra óptica, o par trançado é limitado em distância, largura de banda e taxa de transmissão [18].

3.2.2. Aplicações

- Sistema telefónico. Praticamente todos os telefones estão ligados à uma Central Telefónica através de pares trançados;
- São usadas para a construção de LAN's.

3.2.3. Vantagens

- Possui um bom desempenho;
- É geralmente barato.

3.2.4. Desvantagens

- O par trançado é susceptível a interferências e ruídos pois emana ondas electromagnéticas.

3.3. Cabo Coaxial

Também denominado por *Coax*. Existem dois tipos de cabo coaxial, nomeadamente:

- **Cabo Coaxial de Banda Básica** – é um cabo de 50 ohms usado para a transmissão digital;

- **Cabo Coaxial de Banda Larga** – é um cabo de 75 ohms usado para a transmissão analógica.

3.3.1. Características

Um cabo coaxial consiste em um fio de cobre rígido que forma o núcleo, envolto por um material isolante que, por sua vez, é envolto em um condutor cilíndrico, frequentemente na forma de uma malha cilíndrica entrelaçada. O condutor externo é coberto por uma placa plástica protectora, veja a Figura 8.

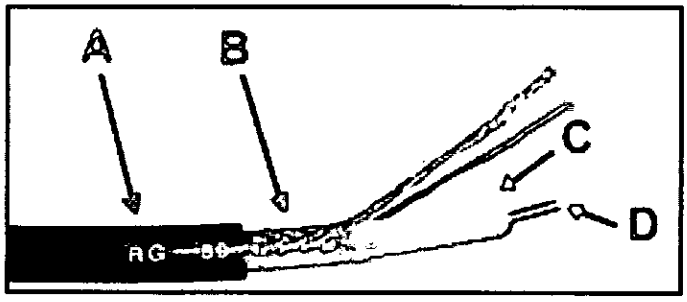


Figura 8 – Cabo Coaxial [5].

A - Revestimento de plástico;

B - Tela de cobre;

C - Isolador dieléctrico interno;

D - Núcleo de cobre.

A forma de construção do cabo coaxial lhe dá boa combinação de alta banda passante. A banda passante possível depende do comprimento do cabo, para cabos de 1 Km pode-se obter uma taxa de 10 Mbps. Taxas de dados mais altas são possíveis em cabos mais curtos. Pode-se usar cabos mais longos, mas as taxas serão mais baixas [18].

Pode ser usado para longas distâncias e suporta mais estações numa linha partilhada que o par trançado.

Usando o Multiplexador Divisor de Frequência podem-se transmitir mais e 10.000 canais de voz simultaneamente.

Existem duas formas de ligar computadores usando um cabo coaxial, nomeadamente [18]:

1. Cortar completamente o cabo e inserir um conector T, que além de reconectar o cabo, provê também uma terceira saída que leva ao computador.
2. Usar uma presa-vampiro (vampire-tap), que é um furo de profundidade e diâmetro extremamente precisos, terminando exactamente no núcleo do cabo.

Nesse furo é inserido um conector especial que alcança o mesmo objectivo que o conector T, mas sem seccionar o cabo em dois.

Quanto as vantagens e desvantagens de cada um os métodos, usar o conector T significa interromper o cabo por alguns instantes, o que para alguns sistemas de Informação é impensável, devido ao grande volume de dados que processam. Além disso, quanto mais conectores existirem na rede maior será a probabilidade de ocorrer problemas intermitentes. As presas-vampiro não têm nenhum destes problemas, mas devem ser instaladas muito cuidadosamente. Se o furo for feito profundo demais, há o risco de seccionar o núcleo em dois pedaços desconectados. Por outro lado, se o furo não for profundo o suficiente a conexão poderá dar origem a erros intermitentes. Os cabos usados para presas-vampiro são mais grossos e mais caros que os cabos usados com os conectores T [18].

3.3.2. Aplicações

- Distribuição Televisiva;
- Transmissões Telefónicas de longa distância, e;
- São usadas para a construção de LAN's.

3.3.3. Vantagens

- Excelente imunidade a ruídos;
- É Barato.

3.3.4. Desvantagens

- A instalação dos conectores é geralmente uma tarefa um bocado complexa, sendo, muitas vezes, responsável pela ocorrência de erros.

3.3.5. Diferença entre a Banda Larga e Básica

A Banda Básica é simples e de instalação barata, e requer interfaces baratas. Ela oferece um único canal digital com taxas de dados de cerca de 10 Mbps sobre uma distância de 1 Km. Para a maioria das aplicações a banda básica é adequada. Por outro lado, a banda larga requer engenheiros com experiência em instalação de rádio para planejar o *layout* dos cabos e dos amplificadores e instalar o sistema. Também é necessário pessoal qualificado para manter o sistema e sintonizar os amplificadores periodicamente durante o seu uso. As interfaces da banda larga também são mais caras do que as adequadas para banda básica [18].

No entanto, a banda larga oferece múltiplos canais (embora normalmente limitados a 3 Mbps cada um) e podem transmitir dados, voz e televisão no mesmo cabo – por dezenas de quilómetros, se necessário. Para maior parte das aplicações, a banda passante adicional da banda larga não justifica o seu custo e complexidade, assim a banda básica tem utilização mais ampla.

É usado para transmitir tanto sinais analógicos como digitais. E é menos susceptível a interferência e cruzamento que os pares trançados.

Para a transmissão a longas distâncias do sinal analógico é necessário o uso de amplificadores, em cada poucos quilómetros, com menor espaçamento se são usadas frequências maiores. Para transmissão de sinais digitais, *repetidores* são necessários em cada quilómetro, com menor espaçamento para taxas altas [7].

3.4. Fibras Ópticas

Este método consiste em transmitir dados através da luz. Um pulso de luz pode ser usado para sinalizar um bit 1 e a ausência deste, sinaliza um bit 0. A luz visível tem uma frequência de cerca 10^8 MHz, dessa forma, a banda passante no sistema de transmissão óptica é potencialmente enorme [18].

3.4.1. Características

Uma fibra óptica é um cabo fino (2 a 125 μm) e flexível, capaz de conduzir um raio óptico (ver Figura 9). Na Figura 9, vemos a constituição duma Fibra Óptica e a direcção da luz na fibra Multimodal e Unimodal.

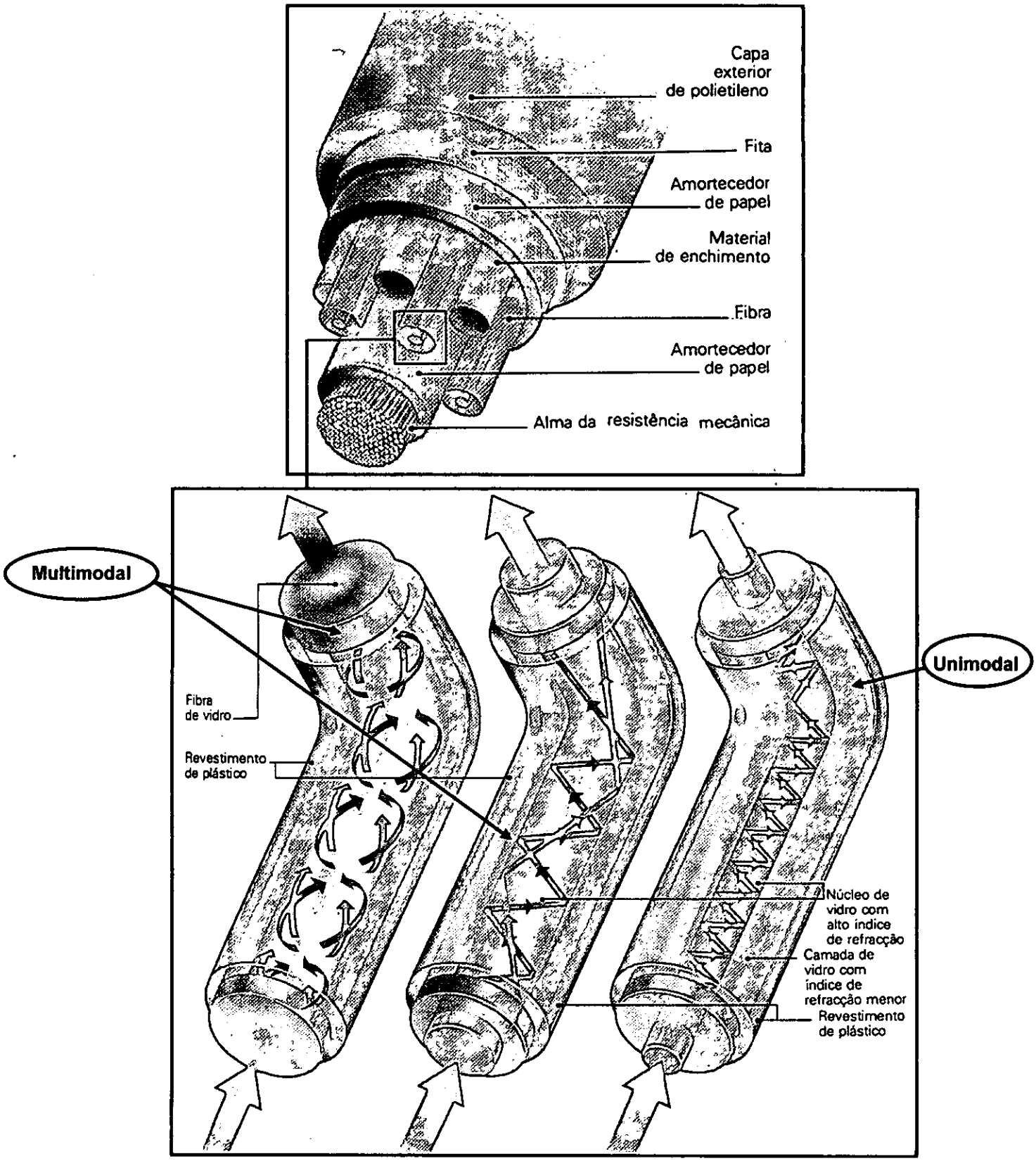


Figura 9 – Fibra Óptica (Multimodal e Unimodal) [8].

Um sistema de transmissão óptica possui três componentes, nomeadamente [18]:

- **Meio de transmissão** é uma fibra ultrafina de vidro ou de sílica fundida;
- **Fonte de luz** é um LED (Ligth Emiting Diode) ou um díodo a Laser, ambos capazes de emitir pulsos de luz quando submetidos a uma corrente eléctrica, e;
- **Detector** é um fotodiodo, que gera um pulso eléctrico quando iluminado por um feixe de luz.

Acoplando-se um LED ou um díodo a Laser a uma das extremidades de uma fibra óptica e um fotodiodo à outra extremidade, temos um sistema de transmissão de dados unidireccional, que aceita um sinal eléctrico, o converte e transmite através de pulsos de luz, e então reconverte a saída em um sinal eléctrico no lado do receptor.

Esse sistema de transmissão vazaria a luz e seria imprestável se não fosse por um princípio da física. Quando um raio de luz passa dum meio para outro, por exemplo da sílica fundida para o ar, o raio é retractado na fronteira da sílica com o ar. Deste modo, se um raio de luz incidir na fronteira com um ângulo α_1 e emergir com um ângulo β_1. A quantidade da refracção depende das propriedades dos meios (em particular os seus índices de refracção). Para os ângulos de incidência acima dum certo valor crítico, a luz é refractada de volta para dentro da sílica, de maneira que, nada escapa para o ar [18].

Assim, um raio de luz que incide em um ângulo pelo menos igual ao ângulo crítico é aprisionado dentro da fibra, como mostra a Figura 9, e pode-se propagar por quilómetros, virtualmente sem perdas. O esboço da Figura 9 mostra apenas um raio aprisionado mas, como qualquer raio incidente na fronteira acima do ângulo crítico será reflectido internamente, muitos raios diferentes estarão ricocheteando lá dentro em ângulos diferentes. Esta fibra é denominada *Multimodal*. No entanto, se o diâmetro da fibra for reduzido a um comprimento de onda de luz, a fibra funciona como um guia de onda, e a luz se propaga em linha recta, sem ricochetear, resultando em uma Fibra *Unimodal*. Para activar as Fibras Unimodais usam-se os díodos a Laser, que são caros, em vez dos LED's, que são baratos, mas que são mais eficientes e podem percorrer distâncias maiores. Contudo, o uso das Fibras Multimodais conduz a perda de alguma luz e o sinal chega com distorção, enquanto que às Unimodais quase não se perde luz.

Os sistemas de Fibra óptica conseguem transmitir dados acima de 1000 Mbps por 1 Km. Lasers potentes podem activar uma fibra de 100 Km de comprimentos sem *repetidores*, embora a velocidades muito inferiores [18].

Também se pode construir uma LAN, usando para tal as fibras, apesar de a tecnologia ser mais complexa. O problema básico é que, muito embora as presas-vampiro possam ser feitas em LAN's de fibra, fundindo-se a fibra proveniente do computador com fibra da LAN, o processo de fabricação do conector é complicado e há uma perda substancial de luz.

A interface de cada computador passa adiante do fluxo de pulsos de luz no próximo elo, e também serve como conector T para permitir ao computador enviar e receber mensagens.

Para se tentar contornar o problema da conexão, usam-se duas interfaces. Uma interface **passiva** consiste em dois conectores fundidos na fibra principal. Um conector possui um LED ou díodo Laser na sua extremidade (para transmissão), e o outro possui um fotodíodo (para recepção). O conector propriamente dito é completamente passivo e, dessa forma, altamente confiável, visto que um LED ou fotodíodo quebrado não interrompe a rede, apenas coloca um computador *offline*. O outro tipo de interface é o repetidor **activo**. A luz incidente é convertida em um sinal eléctrico, regenerado à potência plena caso tenha sido enfraquecido, e retransmitido na forma de luz. A interface com o computador é um fio de cobre ordinário que chega no regenerador do sinal. Se um repetidor activo falha, o anel é seccionado e a rede é derrubada. Por outro lado, visto que o sinal é regenerado em cada interface, os elos individuais computador a computador podem comprimento de quilómetros, com o tamanho total do anel virtualmente sem limite. As interfaces passivas perdem luz em cada junção e, assim, o número total de computadores e o comprimento total são bastantes limitados [18].

Uma topologia em anel não é a única forma de se construir uma LAN usando fibras ópticas. Também é possível usando a estrela passiva. Nesta topologia, cada interface possui uma fibra indo do seu transmissor até um cilindro de sílica, com todas as fibras que chegam sendo fundidas em uma das extremidades do cilindro. Similarmente, as fibras fundidas à outra extremidade do cilindro levam de volta a cada um dos receptores. Sempre que uma interface emite um pulso de luz, ele é difundido no interior da estrela passiva, iluminando todos receptores e assim obtendo a difusão. Efectivamente, a estrela passiva efectua um OU booleano de todos sinais que chegam

e transmite o resultado em todas linhas de saída. Dado que a energia que chega é dividida entre todas as linhas que saem, o número de nós na rede é limitado pela sensibilidade dos fotodíodos [18].

É instrutivo comparar-se o cabo coaxial com as fibras ópticas. A fibra oferece uma banda passante extremamente grande com pouca perda de potência; assim pode-se estender por grandes distâncias entre *repetidores*.

As seguintes características distinguem a fibra óptica dos pares trançados ou do cabo coaxial [7]:

- **Maior capacidade:** A potencial largura de banda, e consequentemente a taxa de transmissão, da fibra óptica é imensa, taxas de transmissão de 2 Gbps em dezenas de quilómetros são facilmente alcançados. Comparando esta capacidade com as centenas de Mbps em cerca de 1 Km do cabo coaxial e por apenas uns poucos Mbps por 1 Km ou até 100 Mbps por poucas dezenas de metros para o par trançado.
- **Menor tamanho e menor peso:** Fibras ópticas são consideravelmente mais finas que o cabo coaxial ou o cabo agrupado de pares trançados.
- **Isolação electromagnética:** Sistemas de Fibras ópticas não são afectados por campos electromagnéticos externos e não é vulnerável a interferência, ruído do impulso, cruzamento de linhas. Pela mesma razão, fibras não irradiam energia, causando, assim, pouca interferência com outro equipamento e assim providenciando um alto nível de segurança contra a espionagem. De salientar que, as fibras são difíceis de espiar, pois qualquer tentativa pode resultar na quebra do cabo, o que diminui o sinal e leva a detecção da acção.
- **Maior espaçamento para o repetidor:** Poucos repetidores significam menos custos e menos origens de erros. Está é uma das grandes vantagens das Fibras Ópticas, pois pode-se chegar a centenas de quilómetros sem o uso do repetidor, enquanto que o par trançado e o cabo coaxial necessitam do repetidor a cada poucos quilómetros.
- **Operam num intervalo de 10^{14} ou 10^{15} Hz.**

3.4.2. Aplicações

- São usadas para comunicação a longa distância e para aplicações militares, devido a grande segurança que oferece;
- São usadas para a construção de LAN'S.

3.4.3. Vantagens

- Não são afectadas por picos em linhas de força, interferência electromagnética ou materiais químicos corrosivos presentes no ar e, assim podem ser usadas em ambientes fabris agressivos, impróprios para os cabos coaxiais;
- Por serem finas permitem que, companhias com milhares de cabos e condutas de cabos inchadas, possam estruturar melhor a sua cablagem;
- São difíceis de seccionar e mais ainda de conectar, o que representa uma maior segurança visto que a fibra não irradia e os intrusos têm dificuldades para se conectarem.

3.4.4. Desvantagens

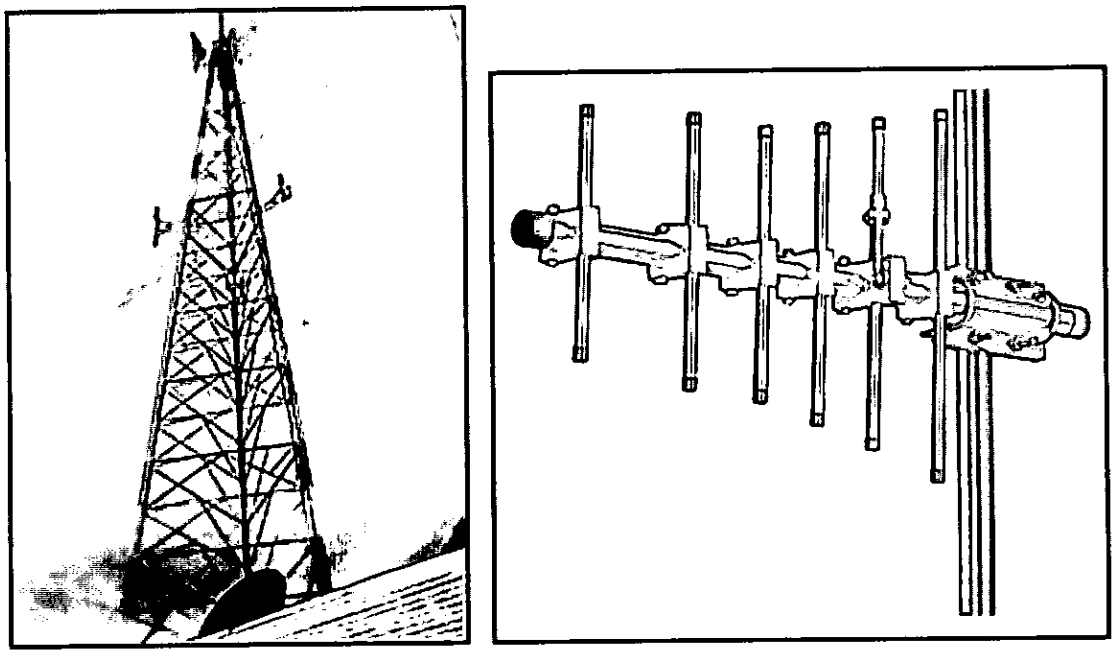
- As interfaces são muito mais caras do que as interfaces eléctricas e a sua montagem é complexa;
- A tecnologia empregue requer aptidões que a maioria dos engenheiros não possui.

3.5. Transmissão em Linha de Visão

As antenas usadas neste tipo de comunicação podem ser as parabólicas em "Prato", que possuem um diâmetro de 10 pés. As antenas são instaladas à uma altura substancial de modo a estenderem a seu área de cobertura e ultrapassarem possíveis obstáculos (ver Figura 10) [18].

3.5.1. Características

As microondas requerem muito menos *repetidores* ou amplificadores que o cabo coaxial e o par trançado numa mesma distância. Os repetidores são colocados a distâncias de 10 à 100 Km [18].



(a) (b)

Figura 10 – Antenas: (a) Transmissão; (b) Recepção [5].

Embora muitos dos sistemas de comunicação de dados usem fios de cobre ou fibra, outros simplesmente enviam os dados pelo ar. Em particular, a transmissão por raios infravermelhos, lasers, microondas e rádio não requerem meios físicos.

Um aplicação comum para qual estender um cabo ou fibra é frequentemente indesejável é uma LAN que atravessa vários prédios num campus universitário, em um parque industrial ou um Complexo Fabril. Neste caso, o mais viável é instalar um transmissor e um receptor a laser ou infravermelho no telhado de cada prédio é barato, fácil de fazer e totalmente legal. A LAN em cada prédio é ligada à linha principal através dum *gateaway*. A comunicação a laser ou infravermelhos é totalmente digital e altamente direccional, tornando-a praticamente imune a grampos ou interferências [18].

Para comunicação a longa distância, a transmissão da rádio em frequência de microondas é uma alternativa aos cabos coaxiais e bastante usada. Antenas parabólicas podem ser montadas em torres, a fim de transmitir para outras antenas a dezenas de quilómetros de distância. Quanto mais alta a antena, maior o alcance. Com torres de 100 metros de altura, são viáveis distâncias de 100 Km entre elas.

Por outro lado, os sinais de antena podem se dividir e se propagar por caminhos ligeiramente diferentes até a antena receptora. Quando esses sinais fora da fase se recombinam, criam interferências, reduzindo a potência do sinal. A propagação de microondas também é afectada por tempestades e por outros fenómenos atmosféricos.

A maior parte das transmissões em microondas ocorre em frequências entre 2 e 4 GHz, correspondendo a comprimentos de onda entre 15 e 0,75 cm. Essas frequências foram divididas em bandas para uso pelas operadoras, pelo Governo, pelas Forças Armadas e outros. A maior parte do tráfego telefónico de longa distância ocorre na faixa dos 4 aos 6 GHz, embora essa faixa esteja ficando cada vez mais superlotada. Frequências mais altas estão disponíveis, mas são menos úteis para tráfego de longa distância, visto que a atenuação é maior nas frequências mais altas [7].

3.5.2. Aplicações

- É amplamente usado, tanto para transmissão telefónica quanto para transmissão televisiva;
- São usadas para a construção de LAN's.

3.5.3. Vantagens

- Por vezes é mais viável e barato construir duas torres que cavar uma trincheira de 100 Km, colocar nela o cabo ou a fibra e fechá-la de novo;
- Nas microondas não existem custos de manutenção do equipamento, como *repetidores*, e dos cabos que podem romper-se por uma série de motivos;
- As microondas permitem uma deslocação mais cómoda e flexível dos terminais.

3.5.4. Desvantagens

- Com o crescimento das microondas aumenta a probabilidade de haver interferência;
- Chuvas e neblinas podem interferir com a comunicação, dependendo do comprimento de onda escolhido.

3.6. Satélites de Comunicação

Uma comunicação por satélite é uma estação de revezamento de microondas. É usado para ligar dois ou mais transmissores/receptores de microondas terrestres. O satélite recebe a transmissão em uma frequência, amplifica ou repete o sinal, e o transmite em outra frequência (ver Figura 11). Um único satélite em órbita irá operar num número de frequências denominados canais *transponders* [18].

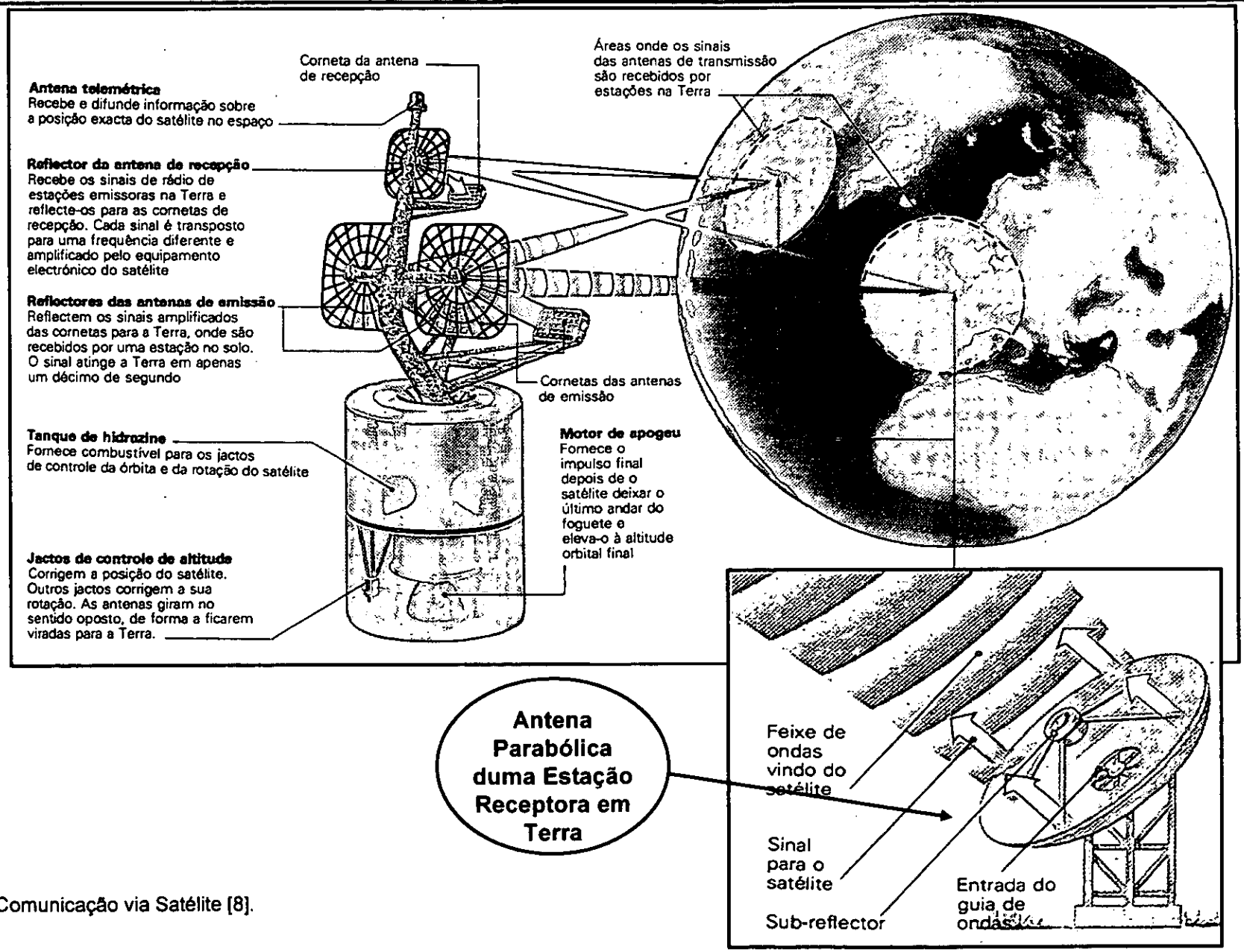


Figura 11 – Comunicação via Satélite [8].

3.6.1. Características

O satélite pode dividir a capacidade total em um número de canais e alugar esses canais para propósitos individuais. Um usuário equipado com antenas num número de sítios pode usar o canal dum satélite para uma rede privada. A frequência óptima para uma transmissão por satélite é de 1 até 10 GHz. Abaixo de 1 GHz haverá um significante ruído de origens naturais, incluindo galáctica, solar, ruído atmosférico, interferência Humana de vários objectos electrónicos. Acima dos 10 GHz, o sinal é muito atenuado pela absorção e precipitação atmosférica [18].

A comunicação por satélite possui três propriedades que a distingue das outras, nomeadamente:

- Devido as grandes distâncias envolvidas, há um atraso na propagação de cerca de um quarto dum segundo entre a transmissão duma estação terrestre e a recepção por outra. Este atraso é notável nas conversações telefónicas;
- As microondas de satélite estão inerentes numa instalação de transmissão. Muitas estações podem transmitir para o satélite, e uma transmissão do satélite pode ser recebida por muitas estações;
- A difusão por satélite, isto é, todas estações debaixo do feixe descendente podem receber a transmissão, incluindo estações piratas desconhecidas pela operadora. As implicações para a privacidade são óbvias.

Pode-se pensar em um Satélite de Comunicação como se fosse um grande *repetidor* de microondas no céu. Ele contém um ou mais *transponders*, cada qual escutando uma parte do espectro, amplificando o sinal de entrada e retransmitindo em outra frequência, para evitar interferência com o sinal de entrada. Os feixes de transmissão podem ser bastantes amplos, iluminando uma parte substancial da superfície terrestre, ou estreitos, iluminando áreas com diâmetro de centenas de quilómetros.

De acordo com a 3ª Lei de Kepler [33]:

> *"Os Quadrados dos períodos de revolução dos planetas são proporcionais aos cubos dos raios das suas órbitas."*

Deste modo, o período orbital de um satélite varia conforme o raio da órbita elevado à potência 3/2. Perto da superfície da Terra, o período é de aproximadamente de 90 minutos. Os satélites de comunicação a essas baixas altitudes não são úteis, pois ficam visíveis pelas estações terrestres por um intervalo de tempo curto demais. No entanto, a uma altitude de aproximadamente 36.000 Km acima do equador, o período

do satélite é de 24 horas; assim, ele gira aproximadamente à mesma velocidade da Terra abaixo dele. Fazendo com que um satélite fique fixo no céu é altamente desejável, pois de outra forma seria necessária uma antena direccionável, que é cara, para mantê-lo em sintonia [18].

A Figura 11 ilustra um satélite com duas antenas, correspondendo a duas áreas espaçadas geograficamente entre si. As duas estações dentro de cada área se revezam na transmissão para o satélite. Os números dentro dos feixes ascendentes indicam o destinatário desejado da mensagem. A medida que as mensagens chegam, elas são comutadas para a antena apropriada e enviadas para baixo. A Figura 11 mostra a retransmissão das mensagens enviadas para cima. Como se pode ver, a Antena Parabólica possui um prato que é feito de painéis de aço ou alumínio, e o seu azimute e elevação, bem como o ângulo do pequeno sub-reflector montado sobre ele é ajustável, de modo a manter a antena constantemente apontada para o Satélite. O sinal é reflectido para um Guia de Ondas que o conduz a um edifício que fica sob a antena, no qual esta instalado equipamento para modulação e amplificação dos sinais para o Satélite, além das ligações à rede de comunicações terrestres para eventual difusão da informação recebida [8].

Os satélites de comunicação possuem várias propriedades que são radicalmente diferentes dos elos terrestres ponto a ponto. Um deles é o **tempo de retardo** introduzido pela grande distância de ida e volta, apesar de que os sinais de e para o satélite viajarem a velocidade da luz (300.000 Km/s). Dependendo da distância do usuário até a estação terrestre e da elevação do satélite acima do horizonte, o tempo de trânsito está entre 250 e 300 ms. Os elos terrestres de microondas possuem um retardo de propagação de aproximadamente 3 ms/Km, e os elos em cabos coaxiais têm um de 5 ms/Km. Resumindo, os elos de satélite têm um retardo maior que os terrestres.

Uma outra diferença entre os elos terrestres e os de satélite é a banda passante disponível. A linha telefónica de considerável velocidade é de 1,544 Mbps. A transmissão por satélite telhado a telhado evita completamente o sistema telefónico e oferece potencialmente taxas de dados 1000 vezes mais altas [7].

Ainda que uma fibra óptica tenha, em princípio, maior banda passante em potencial do que todos satélites jamais construídos, essa banda passante não está disponível para a maior parte dos usuários, pois elas são partilhadas por outros serviços como o

sistema telefónico, por exemplo. Com o satélite é viável um usuário montar uma antena no telhado do seu prédio e evitar essa partilha do canal de transmissão [14].

3.6.2. Aplicações

- Distribuição televisiva;
- Transmissões telefónicas de longa distância;
- Redes privadas de negócio.

3.6.3. Vantagens

- Os custos de transmissão de uma mensagem são independentes da distância percorrida;
- Possui uma maior banda passante, em relação aos outros meios, e não há partilha do canal de comunicação como é o caso da fibra óptica.

3.6.4. Desvantagens

- Não se pode ter satélites muito próximos entre si, o que condiciona o espaço orbital da Terra;
- A chuva é um factor problemático, pois a água absorve as microondas de frequências mais altas;
- O equipamento para este tipo de comunicação é extremamente caro e é necessário pessoal especializado para opera-lo.

CAPÍTULO IV

CRIPTOGRAFIA

- Evolução da Criptografia
- Vantagens e Limitações do uso da Criptografia
- Tipos e Classificação de Sistemas Criptográficos
- Criptoanálise
- Criptografia Convencional
- Criptografia da Chave Pública
- Técnicas Clássicas e Modernas de Encriptação Convencional

4. CRIPTOGRAFIA

Desde sempre que o Homem sentiu necessidade de ocultar a sua informação importante, mesmo estando esta na posse dum intruso, visto que é quase impossível garantir uma segurança física eficaz, o que se agrava, durante o envio da mesma. A única forma capaz de resolver este problema é o uso de códigos que consiste em cifrar a mensagem antes de transmiti-la, de modo que mesmo tendo acesso a mensagem, um intruso não seja capaz de ler o seu conteúdo, este método ficou conhecido como *Criptografia*. A palavra Criptografia tem a sua origem no Grego *Kryptos* que significa oculto, envolto, secreto; *Graphos* significa escrever, grafar. Portanto Criptografia significa *escrita secreta* ou *escrita oculta* [25].

A criptografia, como ciência, comporta dois processos distintos, o da cifragem e o da decifragem da informação, usando, para isso, um sistema composto por *algoritmos* e *chaves*. Uma chave é *uma informação que permite ao remetente e o destinatário encriptar e decriptar um texto*, enquanto que o algoritmo é um *conjunto de operações ou procedimentos que têm como finalidade transformar o texto original num cifrado*.

O sucesso de um sistema criptográfico depende, única e exclusivamente, de se manter a chave secreta, pois o algoritmo pode ser conhecido mas sem a chave é impossível decifrar uma informação.

Antigamente os sistemas criptográficos baseavam-se apenas num algoritmo, com o aparecimento da criptoanálise, esse conceito foi revisto e começou-se a elaborar algoritmos mais complexos que incluíam, no sistema, as chaves e respectivas funções de geração das mesmas para permitir uma maior segurança. O grande problema do uso das chaves é que para garantir a segurança o ideal seria usar uma chave de tamanho considerável de modo que mesmo usando a Força-Bruta seriam necessários triliões de anos para percorrer todas as combinações possíveis, a contrapartida em se usar esta técnica é o facto de que *quanto maior a chave mais tempo é necessário para encriptar ou decriptar a informação* tornando, assim, o sistema lento. A solução foi criar métodos de codificação das chaves mais eficazes, partindo do princípio de que o algoritmo é conhecido [1].

4.1. Evolução da Criptografia

A criptologia é uma ciência que esteve sempre presente na História do Homem, pois este sempre teve necessidade de manter uma informação confidencial, esconder fórmulas secretas e outros, que não podiam cair em mãos estranhas. Daí que o desenvolvimento da criptografia esteve sempre dependente da evolução Humana, seus feitos e descobrimentos, tendo sido usada tanto por militares como por civis.

Vamos agora acompanhar a evolução da Criptografia de acordo com os grandes períodos Históricos do Homem.

4.1.1. Antiguidade ou Idade Antiga

O primeiro exemplo de criptografia, deu-se em aproximadamente **1900 a.C.**, numa vila de nome Menet perto do Rio Nilo, um escrivão Egípcio que tinha a função de documentar os monumentos construídos pelo seu patrão o arquitecto Khnumhotep, teve a ideia de substituir algumas palavras por outras não padronizadas. A intenção dele é que mesmo na posse do documento um ladrão não conseguiria achar o caminho que o levaria ao tesouro [27].

Em **1500 a.C.**, a criptografia da Mesopotâmia ultrapassou a Egípcia, um dos primeiros registos do uso de Sistemas criptográficos esta numa fórmula para fazer esmalte para cerâmica. A tablete que contêm a formula tem apenas cerca de 8 cm x 5 cm e foi achada às margens do Rio Tigre. Nesta época, mercadores assírios usavam *intaglios*, que são peças planas de pedra com símbolos entalhados para sua identificação. Este processo pode ser comparado as assinaturas digitais.

Esta foi também a época em que a Esteganografia foi desenvolvida pelos povos do Egipto, China, Índia e da Mesopotâmia que consistia em [32]:

- **Tatuagem com mensagens na cabeça de escravos**, a única desvantagem é que tinha que se esperar que o cabelo crescesse. De salientar, que a decriptação era feita no Barbeiro;
- **Marcas na madeira de placas de cera**, as marcas eram escondidas com cera nova. Para decifrar bastava derreter a cera;
- **Mensagens dentro do estômago de humanos e animais de caça**.

Entre **600** e **500 a.C.,** escribas Hebreus, escrevendo o Livro de Jeremias, usaram a Cifra de Substituição simples pelo alfabeto reverso conhecida como ATBASH. Jeremias começou a ditar Barush em 605 a.C., mas os capítulos contendo esses bits

de cifras são atribuídos a uma origem chamada "C", que não era Barush, que pode ser um editor escrevendo após o exílio de Babilónia em 587 AC. As cifras mais conhecidas da época são o ATBASH, o ALBAM e o ATBAH e ficaram conhecidas como as *cifras Hebraicas*.

No **Século IV a.C.**, foram encontrados textos gregos antigos de Enéas de Stymphalus, o Táctico, um cientista militar e criptográfico grego; de Políbio e outros onde descreviam vários métodos de ocultar mensagens. Um desses métodos era o Relógio de Água que era um sistema óptico de comunicação semelhante ao telégrafo, inventado por Enéas. Os Relógios de Água são sistemas de comunicação a distância. Cada integrante do sistema possuía jarros exactamente iguais contendo a mesma quantidade de água. Todos os jarros possuíam um furo de diâmetro idêntico, que ficava fechado. Dentro do jarro havia um bastão com diversas mensagens inscritas. Quando um dos integrantes queria fazer contacto com o outro, fazia um sinal de fogo. Quando o outro respondia, ambos abriam simultaneamente o buraco do jarro. Com a ajuda dum segundo sinal de fogo, ambos fechavam o orifício simultaneamente. Desta forma, a superfície da água do jarro apontava para a mensagem desejada [32].

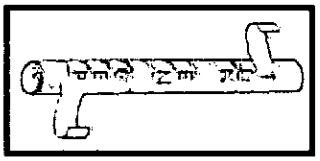


Figura 12 – Bastão de Licurgo [32].

Em **487 a.C.**, Tuídides faz uso, sobre ordens entregues ao príncipe e general espartano Pasanius em 475 a.C., através do que poderia ser o sistema de criptografia militar mais antigo, o scytale ou Bastão de Licurgo (ver Figura 12). Como um dispositivo para esconder mensagens, o scytale consiste num bastão de madeira ao redor do qual se enrola firmemente uma tira de couro ou pergaminho, longo e estreita. Escreve-se a mensagem no sentido do comprimento do bastão, a tira é desenrolada e contêm a cifra. De realçar que, foi escrito um artigo sobre a criptografia em Julho de 1998 intitulado "O Mito do Scytale", onde pressupõe que o uso do Scytale na criptografia é apenas um mito.

Entre **300 a.C.**, Artha-Sastra, um livro atribuído a Kautilya, foi escrito na índia. Neste livro constavam várias cifras criptográficas e recomenda uma variedade de métodos de criptoanálise para obter relatórios de espionagem.

Em **50 a.C.**, Júlio César (100 - 44 a.C.) usou a sua famosa cifra de substituição para cifrar mensagens governamentais. Para produzir a cifra, César alterou as letras deslocando três posições, A se tornava D, B se tornava E, e assim por diante. Por vezes César reforçava o seu algoritmo substituindo letras latinas por gregas. O algoritmo de César era menos forte que ATBASH, mas para um tempo em que poucas pessoas sabiam ler era suficiente.

Em **200**, o Papiro de Leiden, que possuía receitas de poções especiais, possuía texto cifrado nos trechos cruciais das receitas [9].

Em **400**, o Kama Sutra de Vatsayana, classifica a criptografia como a 44ª e 45ª das 64 artes que as pessoas deveriam conhecer e praticar, nomeadamente [32]:

- A arte de saber escrever em Cifras e de escrever palavras de uma forma peculiar;
- A arte de falar mudando as formas das palavras (seria criptofónia). O que pode ser feito de muitas formas, algumas mudando o inicio e o fim das palavras, outras adicionando letras desnecessárias entre todas sílabas duma palavra, e assim por diante.

4.1.2. Idade Média

De **718** à **789**, Al-Khalil, cujo nome completo era Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al-Yahmadi, escreveu o livro *Kitab al Mu'amma* "O Livro das mensagens criptográficas" sobre criptografia, em grego, para o imperador bizantino. Este livro infelizmente perdeu-se. Ele decifrou um antigo criptograma bizantino. Sua solução baseava-se no início do texto original, que ele supôs, correctamente, como sendo "Em Nome de Deus". Este método tornou-se numa referência, tendo sido usado na decifração de mensagens Enigma durante a Segunda Guerra Mundial, e ficou conhecido como o método da palavra provável.

Entre **801** e **873**, Al-Kindi, cujo nome completo era Abu Yusuf Yakub ibn Is-haq ibn as Sabbah ibn 'omran ibn Ismail Al-Kindi, escreveu *Risalah fi Istikhraj al Mu'amma* "Escritos sobre a decifração de mensagens criptográficas". Este livro ainda existe, sendo considerado o mais antigo sobre a criptografia. Nele constam ainda algumas análises de frequência.

Em **855**, Abu Bakr Ahmad bem Ali bem Wahshiyya na-Nabati publicou vários alfabetos de cifras, os quais eram tradicionalmente usados para mágicas [9].

No início do **século XI**, o Emirado Ghaznavid foi fundado por Sebuk-Tigin, um Governador Ghazni, no Afeganistão, revoltando-se contra o Emirado Samanid, ele estabeleceu em estado que controlava o Afeganistão e partes da Pérsia e do Norte da Índia. O Emirado existiu de 977 até 1186. "Alguns documentos com textos cifrados do governo de Ghaznavid na Pérsia conquistada sobrevivem e um cronista relata que altos oficiais recebiam cifras pessoais antes de serem enviados para ocupar novos postos. Mas a falta de continuidade dos estados islâmicos e a consequente falha em desenvolver um serviço civil e em criar embaixadas permanentes em outros países acabou por restringir o uso mais difundido da criptografia" [32].

Entre **1119** e **1311**, O Templo era uma ordem de monges combatente fundada em 1119 pelos cavaleiros Udo Dei Pagani e Geoffrey de Saint-Omer para proteger os peregrinos na Terra Santa. Logo após a sua fundação em Jerusalém, Balduíno II, Imperador de Constantinopla, concedeu-lhes um palácio nas proximidades do Templo de Salomão, donde originou o nome da Ordem. A Ordem enriqueceu devido a numerosas doações e se tornou numa Organização internacional, que por muito tempo, teve uma influência notável, rivalizando com a do Rei de França e até do Papa. Em 1291 os templários foram obrigados a abandonar a Terra Santa, fugindo para a Ilha do Chipre. A Organização cifrava suas letras de crédito usando um método próprio. Em 1311, a ordem dos templários foi dissolvida por Filipe, o Belo. Em sérias dificuldades financeiras, Filipe mandou prender e torturar os templários para que estes entregassem suas riquezas. Um ano mais tarde, em 1312, um decreto do Concílio de Viena aboliu a Ordem.

Entre **1187** e **1229**, Ibn Dunainir, de nome completo Ibrahim ibn Mohammad ibn Dunainir, escreveu o livro *Maqasid al-Fusur al-Mutarjamah na Hall at-Tarjamah* "Explicações claras para a solução de mensagens secretas", de salientar que este livro foi redescoberto em 1987. O livro contém uma inovação importante que são as cifras algébricas (substituição de letra de números e transformá-los aritmeticamente).

Entre **1187** e **1268**, Ibn Adlan, de nome completo Afif Ad-Din Adlan ibn Hammad ibn Ali al-Mousili na-Nahwi al-Mutarjim, escreveu o livro *Al-Um'allaf lil-Malik al-Ashraf* (escrito para o Rei al-Ashraf), de salientar que este livro foi redescoberto em 1987. O livro contém explicações detalhadas sobre a criptoanálise.

Em **1226**, uma criptografia política discreta apareceu nos arquivos de Veneza, onde pontos e cruzes substituíam as vogais em algumas palavras esparsas.

Em aproximadamente **1250**, o frade franciscano Inglês Roger Bacon (1214-1294), cognominado "Doctor Mirabilis". Descreveu sete métodos de cifras e escreveu: "Um homem é louco se escrever um segredo de qualquer outra forma que não seja a de o dissimular do vulgar".

Nos anos **1300**, Abdal-Rahman Ibn Khaldun escreveu o *Muqaddimah*, um importante salto da história que cita o uso de "nomes de perfumes, frutas, passáros ou flores para indicar letras, ou [...] sobre formas diferentes das formas das letras aceites" como um código usado entre escritórios de impostos e militares. Ele também inclui uma referência à criptoanálise observando que "escritos conhecidos sobre o assunto estão em poder do povo".

Entre **1312** e **1361**, Ibn Ad-Duraihim, cujo nome completo era Taj ad-Din Ali ibn Muhammad ibn Abdul'Aziz ad-Duraihim, escreveu o livro *Miftah al-Kunuz fi Idah al-Marmuz* "Chaves para a elucidação de mensagens secretas" contendo uma classificação de cifras, análise de frequências em várias línguas, uma tabela de Trithemius (Vigenère) e Grades [28].

Em **1378**, depois do Cisma de Avignon, o antipapa Clemente VII decide unificar o sistema de cifras da Itália Setentrional e designou tal tarefa a Gabriele Lavinde. Lavinde compilou uma colecção de cifras num manual, do qual o Vaticano conserva uma cópia de 1379. Com seu alfabeto de substituição combinada (código/cifra) ele uniu a cifra de substituição com um código de listas de palavras, sílabas e nomes equivalentes. Este sistema foi amplamente utilizado por diplomatas e alguns civis europeus e americanos por mais de 450 anos.

Em **1392**, Geoffrey Chaucer, considerado o melhor poeta inglês antes de Shakespeare, no seu *The Equatorie of the Planetis*, um suplemento do seu *Teatrise of the Astrolabe*, inclui seis passagens escritas em cifras. O sistema de cifras consiste num alfabeto de símbolos de substituição (ver Figura 13). A solução do criptograma mostrado é *This table servith for to entre in to the table of equation of the mone on either side.*

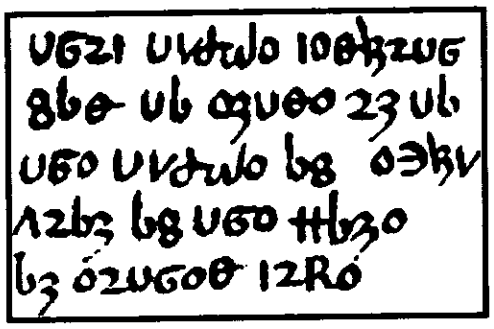


Figura 13 – Substituição de Chaucer [32].

Em **1401**, Simeone de Crema usou uma chave na qual cada vogal do texto original possuía vários equivalentes. Isto comprova que nesta época, o Ocidente conhecia a criptoanálise (ver Figura 14). Não pode haver outra justificação para o aparecimento de destes múltiplos substitutos ou homófonos. O facto dos homófonos serem aplicados a vogais, e não apenas indiscriminadamente, demonstra o conhecimento do esboço de uma análise de frequência. O uso da análise de frequência pode levar a uma solução rápida de cifras de substituição monoalfabéticas simples. Acima, a chave da substituição homofónica de Crema.

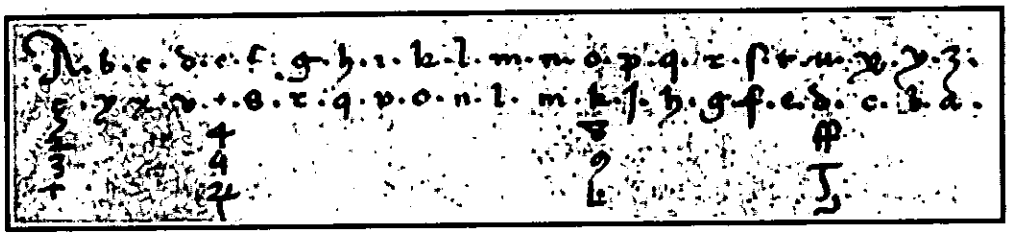


Figura 14 – Substituição homofónica de Crema [32].

Em **1411**, Michele Steno, doge de Veneza, mostra-nos um dos primeiros exemplos de cifras homofónicas: escolhia um dos muitos símbolos para cada carácter, além de usar nulos e caracteres especiais para certas palavras de uso frequente.

Em **1412**, Qalqashandi, de nome completo Shinab al-Din abu `l-`Abbas Ahmad bem `Ali bem Ahmad `Abd Allah al-Qalqashandi, escreveu a *Subh al-a`sha*, uma enciclopédia de 14 volumes em Árabe, na qual incluiu uma secção de Criptologia. Esta informação foi atribuída a Taj ad-Din `Ali ibn ad-Duraihim ben Muhammad ath-Tha`álibi al-Mausili (1312-1361) cujos escritos obre Criptografia perderam-se. A lista de cifras nesta obra inclui tanto a substituição quanto a transposição, e pela primeira vez, uma cifra com múltiplas substituições para cada letra do texto original. Também é atribuída a Ibn al-Duraihim uma explicação com exemplo de criptoanálise, inclusive o uso de tabelas de frequência de letras e conjuntos de letras que podem ocorrer juntas numa palavra [25].

Em **1466**, Leon Baptista Alberti (um amigo de Leonardo Dato, um secretário pontifical que terá, provavelmente, introduzido Alberti na criptografia) inventou e publicou a primeira cifra polialfabética, criando um disco de cifragem (conhecido actualmente como "Captain Midnight Decoder Badge") para simplificar o processo (ver Figura 15). Ao que tudo indica, esta classe de cifra não foi quebrada até os anos de 1800. Alberti também tem muitos escritos sobre o estado da arte em cifras, além da sua própria invenção. Também faz uso do seu disco para obter código cifrado. Estes sistemas eram muito mais fortes que a nomenclatura usada por diplomatas da época e continuaram sendo por muito mais séculos. O *Trattati em cifra* de Leone Battista Alberti foi publicado em Roma em 1470. Se referia a teorias e processos de cifragem, métodos de decifração e dados estatísticos.

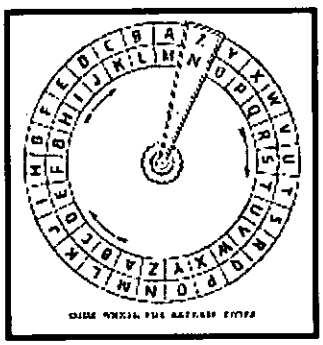


Figura 15 – Disco de cifragem [32].

Entre **1473** e **1490**, um manuscrito de Arnaldus de Bruxella usa cinco linhas de cifras para ocultar a parte crucial da operação que fazia a *Pedra Filosofal*.

Em **1474**, Sicco Simonetta publicou *Regulae ad extrahendum litteras zifferatas sine exemplo*, um pequeno escrito ressaltando métodos de decifragem e fornecendo dados estatísticos consideráveis. De realçar que, a data desta publicação é importante porque se tratava dum período no qual a criptografia se tornou prática Universal e quando as cifras evoluíram para criptogramas complicados [32].

4.1.3. Idade Moderna (1453-1789)

Em **1518**, Johannes Von Heydenberg aus Trittenheim/Mosel, escreveu o primeiro livro impresso de criptologia. Ele inventou uma cifra esteganográfica na qual cada letra era representada como uma palavra obtida de uma sucessão de colunas. A série de palavras resultantes seria uma oração legítima. Também descreveu cifras polialfabéticas na forma de tabelas de substituição rectangulares que, na época, já tinham se tornado padrão. Introduziu a noção da troca de alfabetos a cada letra.

Johannes Trithemius escreveu, porém não publicou sua *Steganographia*, a qual circulou como manuscrito por mais de cem anos, sendo copiada por muitas pessoas que desejavam extrair os segredos que se pensava que continha.

A *Polygraphiae libri sex* de Trithemius, a qual incluía sua tabela de substituição "Tabula recta Caeser" foi publicada em 1518, apesar de haver dúvidas quanto à data correcta (ver Figura 16). Foi reimpressa em 1550, 1564, 1571 e 1600. Uma tradução em Francês apareceu em 1561 e em 1564.

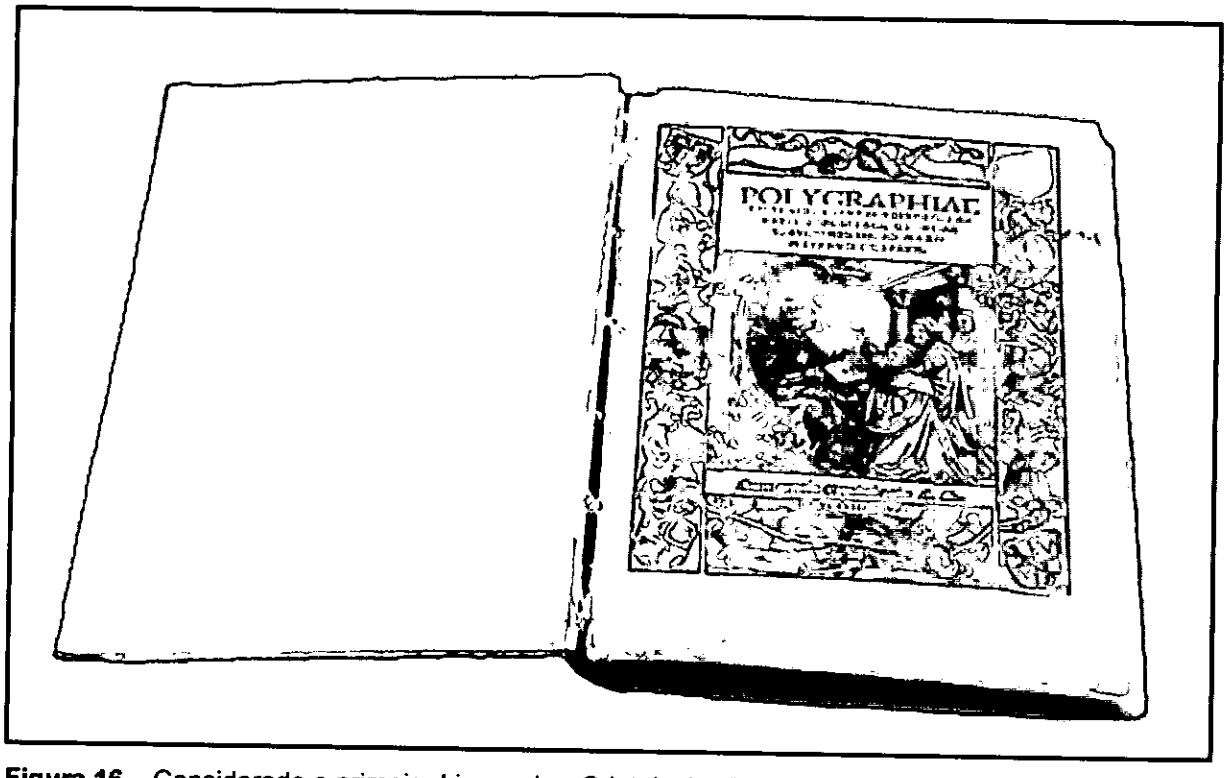


Figura 16 – Considerado o primeiro Livro sobre Criptologia: *Polygraphiae* [25].

Em **1526**, o *Opus novum princibus maxime vtilissimum pro cipharis* do Jacopo Silvestri é impresso. A obra discute seis métodos de cifras, inclusive a Cifra de César, para a qual ele recomendava o uso dum disco de cifragem. *Opum novum* foi escrito para ser um manual prático de criptologia.

O alfabeto-chave de Silvestri não possuía as letras j, v, w e y. No disco ilustrado na Figura 17, as três marcas que sucedem o Z representam: & para *et*, um símbolo usado comumente no Latim medieval para significar *us* ou *um* no final de palavras (p. ex., plurib9 = pluribus), ou *com*, *com*, *cum* ou *cun* no início de palavras (p.ex., 9cedo = concedo); e um símbolo usado para *rum*, a terminação do genitivo plural latino (illo# = illorum). O zig-zag no centro da figura deve corresponder a uma pequena manivela para girar os discos móveis [32].

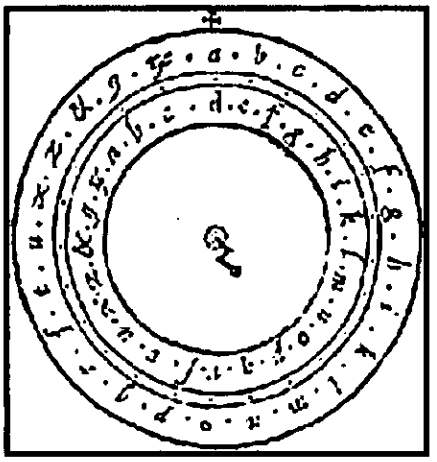


Figura 17 – Disco de cifragem [32].

Em **1533**, Heinrich Cornelius Agripa von Netteisheim publica o *De oculta philosophia*, em Colónia na Alemanha. No livro 3, capitulo 30, descreve sua cifra de substituição monoalfabética, hoje conhecida como cifra de Pin Peg (ver Figura 18). A tradução literal do nome é Porco no Chiqueiro e vem do facto de que cada uma das letras (os porcos) é colocada numa "casa" (o chiqueiro).

Na época a cifra parece ter sido de importância pois, alguns anos mais tarde, Vigenère a reproduz no seu *Traicté dês chiffres*, ou *Secretes manieres d'escrire*. Aparentemente, esta cifra foi usada pela sociedade secreta dos franco-maçons.

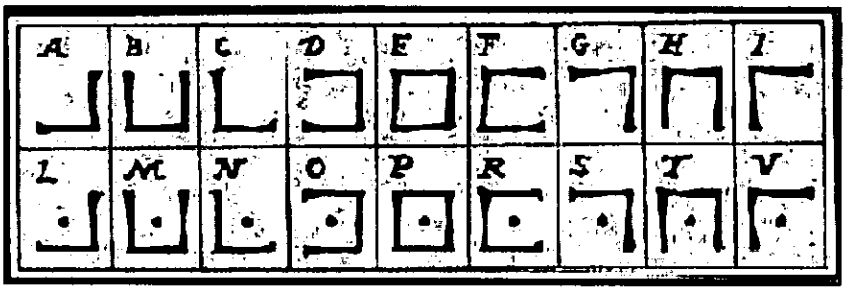


Figura 18 – Cifra de Pin Peg [32].

Em **1540**, Giovanni Battista Palatino publicou seu *Libro nvova d'imparare a scrivere ... Com vn breue et vtile trattato de le cifere*. Foi impresso em 1545, 47, 48, 50, 53, 56, 61, 66, 78 e 1588. Uma versão revisada foi impressa em 1566, 78 e 88.

Em **1550**, foi publicado o *De subtilitate libri XXI* de Girolamo Cardano, esta obra contêm uma quantidade considerável de informações a respeito de processos de cifragem. Foi reimpressa em 1551, duas vezes em 54, 59, outras duas vezes em 60, e em 80 e 82. Uma tradução francesa foi impressa em 1556. Cardano inventou o primeiro procedimento com auto-chave, mas seu sistema era imperfeito. A grelha de Cardano consiste numa folha de material rígido onde se encontram, em intervalos irregulares, pequenas aberturas rectangulares da altura de uma linha de escrita e de comprimento

variável. O remetente escreve o texto nas aberturas, depois retira a folha e completa os espaços vazios com letras quaisquer. O destinatário põe a mesma grelha sobre o texto cifrado para ler a mensagem.

Em **1556**, Cardano publica *De rerum varietate libri XVII*, o qual continha informações criptográficas e era a continuação do seu popular *De subtilitate*. Ambos livros foram traduzidos e pirateados por editores europeus. O *De rerum* foi reimpresso em 1557, 58, 80 e 81.

Em **1551**, John Dee (1527-1608), alquimista e matemático inglês, estudou e ministrou aulas no continente europeu em 1547 e 1550. Retornou à Inglaterra em 1551, tornando-se astrólogo da Rainha Maria Tudor. Logo após foi preso por ser mágico, sendo libertado em 1555. Entre 1583 e 1589 viajou pela Polónia e Boémia exibindo-se como mágico na corte de vários príncipes. Trabalhou com o alfabeto Enoquiano, também denominado linguagem "Angelical". O alfabeto desta linguagem arcaica é composto por 21 letras e foi descoberto por Dee e Edward Kelley. A linguagem possui gramática e sintaxe próprias, porém apenas pequenos exemplos foram traduzidos para o Inglês. John Dee também possui uma escrita encriptada que ainda não foi quebrada [32].

Em **1553**, Giovanni Battista Bellaso, secretário do cardeal Duranti e do cardeal Rodolfo Pio, introduziu a noção de uso de uma senha como chave para uma cifra polialfabética. *La cifra delm Sig. Giovan Battista Bellaso* foi publicado em 1553, depois corrigido e reimpresso em 1557 e 1564.

Em **1564**, Bellaso publicou uma cifra de *auto-chave*, melhorando o trabalho de Cardano, o qual parece ter sido o autor da ideia. Esta é a operação padrão das cifras polialfabéticas denominada *Vigenère*.

Em **1556**, a Espanha sob regência de Filipe II, adoptou as mais modernas nomenclaturas com homófonos (2 símbolos para as consoantes e 3 para as vogais) e listas para a substituição dos digrafos e trígrafos mais usados. Associados à nomenclatura e às letras, utilizaram códigos. O sistema foi usado até o século XVII e, a cada 3 a 5 anos, os códigos eram modificados.

Em **1558**, Philibert Babou, embaixador em Roma do Rei Henrique II, adoptou as mais modernas nomenclaturas com homófonos na correspondência oficial. Pode-se dizer que a cifra de Babou era uma substituição homofónica simplificada.

Em **1563**, o *Magiae natvralis libri XX* de Giambattista Della Porta, que no Livro XVI trata de decifração, foi publicado em 1558. Foi reimpresso em 1560, duas vezes em 61, 62, 64, 67, 76, 85, 91, 97 e 1607. Uma tradução francesa anónima foi impressa em 1565, 67, 70, 71 e 84.

Em **1563**, Della Porta escreveu um texto sobre cifras introduzindo a cifra digrâmica (ou digráfica). Ele classificou as cifras em cifras de transposição, de substituição e de substituição por símbolos. Sugeriu o uso de sinónimos e erros ortográficos para confundir os criptoanalistas. Aparentemente introduziu a noção de alfabeto misto numa tabela polialfabética. Neste ano, foi também publicado o *De fvrtivis literarvm notis, vvlgo de ziferis Libri IIII*, do mesmo autor. No mesmo ano apareceu traduzido em Inglês sob o título *On secret notations for letters, commonly called ciphers*. Seus quatro livros, tratando respectivamente de cifras arcaicas, cifras modernas, criptoanálise e uma lista de peculiaridades linguísticas que ajudavam na solução, compilavam o conhecimento criptológico da época. Um conjunto rococó de discos de cifragem acompanhava os livros. A obra foi reimpressa em 1591, 93, duas vezes em 1602, em 1603 e 1606. Em 1591, o *De fvrtivis* de Della Porta foi reimpresso por John Wolfe em Londres, o qual aprimorou a edição original em 1563 tornando-a praticamente perfeita. Em 1593, o *De fvrtivis* foi reeditado, sem permissão, como *De occvltis literarvm notis* e incluía o primeiro jogo de tabelas criptológicas sinópticas jamais publicadas. Foi reimpresso em 1603 e 1606 [32].

Em **1588**, François Viete, matemático francês, introduziu a primeira notação algébrica sistematizada e contribuiu para a teoria das equações. Apesar de ser mais conhecido como matemático, ele também foi um dos melhores especialistas em cifras de todos os tempos.

No final do **século XVI**, o império espanhol dominava grande parte do mundo, e por isso, os agentes espanhóis tinham que se comunicar usando uma cifra muito intrincada. Na realidade, a cifra era composta por mais de 500 caracteres, usados pelo Rei Filipe II da Espanha durante sua guerra em defesa do Catolicismo Romano e dos hunguenotes franceses. Algumas mensagens de soldados espanhóis foram interceptadas pelos franceses e acabaram nas mãos do Rei Henrique IV da França. O rei entregou estas mensagens espanholas para Viete, o matemático, na esperança de que ele as decifrasse. O matemático teve sucesso e guardou o segredo quando, após dois anos, os espanhóis descobriram seu feito. O rei Filipe de Espanha, acreditando que uma cifra tão complexa nunca pudesse ser quebrada, sendo informado de que os

franceses conheciam seus planos militares, foi se queixar ao Papa alegando que se estava usando magia negra contra o seu país. O Papa, no entanto, não acreditou na história [32].

Em **1585**, Blaise de Vigenère, escreveu um livro sobre cifras, incluindo os primeiros sistemas autênticos de texto em claro e de texto cifrado com auto-chave, nos quais letras prévias do texto em claro ou cifrado são usadas para a letra chave actual. A ideia da auto-chave sobrevive até os dias de hoje nos modos CBC e CFB do DES [32].

Em **1586**, Blaise de Vigenère publica o seu *Traicté dês chiffres*, um tratado de 600 páginas. Nele discute muitas cifras, inclusive o sistema de "auto-chave corrente", usada em algumas máquinas de cifragem modernas, e o assim chamado método "Vigenère Tableau".

Em **1587**, Maria, Rainha da Escócia, é decapitada por tentar organizar o assassinado da rainha Elizabete I. Os agentes da rainha Elizabete I desmascararam os planos de Maria com a ajuda da criptoanálise.

Em **1591**, Matteo Argenti, sobrinho de Della Porta, publica um folheto de 135 páginas sobre criptologia. Ele usa uma chave mnemónica para misturar o alfabeto secreto onde deixa de lado as letras duplas.

Em **1592**, Julius Caeser Scaliger publicou seu *Exotericarvm exercitationvm liber XV* de 1220 páginas. Foi reimpresso em 1557, 60 e 76.

No final do **século XVI**, a França começa a liderar o mundo da criptoanálise.

Em aproximadamente **1620**, o cardeal francês Richelieu usou um sistema parecido com o de Cardano. Escrevia uma mensagem qualquer, que fazia algum sentido e que continha as letras da mensagem secreta na ordem correcta. O destinatário possuía uma grelha preparada previamente por Richelieu que permitia desvendar a mensagem enviada [32].

Em **1623**, Sir Francis Bacon (que se supõe ter sido William Shakespeare) inventou um sistema de esteganografia que ele publicou em *De dignitate et augmentis scientiarum*. Denominou seu alfabeto bilateral porque utiliza uma combinação das duas letras A e B em grupos de cinco. A cifra é conhecida como "Cifra de Bacon", hoje em dia classificada como codificação binária de 5 bits.

Em **1641**, John Wilkins, Bispo de Chester, Inglaterra, na sua obra *Mercury or The Secret Swift Messenger* descreve uma cifra empregando a notação musical. Além disso, descreve várias formas de sistemas esteganográficos como tintas secretas. Menciona o assim chamado Pig Latim, uma forma de encriptação falada que pode ser chamada *criptofónia*. A criptofónia já foi muito usada pelos índios ancestrais [28].

Em **1663**, Athanasius Kirchner (1601-1680), estudioso e matemático alemão, publicou *Polygraphia Nova et Vniversales ex Combinatória Arte Detecta* baseado principalmente em Trithemius e Vigenère. Transformou as cifras multialfabéticas em cifras numéricas. Na primeira parte da obra, Kirchner propõe um sistema de *Pasigrafia*, ou escrita Universal, empregando números que correspondiam a palavras de sentido semelhante em Latim, Italiano, Francês, Alemão e Espanhol.

Em **1670**, Francesco Lana Terzi (1631-1687), físico e naturalista Italiano, publica *Padromo all'Arte Maestra*. Nesta obra esta patente uma descrição ilustrada duma cifra usando a notação musical. Também propõe métodos para escrever para cegos e de como ensinar surdos a falar.

Em **1671**, Gottfried Wilhelm von Leibniz (1646-1716), filósofo e matemático alemão, inventou o cálculo diferencial e integral (independentemente de Sir Isaac Newton), a máquina de calcular e descreveu o sistema binário. Sua máquina de calcular usava a escala binária. Esta escala é usada até hoje e é conhecida como código ASCII.

De **1685** à **1692**, os trabalhos do Inglês John Falconer sobre escritas secretas e transmissão de mensagens cifradas incluem *Cryptomenysis Patefacta* ou "A Arte da Informação Secreta Revelada sem uma chave" (1685) e "Regras para explicar e decifrar todo Tipo de Escritas Secretas" (1692). Uma das partes mais interessantes do *Cryptomenysis Patefacta* é a que se refere a semiologia, que Falconer define como "Métodos de informação secreta através de sinais e gestos". Entre tais sinais e gestos inclui os hieróglifos egípcios e alfabetos através do uso dos dedos (dactilografia).

Em **1691**, Antoine Rossignol e seu filho Bonaventure elaboraram a grande cifra de Luís XIV. Ela caiu em desuso após a morte dos seus inventores e suas regras precisas foram rapidamente perdidas. A grande cifra era muito robusta, tanto que só foi quebrada no final do século XIX. Hipoteticamente foi quebrada por Bazeries ou por Victor Gendron.

O **século XVIII** ficou conhecido como a era da espionagem das "Black Chambers" (Câmaras Escuras) na Europa. Viena possui uma das mais eficientes, chamada de

Geheime Kabinettskanzlei, liderada pelo Barão Ignaz von Koch. Sua função consistia em ler a correspondência diplomática internacional, copiar as cartas e devolvê-las às agências de correio na mesma manhã. Relata-se que cerca de 100 cartas eram manipuladas diariamente. Na França era chamada de "Cabinet Noir" e existia desde 1680, formada por vários criptoanalistas contratados pelo Governo. A "Black Chamber" inglesa foi formada por John Wallis em 1701. Após a sua morte, em 1703, seu neto, William Blencowe, assumiu seu posto e recebeu o título de Decypherer [32].

Em **1850**, as "Black Chambers" foram dissolvidas.

Em **1734**, o Belga José de Bronckhorst, Conde de Gronsfeld, melhora a cifra de César usando um deslocamento variável baseado numa chave numérica. Analisando a "Cifra de Gronsfeld", como ficou conhecida, verifica-se que se parece com uma cifra de Vigenère, porém com apenas 10 deslocamentos possíveis ao invés de 26.

Em **1738**, Crystobal Rodriguez, escreveu a *Biblioteca Universal de la Polygraphia Español*, publicada em Madrid em 1738. Esta foi o primeiro estudo completo sobre a criptografia e paleografia de Espanha. Consiste, principalmente, de numerosas tabelas de alfabetos e sinais e de fac-similes de apontamentos e documentos escritos em forma abreviada. Rodriguez. A introdução é de Bias António Nassarre y Ferriz e trata da escrita na Espanha entes da invasão dos Árabes em 711.

Em **1772**, Philip Thicknesse (1719-1792) escreveu *A Treatise on the Art of Decyphering, and of writing in Cypher* publicado em Londres em 1772. Esta obra retrata a teoria da escrita secreta não entrando em detalhes acerca nas aplicações dos métodos criptográficos. Esta obra possui uma secção de interesse especial sobre o uso do alfabeto harmónico, onde notas musicais representam as letras do alfabeto [32].

4.1.4. Recentemente

Em aproximadamente **1795**, Thomas Jefferson, com a ajuda do Dr. Robert Patterson, um matemático da Universidade da Pensilvânia, inventa um cilindro cifrante (ou cifra de roda). Apesar da criatividade deste dispositivo composto por 26 discos, este nunca chegou a ser usado. O cilindro de Jefferson é um dispositivo que permite realizar com rapidez e segurança uma substituição polialfabética. Os cilindros cifrantes são uma invenção do século XIX. Foram reinventados por diversas vezes e utilizados pelos militares no século XX até a Segunda Guerra Mundial.

Em **1799**, é descoberta a Pedra da Roseta, com a qual foi possível decifrar os hieróglifos egípcios. As mensagens da pedra, que pode ser considerada um "dicionário" em três línguas, foram decifradas somente em 1822 por Champollion, após uma tentativa frustrada feita por Thomas Young em 1814.

Ainda em **1799**, a bateria do Allesandro Volta (1745-1827), nascido em Como, na Itália, proporciona a primeira fonte prolongada de electricidade.

Em **1808**, o espanhol Francisco de Paula Martí (1762-1827), baseado nas obras de Trithemius e Kircher, escreve *Poligrafía, ó Arte de Escribir en Cifra de Diferenter Modos*. Descreve cifras de substituição numéricas e alfabéticas. A segunda parte da obra trata da escrita invisível, onde Martí descreve métodos para tornar textos legíveis em mensagens onde a tinta tenha desbotado ou que tenham sido escritas com tinta invisível.

Em **1817**, o coronel Decius Wadsworth, engenheiro, produziu um disco cifrante em que as engrenagens possuíam um número diferente de letras nos alfabetos claro e cifrante, o que resulta numa cifra progressiva na qual os alfabetos são usados irregularmente, dependendo do texto em claro utilizado.

Em **1834**, Louis Braille (1809-1852), educador francês, cego desde os 3 anos de idade. Interessou-se por um sistema de escrita, apresentado na escola Charles Barbier, no qual uma mensagem codificada em pontos era cunhada em papel-cartão. Aos 15 anos de idade trabalhou numa adaptação, escrita com um instrumento simples. O Código Braille consiste de 63 caracteres, cada um deles constituído por 1 a 6 pontos dispostos numa matriz ou célula de seis posições. Mais tarde adaptou este sistema para a notação musical. Publicou tratados sobre seu sistema em 1829 e 1837. O sistema Braille é universalmente aceito e utilizado até os dias de hoje.

Em **1839**, Sir William Brooke O'Shaughnessy, cirurgião inglês, desenvolve um sistema de telegrafia próprio e muda a história do colonialismo britânico e da Guerra da Criméia. Apesar disso, os contemporâneos, Morse (nos EUA), Cooke e Wheatstone (na Inglaterra) e O'Shaughnessy (na Índia) desenvolvem sistemas de comunicação independentes. O mais amplo e que entrou em funcionamento mais rapidamente foi o de O'Shaughnessy, pois em três anos havia puxado 6.500 km de linhas que interligavam toda a Índia [32].

Em **1840**, Samuel Morse (1791-1872) desenvolve o código que recebeu o seu nome. Na verdade não é um código, mas sim um alfabeto cifrado em sons curtos e longos.

Morse também foi o inventor de um dispositivo que chamou de telégrafo e, em 1844, enviou sua primeira mensagem com os dizeres "What hath God wrought". A invenção do telégrafo altera profundamente a criptografia e torna a cifragem uma necessidade absoluta.

Em **1843**, Edgar Allan Poe publicou um escrito intitulado *O escaravelho de ouro*, na qual ele narra a aventura de um indivíduo que encontra uma mensagem cifrada no escaravelho, a qual indica a localização de uma fabuloso tesouro. Poe, um excelente criptoanalista aficcionado, explica em detalhes como a mensagem pode ser decifrada usando-se técnicas estatísticas [32].

Em **1854**, Charles Babbage, matemático, quebra a cifra de Vigenère e projecta as primeiras máquinas de cálculo sofisticadas: a "Máquina das Diferenças" e a "Máquina Analítica". A cifra Playfair é inventada por Sir Charles Wheatstone e publicada pelo seu amigo Lyon Playfair. Esta cifra usa uma matriz de letras com chaves para produzir uma cifra digráfica, fácil de ser utilizada em campos de batalha. Wheatstone também reinventou o dispositivo de Wadsworth.

Em **1857**, após sua morte, a cifra do almirante Sir Francis Beaufort (uma variação da cifra de Vigenère), sob a forma de um cartão de cerca de 10x13 cm, é publicada por seu irmão.

Em **1859**, Pliny Earle Chase publica a primeira descrição de uma cifra fraccionante (tomográfica).

Em **1863**, Friedrich Wilhelm Kasiski (1805-1881), publicou seu texto de 95 páginas Die *Geheimschriften und die Dechiffrierkunst* ou "As escritas secretas e a arte da decifração". Que refere-se à solução de cifras polialfabéticas de chave repetida, um problema que vinha atormentando os criptoanalistas durante séculos. Basta lembrar que a cifra de Vigenère era considerada inquebrável desde o século 17. Desapontado com a falta de interesse pelas suas descobertas, Kasiski voltou sua atenção para outras actividades, inclusive para a antropologia [32].

De **1861** à **1865**, na Guerra Civil Americana, a União utilizou a substituição de palavras seleccionadas seguida de uma transposição colunar de palavras enquanto que os Confederados usaram Vigenère.

Em **1881**, o austríaco Eduard Baron (Freiherr) von Fleissner von Wostrowitz (1825-1888), publicou em Viena seu livro *Handbuch der Kryptographie* ou "Manual de Criptografia". É o inventor da Grade Giratória.

Em **1890**, Júlio Verne (1828-1905) utilizou a criptografia em três de suas novelas, "Viagem ao centro da Terra", "Mathias Sandorf" e "A Jangada".

Em **1891**, o major Etienne Bazeries (1846-1931), comandante francês, cria uma nova versão de cilindro cifrante, semelhante ao Cilindro de Jefferson. Oferece o aparelho ao exército francês, mas seu cilindro acabou sendo rejeitado.

Em **1893**, as primeiras transmissões de sinais telegráficos e da voz humana em telefonia sem fio são realizadas em São Paulo, Brasil, pelo padre Roberto Landell de Moura. Apesar disso, o mérito de inventor da telegrafia sem fio acaba ficando com o italiano Marconi. Provavelmente nenhum dos dois tinha noção do impacto dos seus inventos sobre a criptologia [32].

4.1.5. Actualidade

Em **1901**, Guglielmo Marconi inicia a era da comunicação sem fio. Apesar da vantagem de uma comunicação de longa distância sem o uso de fios ou cabos, o sistema é aberto e aumenta o desafio da criptologia. Inicialmente a telegrafia sem fio utilizava apenas o código Morse, acessível a todos que captassem os sinais. Impunha-se a necessidade de codificações que garantissem o sigilo das mensagens.

Em **1913**, o Capitão Parket Hitt reinventou o cilindro cifrante, em forma de fita, abrindo caminho para o M-138-A da Segunda Guerra Mundial.

Em **1916**, o Major Joseph O. Mauborgne passou a cifra de fita de Hitt novamente para a forma de cilindro, fortaleceu a construção alfabética e produziu o dispositivo que se transformaria no M-94. Em 1918 aperfeiçoou a cifra de Vernam: o One-Time-Pad, cuja tradução livre para o Português seria "Bloco Descartável".

Em **1917**, William Frederick Friedman o "pai" da criptoanálise nos Estados Unidos, começa a trabalhar como criptoanalista civil no Riverbank Laboratories, que também presta serviços ao governo dos EUA. Mais tarde Friedman cria uma escola de criptoanálise militar, inicialmente no Riverbank e depois em Washington.

Ainda em **1917**, um funcionário da AT&T, Gilbert Sandford Vernam, inventa uma máquina de cifragem polialfabética capaz de usar uma chave totalmente aleatória e

que nunca se repete. Esta máquina foi oferecida ao governo dos EUA para ser usada na Primeira Guerra Mundial, porém foi rejeitada. Foi colocada no mercado comercial em 1920. Vernam desenvolveu uma única cifra inviolável, baseada na cifra de Vigenère, que leva seu nome. Com o aperfeiçoamento feito por Mauborgne, nasce o One-Time-Pad [32].

Em **1918**, os alemães começam a usar o sistema ADFGVX no final da Primeira Guerra Mundial. Era uma cifra baseada em substituição (através de uma matriz com chave), fraccionamento e depois na transposição das letras fraccionadas. Foi quebrada pelo criptoanalista francês, tenente Georges Painvin. Arthur Scherbius patenteia uma máquina de cifragem e tenta vendê-la ao exército alemão, mas a máquina é rejeitada.

Em **1919**, Hugo Alexander Koch patenteia na Holanda uma máquina cifrante baseada em rotores. Em 1927, passa os direitos de patente para Arthur Scherbius, inventor e distribuidor da máquina Enigma (ver Figura 19) desde 1923. Arvid Gerhard Damm requer uma patente na Suécia para uma máquina cifrante de rotores mecânicos. Esta máquina, sob a direcção de Boris Caesar Wilhelm Hagelin, evoluiu para uma família de máquinas cifrantes. À frente dos negócios, Hagelin foi o único criptógrafo comercial do seu tempo que teve sucesso no seu empreendimento. Após a guerra, uma lei sueca que permitia ao governo apropriar-se de inventos que considerasse importante serem defendidos, fez com que Hagelin se mudasse para Zug, na Suiça, onde foi incorporado pela Crypto AG. Esta empresa ainda está em actividade apesar de estar envolvida numa controvérsia: alega-se que tenha enfraquecido um produto cifrante para poder vendê-lo para o Irão [32].

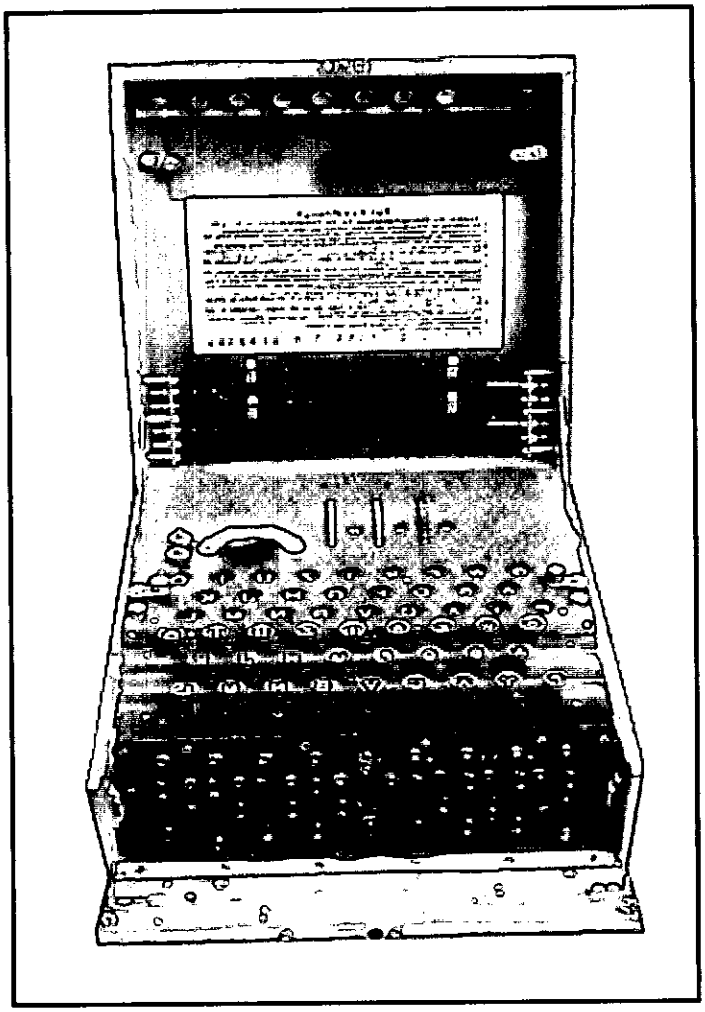


Figura 19 – Máquina Enigma [25].

Em **1921**, Edward Hugh Hebern funda a Hebern Electric Code, uma empresa produtora de máquinas de cifragem electromecânicas baseadas em rotores que giram, no estilo de odómetros, a cada carácter cifrado.

Em **1923**, Arthur Scherbius funda um empreendimento, o Chiffriermaschinen Aktiengesellschaft, para construir e finalmente vender sua máquina Enigma (ver Figura 19) para o exército alemão.

Em **1924**, Alexander von Kryha produz sua "máquina codificante" que foi utilizada até os anos 1950, inclusive pelo Corpo Diplomático alemão. Entretanto, era criptograficamente fraca por possuir um limite pequeno. Um criptograma de teste, com 1135 caracteres, foi decifrado em 2 horas e 41 minutos pelos criptoanalistas Friedman, Kullback, Rowlett e Sinkov.

De **1927** á **1933**, foi um período em que cada vez mais os criminosos, especialmente os contrabandistas, usam a criptografia para os seus propósitos. Elizabeth Smith Friedman decifra os códigos dos contrabandistas de rum na vigência da lei seca [9].

Em **1929**, Lester S. Hill publica seu livro *Cryptography in an Algebraic Alphabet*, no qual um bloco de texto em claro é cifrado através de uma operação com matrizes.

Durante os anos **1930**, a máquina SIGABA (M-134-C) é inventada nos EUA por William F. Friedman. Deavours atribui a ideia a Frank Rowlett, um dos primeiros a serem contratados por Friedman. As invenções de rotores de Hebern e Scherbius foram aperfeiçoadas usando escalonamentos pseudo-aleatórios de múltiplos rotores em cada passo da cifragem ao invés dos escalonamentos uniformes, do tipo odómetro, dos rotores da Enigma. Além disso, usava 15 rotores (10 para a transformação de caracteres e 5, provavelmente, para controlar os estágios) no lugar dos 3 ou 4 rotores da Enigma. A máquina inglesa TYPEX era uma imitação da Enigma comercial adquirida pelos britânicos em 1920 para estudos. Era uma máquina de 5 rotores, dos quais os dois primeiros eram "stators" (estáticos) cuja função era a mesma do painel de plugs da Enigma alemã [32].

Entre **1933** e **1945**, a máquina Enigma não foi um sucesso comercial, porém foi aperfeiçoada até se transformar na ferramenta criptográfica mais importante da Alemanha nazista. O sistema foi quebrado pelos matemáticos polones Marian Rejewski que se baseou apenas em textos cifrados interceptados e numa lista de três meses de chaves diárias obtidas através de um espião, Alan Turing e Gordon Welchman e outros, em Bletchley Park, Inglaterra, deram continuidade à criptoanálise do sistema Enigma.

Em **1937**, a Máquina Púrpura (Purple Machine) dos japoneses foi inventada a partir das revelações feitas por Herbert O. Yardley e seu sistema foi quebrado por uma equipa liderada por William Frederick Friedman. A Máquina Púrpura usava relês telefónicos escalonados ao invés de rotores, apresentando, portanto, permutações totalmente diferentes a cada passo ao invés das permutações relacionadas de um rotor em diferentes posições. Os japoneses não foram capazes de quebrar os códigos dos EUA e imaginavam que seu próprio código também fosse inquebrável, o que não era verdade [32].

Em **1943**, Colossus, um computador para quebrar códigos, é posto em funcionamento no Bletchley Park.

Entre **1943** e **1980**, o projecto criptográfico Venona, conduzido pela NSA (National Security Agency dos EUA), é o mais duradouro dos projectos deste tipo.

Em **1948**, Claude Elwood Shannon, um dos primeiros criptólogos a introduzir a matemática na criptologia, publica seu livro *A Communications Theory of Secrecy Systems*.

Durante a década de **1960**, o Dr. Horst Feistel, liderando um projecto de pesquisa na IBM Watson Research Lab, desenvolve a cifra Lucifer. Alguns anos depois, esta cifra servirá de base para o DES e outros produtos cifrantes, criando uma família conhecida como "Cifras de Feistel" (ver ANEXO D).

Em **1969**, James Ellis desenvolve um sistema de chaves públicas e chaves privadas separadas.

Em **1974** a IBM apresenta a cifra Lucifer ao NBS (National Bureau of Standards) o qual, após avaliar o algoritmo com a ajuda da NSA (National Security Agency), introduz algumas modificações (como as Caixas-S e uma chave menor) e adopta a cifra como padrão de encriptação de dados para os EUA o FIPS PUB-46, conhecido hoje como DES (Data Encryption Standard). Na ocasião, Diffie e Hellman já lançaram dúvidas quanto à segurança do DES, apontando que não seria impossível obter a chave através da Força-Bruta, o que acabou acontecendo 20 anos mais tarde e com um custo 100 vezes inferior ao inicialmente estimado. Hoje o NBS é chamado de National Institute of Standards and Technology, NIST [32].

Em **1976**, Whitfield Diffie e Martin Hellman publicam seu livro *New Directions in Cryptography*, introduzindo a ideia de uma criptografia de chave pública. Também reforçaram a concepção da autenticação através de uma função de via única (one way function), agora usada no utilitário S/Chave pedido de senha/resposta.

Em Abril de **1977**, inspirados no texto publicado por Diffie e Hellman e como absolutos principiantes na criptografia, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman começaram a discutir como criar um sistema de chave pública prático. Ron Rivest acabou tendo uma grande ideia e a submeteu à apreciação dos amigos: era uma cifra de chave pública, tanto para confidencialidade quanto para assinaturas digitais, baseada na dificuldade da factoração de números grandes. Foi baptizada de RSA, de acordo com as primeiras letras dos sobrenomes dos autores. Confiantes no sistema, em 4 de Abril de 1970 os três entregaram o texto para Martin Gardner para que fosse publicado na revista Scientific American. O artigo apareceu na edição de Setembro de 1977 e incluía a oferta de enviar o relatório técnico completo para qualquer um que enviasse um envelope selado com o próprio endereço. Foram recebidos milhares de

pedidos provenientes dos quatro cantos do mundo. Alguém da NSA (National Security Agency dos EUA) contestou a distribuição deste relatório para estrangeiros e, durante algum tempo, os autores suspenderam a correspondência. Como a NSA não se deu ao trabalho de informar a base legal desta proibição, solicitada pelos autores, os três voltaram a enviar os relatórios solicitados. Dois jornais internacionais, "Cryptologia" e "The Journal of Cryptology", foram fundados logo após esta tentativa da NSA de censurar publicações. Rivest, Shamir e Adleman, não publicaram a cifra antes de patenteá-la, aliás, foi uma novidade conseguir patentear um algoritmo [32].

Em **1978**, o algoritmo RSA é publicado nas "Communication" da ACM.

Entre **1984** e **1985**, a cifra ROT13 foi introduzida no software USENET News para permitir a cifragem de mensagens, prevenindo que olhos inocentes fossem assaltados por algum texto questionável.

Em **1986**, Miller sugere a Criptografia de curva elíptica.

Durante a década de **1990**, foram feitos trabalhos em computadores quânticos e criptografia quântica. Trabalhos com biométrica para autenticação (impressões digitais, a íris, etc.).

Em **1990**, Xuejia Lai e James Massey publicam na Suiça *A Proposal for a New Block Encryption Standard* ou "Uma Proposta para um Novo Padrão de Encriptação de Bloco", o assim chamado IDEA (International Data Encryption Algorithm), para substituir o DES. O IDEA utiliza uma chave de 128 bits e emprega operações adequadas para computadores de uso geral, tornando as implementações do software mais eficientes. Charles H. Bennett, Gilles Brassard e colaboradores publicam seus resultados experimentais sobre Criptografia Quântica, a qual usa fotões únicos para transmitir um fluxo de bits chave para uma posterior cifragem Vernam da mensagem (ou outros usos). Considerando as leis que a mecânica quântica possui, a Criptografia Quântica não só oferece a possibilidade do segredo como também uma indicação positiva de interceptação e uma medida do número máximo de bits que possam ter sido interceptados. Uma desvantagem é que a Criptologia Quântica necessita de um cabeamento de fibra óptica entre as partes que se comunicam [32].

Em **1991**, Phil Zimmermann torna pública sua primeira versão de PGP (Pretty Good Privacy) como resposta ao FBI, o qual invoca o direito de acessar qualquer texto em claro da comunicações entre cidadãos. O PGP oferece uma segurança alta para o cidadão comum e, como tal, pode ser encarado como um concorrente de produtos

comerciais como o Mailsafe da RSADSI. Entretanto, o PGP é especialmente notável porque foi disponibilizado como freeware e, como resultado, tornou-se um padrão mundial enquanto que seus concorrentes da época continuaram absolutamente desconhecidos.

Em **1993**, a criptoanálise diferencial é desenvolvida por Biham e Shamir.

Em **1994**, o professor Ron Rivest, autor dos algoritmos RC2 e RC4 incluídos na biblioteca de criptografia BSAFE do RSADSI, publica a proposta do algoritmo RC5 na Internet. Este algoritmo usa rotação dependente de dados como sua operação não linear e é parametrizado de modo que o usuário possa variar o tamanho do bloco, o número de estágios e o comprimento da chave. Ainda é cedo para se avaliar correctamente os parâmetros em relação à força desejada, apesar de que uma análise feita pelo RSA Labs, mostrada na CRYPTO '95, tenha sugerido que w=32 e r=12 proporcionam uma segurança maior que a do DES. O algoritmo blowfish, uma cifra de bloco (ver ANEXO C) de 64 bits com uma chave de até 448 bits de comprimento, é projectado por Bruce Schneier [28].

Em **1997**, o PGP 5.0 Freeware é amplamente distribuído para uso não comercial. O código DES de 56 bits é quebrado por uma rede de 14.000 computadores.

Em **1998**, o código DES é quebrado em 56 horas por pesquisadores do Vale do Silício e em 1999 é quebrado em apenas 22 horas e 15 minutos.

Em **2000**, o algoritmo Rijndael é seleccionado como Advanced Encryption Standard para substituir o DES.

4.2. Vantagens do uso da Criptografia

O desenvolvimento da criptografia permitiu, garantir [16]:

- **Confidencialidade** ⇨ a informação deve ser lida apenas pelo destinatário, e só ele deve ter acesso a mesma;
- **Autenticação** ⇨ evita que alguém se comunique com o sistema em nome de outro e permite certificar se uma mensagem recebida foi enviada pelo verdadeiro remetente;
- **Integridade** ⇨ permite que a informação recebida seja correcta, original e sem alterações, nem intencionais ou acidentais;
- **Não-Repudiação** ⇨ impede que o destinatário, após receber a mensagem, clame que não a recebeu;

- **Controlo de acesso** ⇨ capacidade de limitar e controlar o acesso ao sistema, através da requisição de uma identificação antes de se permitir o acesso, e;
- **Disponibilidade** ⇨ a informação deve estar disponível para acesso no momento desejado, mesmo em caso de perda.

4.3. Limitações do uso da Criptografia

Apesar das grandes vantagens em se usar a Criptografia, esta tem as suas limitações, nomeadamente [15]:

- Se a mensagem encriptada for alterada durante o seu envio o destinatário não poderá decripta-la;
- A mensagem pode ser captada durante o envio e apesar do intruso não poder lê-la o destinatário não terá acesso a mesma;
- Os algoritmos mais seguros são os que usam operações complexas e chaves de tamanho considerável o que faz com que o sistema criptográfico consuma mais recursos computacionais;
- Geralmente, o Texto Cifrado é maior que o Texto em Claro o que aumenta o volume de dados a ser enviado, aumentando, assim o tempo de envio.

4.4. Tipos de Sistemas Criptográficos

Os sistemas criptográficos dividem-se em *simétricos* ou *convencionais* ou *da chave secreta* e *assimétricos* ou *da chave pública*. Os simétricos fazem uso duma mesma chave para encriptar e decriptar a mensagem, isto é, para que haja comunicação entre duas pessoas ambas deverão conhecer a chave para encriptar e decriptar a mensagem (Ver Figura 20), como exemplo podemos citar o DES, o Triple DES, IDEA, Blowfish e o RC2. Quanto aos assimétricos, estes usam duas chaves uma privada e uma pública onde tanto a pública como a privada são usadas para a encriptação e a outra para a decriptação (ver Figura 21), neste caso a usuário possui uma chave pública que distribui de modo à que quem lhe quiser enviar uma mensagem use essa chave para encriptar e outra privada que fica consigo e serve para decriptar, como exemplo podemos citar o RSA, ElGamal, Diffie-Hellman e as Curvas elípticas [12]. Inicialmente a Criptografia baseava-se na encriptação Convencional para manter a confidencialidade, mas nos últimos tempos, houve necessidades de aumentar a funcionalidade da Criptografia, implementando, a autenticação da informação, garantia da integridade da informação, incorporação das assinaturas digitais e uso da Encriptação da Chave Pública.

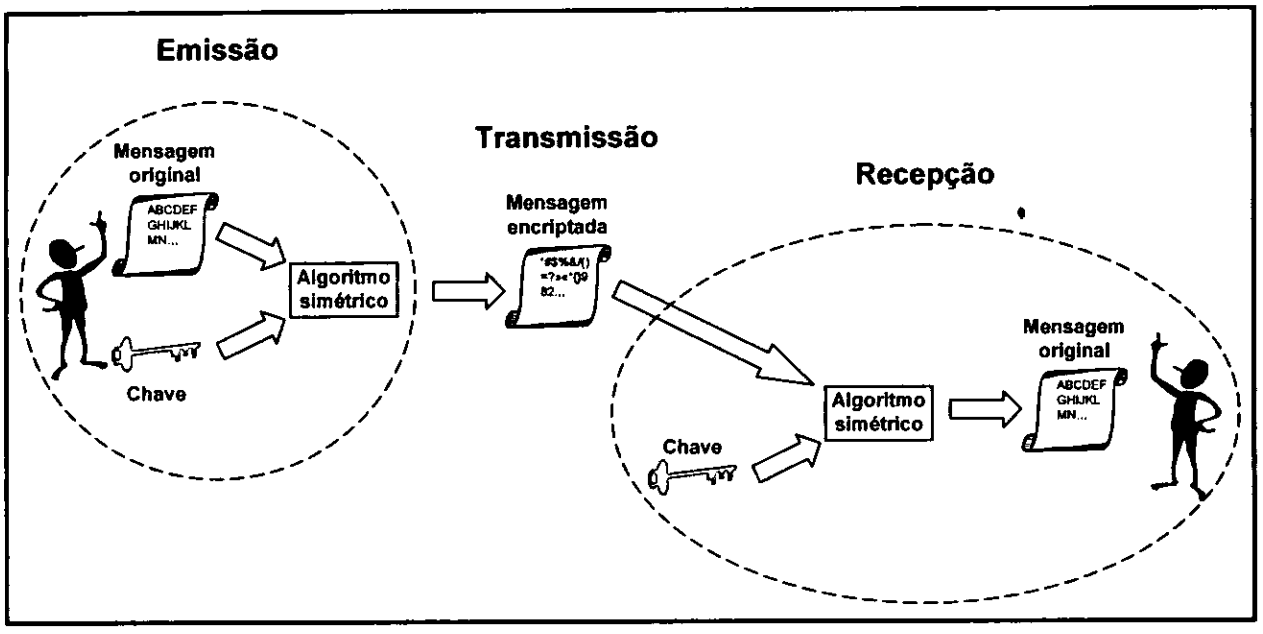


Figura 20 – Sistema de criptografia simétrica.

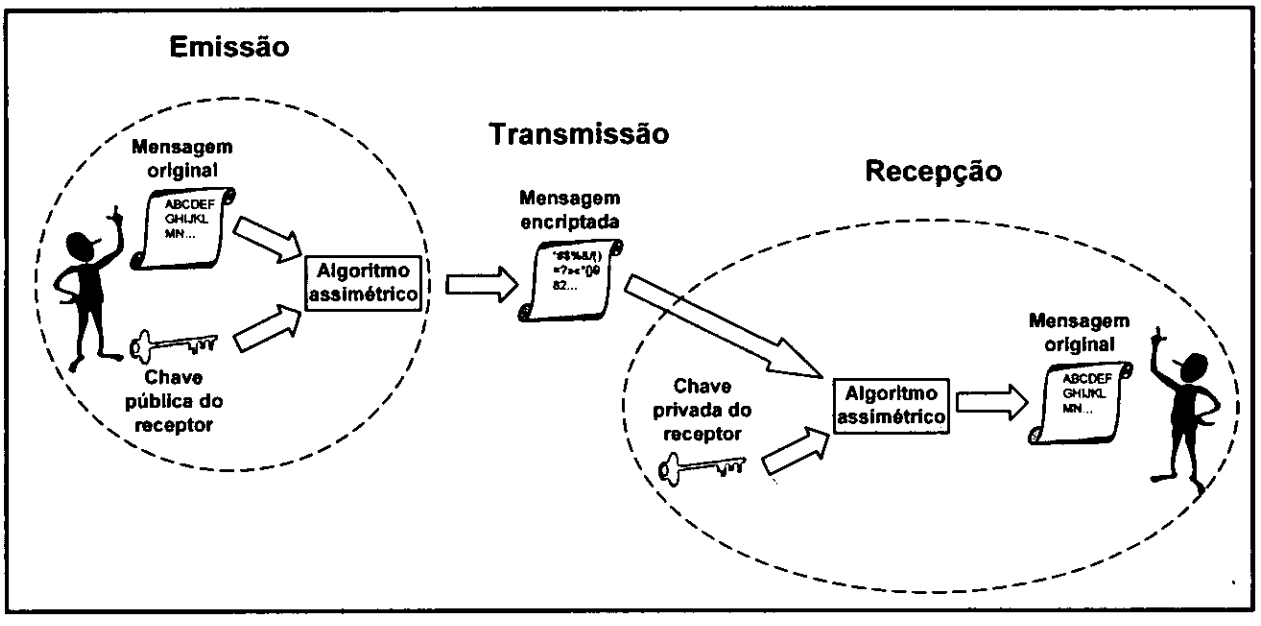


Figura 21 – Sistema de criptografia assimétrica.

4.4.1. Comparação entre os sistemas simétricos e assimétricos

- Nos algoritmos simétricos para que dois elementos se comuniquem é necessário que, antes, ambos conheçam a chave, no caso em que temos *n* usuários precisaríamos de n^2 chaves para que todos se comunicassem entre si, o que traz *problemas para a gestão das chaves*, pois cada par se comunica com uma chave diferente dos restantes e essa chave deve ser mantida secreta. Este problema não acontece nos sistemas assimétricos em que quando um elemento do sistema deseja se comunicar com o outro precisa apenas de procurar a

chave pública deste, e atenção que esta chave não é mantida secreta muito pelo contrário ela é publicada;

- A criptografia simétrica não tem mecanismos de autenticação, isto é, não dá a garantia de que quem enviou a mensagem é de facto quem disse ser, e de não-repudiação, ou seja, se enviarmos uma mensagem para alguém não temos mecanismos que nos avisem quando a pessoa receber a mensagem. Na criptografia assimétrica possuímos uma ferramenta muito poderosa denominada *assinatura digital*, isto é, quando alguém deseja enviar uma mensagem primeiro encripta a mensagem com a sua chave privada e depois volta a encriptar a mensagem com a chave pública do destinatário. Quando o destinatário recebe a mensagem primeiro usa a sua chave privada para decriptar a mensagem e depois usa a chave pública do remetente para decriptar novamente obtendo assim a mensagem original. Como a mensagem encriptada pela chave privada do remetente só pode ser decriptada com a chave pública do mesmo, assim o destinatário tem a certeza que o remetente é autêntico, e;
- Os sistemas baseados na criptografia simétrica são mais rápidos que os da assimétrica.

4.5. Classificação dos Algoritmos Criptográficos

Os algoritmos criptográficos são, geralmente classificados de acordo com três diferentes características [16]:

- **O tipo de operações usadas para transformar o texto em claro em texto cifrado:** Todos algoritmos de encriptação são baseados em dois princípios genéricos: **substituição**, onde cada elemento do texto em claro (bit, letra, grupo de bits ou letras) são mapeados como se tratasse de outro elemento, e **transposição**, onde os elementos do texto em claro são rearranjados. O requisito fundamental é que nenhuma informação seja perdida, isto é, todas operações devem ser reversíveis. A maioria dos sistemas, referidos como produtos do sistema, envolve múltiplos passos de substituição e transposição;
- **O número de chaves usadas:** se tanto o emissor como o receptor usarem a mesma chave, o sistema é denominado simétrico, o de chave única, ou da chave secreta ou ainda encriptação convencional. Se o emissor e o receptor usarem chaves diferentes o sistema é denominado como assimétrico, de chave dupla ou, ainda, de chave pública, como veremos mais adiante.

- **A forma como o texto em claro é processado:** a cifração de bloco processa os dados de entrada, em blocos, um por um, produzindo um bloco de saída por cada bloco de entrada. A cifração de fluxo processa os dados de entrada continuamente, produzindo uma saída de elemento por vez.

4.6. Criptoanálise

Com o desenvolver da criptografia surgiu a *criptoanálise*, esta ciência, ao contrário da criptografia, dedica-se a *decifragem ilegal da mensagem encriptada*, mas sem a posse da chave, usando para isso, principalmente a Força-Bruta, que consiste em usar-se todas as chaves possíveis dum determinado tamanho até se encontrar a certa. A criptoanálise é efectuada por pessoas estranhas a mensagem, isto é, intrusos que podem, tanto, pertencer a organização como não.

Deste modo, podemos definir a Criptoanálise como a Ciência em que se tenta descobrir os valores de X (Texto em Claro) e/ou ou C (Chave). A estratégia usada pelo criptoanalista depende da natureza do esquema de encriptação e da informação disponível para o criptoanalista [24].

Um esquema criptográfico é incondicionalmente seguro se o texto cifrado gerado não conter informação suficiente que determine unicamente o correspondente texto em claro. No entanto, os usuários dum sistema criptográfico devem-se preocupar se o algoritmo seja de tal forma complexo que [16]:

- O custo de quebrar uma mensagem encriptada seja superior ao valor da informação;
- O tempo necessário para quebrar uma mensagem encriptada seja superior ao período de validade da informação.

Se um algoritmo cumprir as condições acima diz-se, então, que é um algoritmo computarizadamente seguro. O problema é que é difícil definir o tempo em que um ataque de criptoanálise necessita para ter sucesso ou o tempo usado para o sucesso dum ataque de Força-Bruta. Na tabela 1 mostra-se o tempo que leva para tentar metade das chaves dependendo do tamanho das mesmas. Os resultados foram calculados prevendo que cada decriptação leva 1 μs, o que é razoável devido a capacidade dos computadores de hoje em dia, claro que com o uso em paralelo de microcomputadores é possível obter-se valores menores [16].

Tamanho da Chave (bits)	Número de chaves alternativas	Tempo necessário para 1 encriptação (μs)	Tempo necessário para 10^6 encriptações (μs)
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutos	2.15 milissegundos
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 anos	10.01 horas
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} anos	5.4×10^{18} anos
26 caracteres (Permutação)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} anos	6.4×10^6 anos

Tabela 1 – Tempo médio requerido para o sucesso do ataque Força-Bruta [16].

Todos os esquemas de criptoanálise são concebidos de forma a explorar partes estruturais do texto em claro que escaparam a Encriptação. Na Tabela 2 descreve-se os mecanismos de segurança e seus ataques.

Segurança	Inteligência
Segurança da comunicação	**Inteligência da comunicação**
➢ Estenografia	➢ Intercepção
➢ Criptografia	➢ Criptoanálise
➢ Segurança do tráfico	➢ Análise de tráfico
Segurança electrónica	**Inteligência electrónica**
➢ Segurança da emissão	➢ Reconhecimento electrónico
➢ Contra-Contramedidas	➢ Contramedidas

Tabela 2 – Métodos de Segurança e seus Objectivos [16].

4.6.1. Tipos de ataques

Como se referiu acima, a criptoanálise depende da informação ou a hipotéticos elementos a que o intruso pode ter acesso, e é com base neles que este define o tipo de ataque a executar para ter acesso a mensagem.

4.6.1.1. Apenas o texto cifrado

Neste caso o intruso tem acesso a:

- Algoritmo de encriptação;
- Texto cifrado para ser decriptado.

Como se pode notar este é um ataque de difícil sucesso, pois o intruso dispõe de pouca informação. Um dos exemplos deste ataque é o de Força-Bruta que consiste em tentar todas as chaves possíveis até que se obtenha uma palavra legível do Texto cifrado. Quanto maior for o tamanho da chave mais impraticável se torna este ataque,

pois as combinações crescem consideravelmente aumentando assim o tempo para que sejam tentadas todas combinações, em média para se obter sucesso neste ataque metade das chaves devem ser tentadas. Além disso, antes de este ataque ser perpetrado o intruso deve efectuar uma análise para recolher dados como, a língua da comunicação, o tipo de ficheiro, o género de informação e outros. Só um algoritmo muito fraco não resiste a este ataque [15].

4.6.1.2. Texto em claro conhecido

Neste ataque o intruso conhece:

- Algoritmo de encriptação;
- Texto cifrado para ser decriptado;
- Um ou mais pares de texto em claro-texto cifrado formados com o auxilio da chave secreta.

Neste caso o atacante procura uma mensagem específica, podendo ser um ficheiro de contabilidade, em que o intruso já sabe onde se localizam certos elementos como cabeçalhos, logótipos, etc., ou códigos fontes de aplicações em que o intruso sabe onde se encontra a assinatura da Organização, este elementos facilitam a dedução de certos pares texto em claro-texto cifrado [15].

4.6.1.3. Texto em claro escolhido

Neste caso o intruso tem acesso a:

- Algoritmo de encriptação;
- Texto cifrado para ser decriptado;
- Texto em claro escolhido pelo criptoanalista e em conjunto com o respectivo texto cifrado gerado pela sua chave secreta.

Neste caso o intruso introduz no sistema um texto em claro por si escolhido de modo que após encriptado ele capture o respectivo texto cifrado, deste modo ele obtém um texto em claro e o correspondente texto cifrado [15].

4.6.1.4. Texto cifrado escolhido

Neste caso o intruso tem acesso a:

- Algoritmo de encriptação;
- Texto cifrado para ser decriptado;
- Texto cifrado escolhido pelo criptoanalista e em conjunto com o respectivo texto em claro decriptado gerado pela sua chave secreta.

4.6.1.5. Texto escolhido

Neste caso o intruso tem acesso a:

- Algoritmo de encriptação;
- Texto cifrado para ser decriptado;
- Texto em claro escolhido pelo criptoanalista e em conjunto com o respectivo texto cifrado gerado pela sua chave secreta;
- Texto cifrado escolhido pelo criptoanalista e em conjunto com o respectivo texto em claro decriptado gerado pela sua chave secreta.

Estes últimos dois ataques não são muito comuns pois consistem em obter um texto em claro introduzindo no sistema um texto cifrado previamente capturado, o que é uma operação de difícil sucesso [15].

4.7. Criptografia Convencional

A Criptografia Convencional, que é também conhecida como *Encriptação Simétrica* ou *Encriptação da Chave Única*, foi o tipo de encriptação usada antes do desenvolvimento da Encriptação da Chave Pública. A Figura 22 ilustra o processo de Encriptação Convencional. A mensagem original, referida como *texto em claro*, é convertida para uma mensagem, aparentemente, sem sentido, referida como *texto cifrado*. O processo de Encriptação consiste em uma chave e um algoritmo. A chave é um valor independente do texto em claro. O algoritmo produz uma saída diferente dependendo da chave que é usada, isto é, mudando a chave estaremos mudando a saída do algoritmo.

Após a produção do texto cifrado este pode ser transmitido. Na recepção, o texto cifrado é, também, transformado para o texto original usando um algoritmo de Decriptação e a mesma chave usada na Encriptação [12].

4.7.1. Segurança da Encriptação Convencional

A segurança da Encriptação Convencional depende de vários factores, dentre eles:

- O algoritmo de encriptação deve ser forte o suficiente para que seja impossível decriptar a mensagem baseando-se apenas no texto cifrado.
- Além deste factor a segurança da Encriptação Convencional depende do secretismo da chave e não no secretismo do algoritmo, pois este pode ser conhecido.

Resumindo, assume-se que é impossível decifrar a mensagem baseando-se no texto cifrado e no conhecimento do algoritmo de encriptação e ou de decriptação. Em outras palavras, não precisamos manter o algoritmo em segredo mas é crucial manter a chave secreta, e é aqui que reside a grande desvantagem da Encriptação Convencional. O facto de que o algoritmo pode ser exposto sem prejudicar a segurança da Encriptação Convencional, faz com que a Encriptação Convencional seja mais usada. Pois o facto de não ser necessário manter o algoritmo secreto faz com que os produtores possam desenvolver chip´s que implementam um algoritmo de encriptação de dados a baixo custo. Esses chip´s são largamente usados em muitos produtos.

4.7.2. Princípios da Encriptação Convencional

O funcionamento da Encriptação Convencional é ilustrado na Figura 22, onde uma origem qualquer, que pode ser um computador ou um usuário, produz a mensagem em texto em claro, $X = [X_1, X_2, X_3, \ldots, X_M]$. Os M elementos de X são letras dum alfabeto finito qualquer. Tradicionalmente o alfabeto consiste de 26 letras. Nos dias de hoje usa-se muito o alfabeto binário {0,1} é muito usado. Para a encriptação, uma chave como $C = [C_1, C_2, C_3, \ldots, C_J]$ é gerada. Se a chave é gerada na origem da mensagem, então deve ser disponibilizada no destino através dum canal seguro. Uma outra alternativa seria que a chave fosse gerada por uma terceira entidade que iria difundi-la de forma segura para a origem e o destino [16].

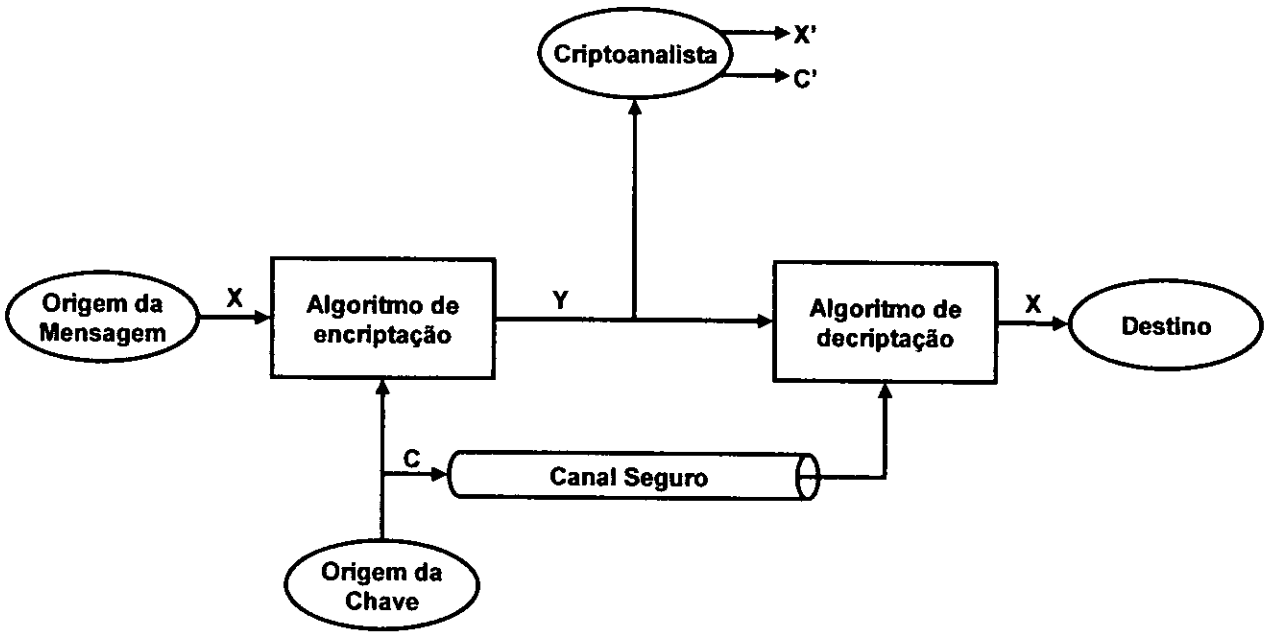


Figura 22 – Modelo do Criptosistema Convencional [16].

Com a mensagem X e a chave de encriptação C como entrada, o algoritmo de encriptação formaria o texto cifrado $Y = [Y_1, Y_2, Y_3, \ldots, Y_N]$, podemos escrever isto como:

$$Y = E_C(X) \qquad (1)$$

Esta notação indica que Y é produzido usando o algoritmo de encriptação E como uma função do texto em claro X, com a função específica determinada pelo valor da chave C. O suposto destinatário, na posse da chave, pode inverter a transformação:

$$X = D_C(Y) \qquad (2)$$

Um intruso, com acesso a Y mas não a X ou C, pode tentar obter ou X ou C. Assume-se que o intruso conheça o algoritmo de encriptação (E) e decriptação (D). Se o intruso estiver com interesse apenas naquela mensagem então o esforço deverá ser concentrado em recuperar X gerando um texto em claro estimado X'. Contudo, se o intruso estiver interessado em ler futuras mensagens, ele deverá tentar recuperar C gerando um C' estimado.

4.8. Criptografia da Chave Pública

Esta foi uma das grandes invenções no campo da Criptografia. A Criptografia da Chave Pública é baseada em Matemática em vez de operações de Permutação e Substituição como é o caso da Criptografia Convencional. Mais ainda, a criptografia da Chave Pública é assimétrica envolvendo o uso de duas chaves, em contraste com a Criptografia Convencional que usa uma chave apenas. Usando duas chaves conseguimos manter a confidencialidade, facilita a distribuição da chave e a autenticação.

Para discriminar entre os dois métodos criptográficos vamos referir a criptografia Convencional como da *Chave Secreta*. As duas chaves usadas na encriptação da Chave Pública serão referidas como *Chave Pública* e *Chave Privada*. Invariavelmente, a chave privada é guardada em segredo, mas é referida como *Chave Privada* em vez de *Chave Secreta* para evitar confusão com a encriptação Convencional [16].

4.8.1. Inovações dos Criptosistemas da Chave Pública

A criptografia de Chave Pública veio resolver o problema da distribuição da chave. Como se viu, a criptografia Convencional requer que os dois comunicantes [16]:

- Já partilhem a chave, que de alguma forma lhes foi distribuída;

- Tenham que usar um centro de Distribuição da Chave, o que de certa forma poderia comprometer o sistema.
- Outro problema está relacionado com as assinaturas digitais, pois se a criptografia era para se tornar abrangente não só para os serviços militares mas também para o Comércio e propósitos privados, então as mensagens e documentos electrónicos precisariam dum equivalente as assinaturas usadas num papel.

4.8.2. Princípios da Criptografia da Chave Pública

Algoritmos de Chave Pública baseiam-se em uma chave para encriptação e uma diferente, apesar de relacionada, para a decriptação. Esses algoritmos tem as seguintes características:

- É computacionalmente impraticável determinar a chave de decriptação tendo apenas o conhecimento acerca do algoritmo criptográfico e a chave de encriptação, e;
- Qualquer uma das chaves pode ser usada para a encriptação e a outra usada para a decriptação.

A Figura 23 ilustra o processo de encriptação da Chave Pública, cujos passos são:

1. Cada sistema final numa rede gera um par de chaves para serem usadas para a encriptação e decriptação de mensagens que irá receber;
2. Cada sistema publica a sua chave de encriptação colocando-a num registo ou ficheiro público. Esta é a chave pública. A outra chave é mantida em segredo.
3. Se A deseja enviar uma mensagem a B, ele encripta a mensagem com a chave pública de B;
4. Quando B recebe a mensagem, B decripta a mesma usando a sua chave privada. Nenhum outro interveniente poderá decriptar a mensagem pois só B conhece a chave privada de B.

Com esta aproximação, todos participantes tem acesso as chaves públicas, e chaves privadas são geradas localmente por cada participante e por isso não precisam de ser distribuídas. Enquanto um sistema controlar a sua chave privada, as suas comunicações estarão seguras. A qualquer momento o sistema pode mudar a sua chave privada e publicar a respectiva chave pública para substituir a antiga.

Vamos olhar pormenorizadamente os elemento essenciais da encriptação da chave pública, usando a Figura 23, existe uma origem A para uma mensagem a, que produz

uma mensagem em texto em claro, $X = [X_1, X_2, \ldots, X_M]$. Os M elementos de X são letras em algum alfabeto finito. A mensagem é destinada a um destino B, B gera um par de chaves relacionadas, uma chave pública, CP_b, e uma chave privada, CR_b. CR_b é conhecida apenas por B, onde CP_b é disposta publicamente e por isso acessível a A [16].

Com a mensagem X e a chave de encriptação CP_b como entrada, A forma o texto cifrado $Y = [Y_1, Y_2, \ldots, Y_N]$:

$$Y = E_{CPb}(X) \qquad (3)$$

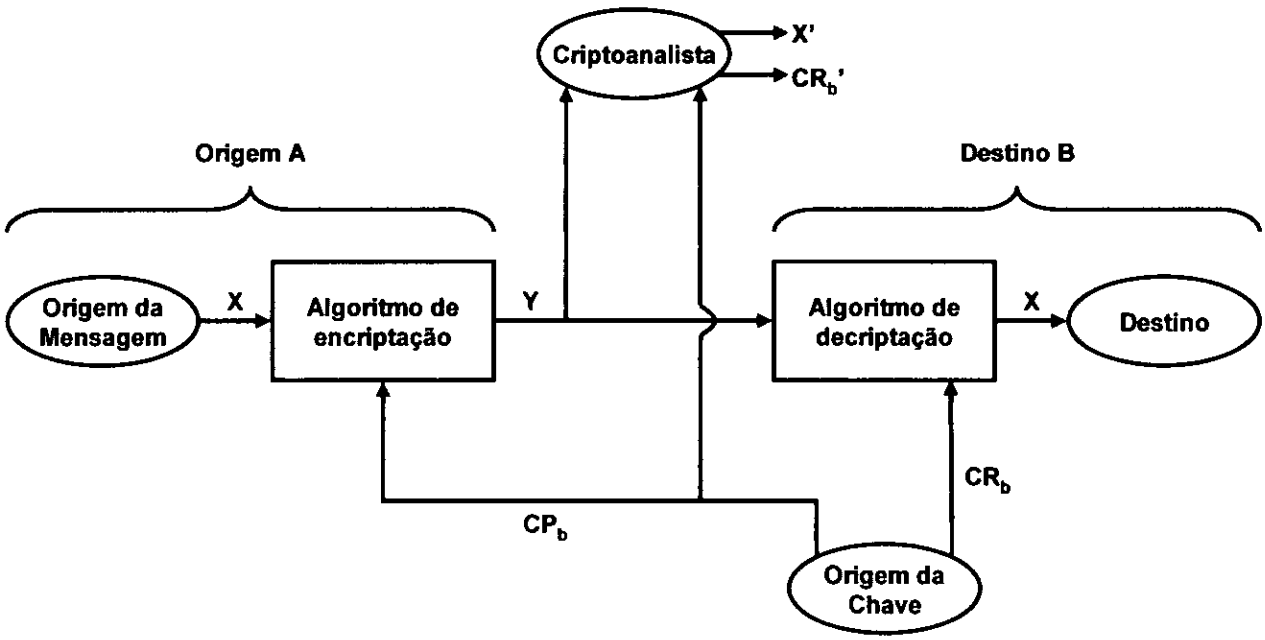


Figura 23 – Criptosistema da Chave Pública: Secretismo [16].

O respectivo receptor, possuindo a sua chave privada, poderá inverter a transformação:

$$X = D_{CRb}(Y) \qquad (4)$$

Um oponente, observando Y e tendo acesso a CP_b mas não a CR_b ou X, deve tentar obter CR_b e/ou X. É assumido que o intruso tem o conhecimento acerca do algoritmo de encriptação (E) e decriptação (D). Se o oponente está interessado apenas naquela mensagem, então o esforço será recuperar o X, gerando um texto em claro estimado X'. Contudo, geralmente o intruso esta interessado em ler futuras mensagens, e neste caso o esforço será obter CR_b, gerando o um CR_b' estimado.

Como se falou antes, tanto uma como outra chave pode ser usada para encriptar, com a outra sendo usada para encriptar, com a outra sendo usada para decriptação.

Enquanto o esquema da Figura 23 providencia confidencialidade o da Figura 24 providencia autenticação:

$$Y = E_{CRa}(X) \qquad (5)$$

$$X = E_{CPa}(Y) \qquad (6)$$

Neste caso, A prepara uma mensagem para B e encripta usando a chave privada de A antes de transmiti-la. B pode decriptar a mensagem usando a chave pública de A, porque a mensagem foi encriptada usando a chave privada de A, então só A poderia ter preparado a mensagem. Deste modo, toda mensagem encriptada serve como uma assinatura digital. Por outro lado, é impossível alterar a mensagem sem o acesso a chave privada de A, então a mensagem é autêntica em termos da **origem** e da **integridade da informação** [16].

No esquema precedente, toda mensagem é encriptada, o que apesar de validar ambos, o autor e o conteúdo, requer um grande esforço de armazenamento. Cada documento deve ser guardado em texto em claro para ser usado em propósitos práticos. Uma cópia deve ser em texto cifrado de modo que a origem e o conteúdo possam ser verificados em caso de discórdia. Uma forma mais eficaz de o fazer é de encriptar um bloco pequeno de bits que é uma função do documento. Esse bloco, denominado *autenticador*, deve possuir a propriedade de que é impraticável mudar o documento sem mudar o autenticador. Se o autenticador é encriptado com a chave privada do emissor, serve de assinatura que verifica a origem, conteúdo e sequenciamento.

É importante realçar que o processo de encriptação descrito não providencia confidencialidade, isto é, a mensagem a ser enviada esta segura contra alteração, mas não contra a escuta. Isto é óbvio no caso da assinatura digital baseada em uma porção da mensagem, pois o resto da mensagem é transmitido normalmente. Mesmo no caso da encriptação completa, como mostrado na Figura 24, não há protecção contra confidencialidade, porque qualquer oponente pode decriptar a mensagem usando a chave pública do emissor.

É, contudo, possível providenciar ambos a função de autenticação e confidencialidade pelo duplo uso do esquema de chave pública, Figura 25:

$$Z = E_{CPb}[E_{CRa}(X)] \qquad (7)$$

$$X = D_{CPa}[D_{CRb}(Z)] \qquad (8)$$

Neste caso, começamos como anteriormente encriptando uma mensagem, usando a chave privada do emissor, isto providencia **assinatura digital**. Em seguida, encripta-se, de novo, usando a chave pública do receptor. O texto cifrado final só pode ser decriptado pelo respectivo receptor, que sozinho possui a respectiva chave privada, assim, a confidencialidade é providenciada. A desvantagem deste método é que o algoritmo da Chave Pública, que é complexo, deve ser executado quatro vezes, em vez de duas, em cada comunicação [16].

4.8.3. Aplicação de criptosistemas de Chave Pública

Sistemas de chave pública são caracterizados pelo uso de um tipo de algoritmo criptográfico com duas chaves, uma privada e outra pública. Dependendo da aplicação, o emissor usa tanto a chave privada do emissor ou a chave pública do receptor, ou ambas, para executar algum tipo de função criptográfica.

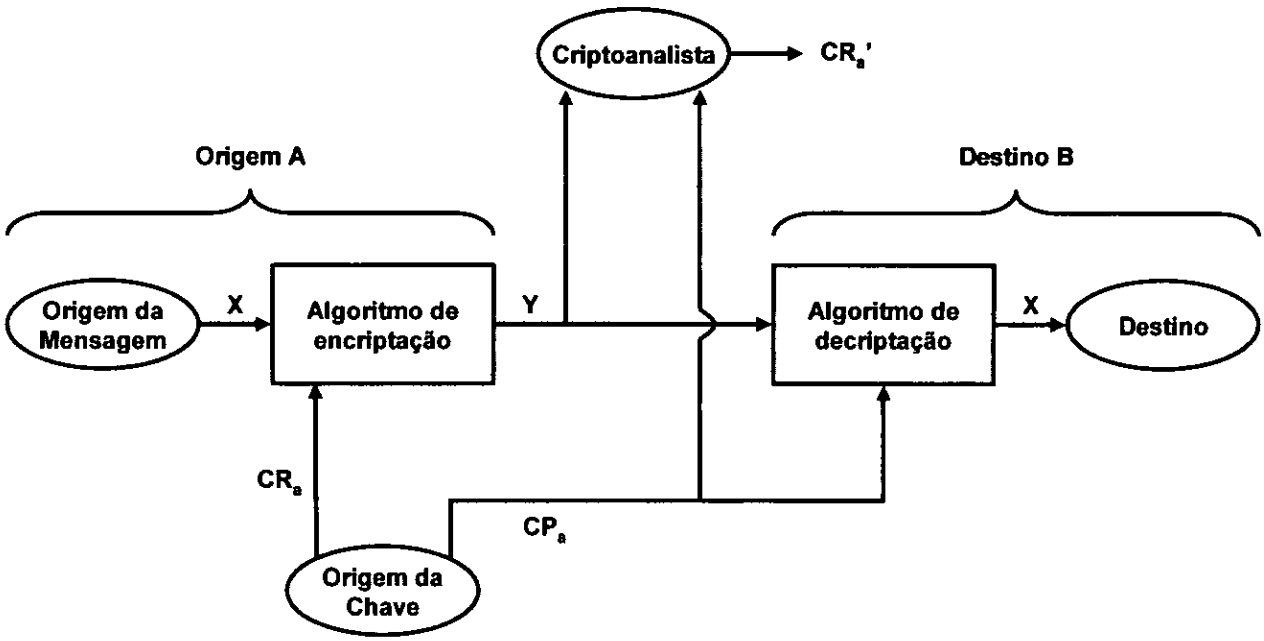


Figura 24 – Criptosistema da Chave Pública: Autenticação [16].

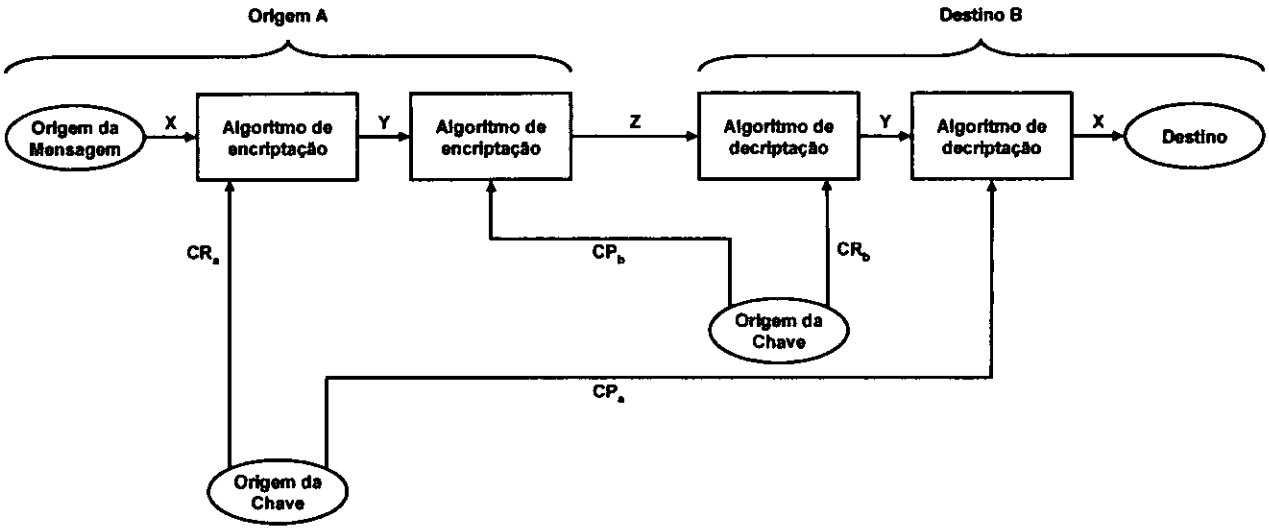


Figura 25 – Criptosistema da Chave Pública: Secretismo e Autenticação [16].

Em termos mais simples, podemos classificar os criptosistemas de chave pública em 3 categorias:

- **Encriptação/Decriptação:** o emissor encripta uma mensagem com a chave pública do destinatário;
- **Assinatura digital:** o emissor assina a mensagem com a sua chave privada. Assinando é conseguido através dum algoritmo criptográfico aplicado a mensagem ou a um pequeno bloco de dados que é uma função da mensagem;
- **Troca de chave:** duas partes cooperam para trocar a chave da sessão. Existem muitas formas de o fazer, envolvendo a chave privada de um ou ambas partes.

Em alguns algoritmos aplicam-se todas funcionalidades, enquanto que em outros só se aplica um ou dois. A Tabela 3 indica as aplicações de alguns algoritmos Assimétricos:

Algoritmo	Encriptação/Decriptação	Assinatura digital	Troca de chave
RSA	Sim	Sim	Sim
DSS	Não	Sim	Não
Diffie-Hellman	Não	Não	Sim

Tabela 3 – Funcionalidades de alguns Algoritmos de Chave Pública [15].

4.8.4. Requisitos da criptografia de chave pública

O criptosistema da Figura 23 depende dum algoritmo criptográfico baseado em duas chaves relacionadas. Diffie e Helman postularam que é computacionalmente:

1. Fácil para uma parte B gerar um par (chave pública CP_b, chave privada CR_b);
2. Fácil para um emissor A, conhecendo a chave pública e a mensagem a ser encriptada, X, gerar o texto cifrado correspondente:

$$Y = E_{CPb}(X) \qquad (9)$$

3. Fácil um receptor B decriptar o texto cifrado resultante usando a chave privada para recuperar a mensagem original:

$$X = D_{CRb}(Y) = D_{CRb}[E_{CPb}(X)] \qquad (10)$$

4. Impraticável para um intruso, conhecendo a chave pública, CP_b, determinar a chave privada CR_b;
5. Impraticável para um intruso, conhecendo a chave pública, CP_b, e um texto cifrado, Y, recuperar a mensagem original, X;

A estes postulados pode-se acrescentar:

6. A encriptação e decriptação podem ser aplicadas nas duas ordens:

$$X = E_{CPb}\,[D_{CRb}(X)] \qquad (11)$$

4.8.5. Criptoanálise de Chave Pública

Como na Encriptação Convencional, o esquema da Encriptação de Chave Pública é vulnerável ao ataque da Força-Bruta. A contramedida é a mesma: *usar chaves longas.* Contudo, existe um factor a ser considerado. Os sistemas de Chave Pública dependem do uso de algum tipo de função Matemática inversível. A complexidade no cálculo dessas funções pode não ser escaladas linearmente com o número de bits da chave, mas crescem mais rapidamente que isso. Assim, o tamanho da chave deve ser largo o suficiente para tornar o ataque de Força-Bruta impraticável, mas pequeno o suficiente para que a encriptação e decriptação seja praticável. Na prática, os tamanhos de chave propostos tornam o ataque de Força-Bruta impraticável mas resulta em velocidades de encriptação e decriptação muito pequenas para o uso geral. Apesar do que se disse antes, a encriptação da chave pública é correntemente confinada a aplicações de Gestão da chave e assinatura [16].

Outra forma de ataque é tentar encontrar a chave privada sendo dado a chave pública até hoje não foi provado que este tipo de ataque é praticável para um algoritmo de chave pública. Mesmo assim, qualquer algoritmo, incluindo o RSA, é suspeito.

Finalmente, há um ataque que é peculiar aos sistemas de chave pública. Isto é, provavelmente um ataque de mensagem. Suponha, que uma mensagem que esta a ser enviada consiste apenas em uma chave DES de 56 bits. Um intruso pode encriptar todas as chaves possíveis usando a chave pública e poderia decifrar qualquer mensagem correspondendo o texto cifrado transmitido. Assim, não importa o tamanho da chave do esquema da chave pública, o ataque é reduzido a um ataque de Força-

Bruta em uma chave de 56 bits. Este ataque pode ser contrariado acrescentando alguns bits arbitrários as mensagens.

4.9. Técnicas Clássicas de Encriptação Convencional

4.9.1. Substituição

Consiste em substituir as letras por outras, números ou símbolos. Se o texto em claro é visto como uma sequência de bits, então a substituição envolve a troca dum conjunto de bits do texto em claro por bits do texto cifrado.

4.9.1.1. Cifra de César

Um dos primeiros e mais simples métodos de encriptação usando a técnica de substituição foi à de Julios César, que consistia em substituir uma letra do alfabeto pela terceira letra que o precede [16].

Deste modo teríamos:

Claro: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cifra: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Se atribuirmos um valor numérico a cada letra (a=0, b=1, ..., z=25), então podemos expressar este algoritmo matematicamente da seguinte forma:

$$Y = E(X) = (X + 3) \text{ Mod } 26 \qquad (12)$$

Podemos, ainda, generalizar este algoritmo, para C deslocações:

$$Y = E(X) = (X + C) \text{ Mod } 26 \qquad (13)$$

Onde: C = 1 .. 25

Deste modo o algoritmo de decriptação seria é:

$$X = D(Y) = (Y - C + 26) \text{ Mod } 26 \qquad (14)$$

Para o caso da criptoanálise, se conhecer que o Texto cifrado foi obtido usando esta técnica, então o intruso deve tentar as 25 chaves possíveis (ver Tabela 4).

	Texto cifrado
Chave	**TIZGKFXIRWZR TFEMVETZFERC**
1	SHYFJEWHQVYQ SEDLUDSYEDQB
2	RGXEIDVGPUXP RDCKTCRXDCPA
3	QFWDHCUFOTWO QCBJSBQWCBOZ
4	PEVCGBTENSVN PBAIRAPVBANY
5	ODUBFASDMRUM OAZHQZOUAZMX
6	NCTAEZRCLQTL NZYGPYNTZYLW
7	MBSZDYQBKPSK MYXFOXMSYXKV
8	LARYCXPAJORJ LXWENWLRXWJU
9	KZQXBWOZINQI KWVDMVKQWVIT
10	JYPWAVNYHMPH JVUCLUJPVUHS
11	IXOVZUMXGLOG IUTBKTIOUTGR
12	HWNUYTLWFKNF HTSAJSHNTSFQ
13	GVMTXSKVEJME GSRZIRGMSREP
14	FULSWRJUDILD FRQYHQFLRQDO
15	ETKRVQITCHKC EQPXGPEKQPCN
16	DSJQUPHSBGJB DPOWFODJPOBM
17	**CRIPTOGRAFIA CONVENCIONAL**
18	BQHOSNFQZEHZ BNMUDMBHNMZK
19	APGNRMEPYDGY AMLTCLAGMLYJ
20	ZOFMQLDOXCFX ZLKSBKZFLKXI
21	YNELPKCNWBEW YKJRAJYEKJWH
22	XMDKOJBMVADV XJIQZIXDJIVG
23	WLCJNIALUZCU WIHPYHWCIHUF
24	VKBIMHZKTYBT VHGOXGVBHGTE
25	UJAHLGYJSXAS UGFNWFUAGFSD

Tabela 4 – Criptoanálise na Cifra de César.

Este algoritmo possui três principais características que nos permitam usar o ataque Força-Bruta, nomeadamente:

1. Os algoritmos de encriptação e decriptação são conhecidos;
2. O número de chaves possíveis é reduzido, apenas 25;
3. A língua do texto em claro é conhecida e facilmente reconhecida.

De salientar que, na maior parte das vezes os algoritmos de encriptação e decriptação são conhecidos.

4.9.1.2. Encriptação Monoalfabética

Com 25 chaves possíveis o algoritmo de César não é seguro. Uma melhor segurança pode ser obtida efectuando uma substituição arbitrária, neste caso a linha poderia ser qualquer permutação das 26 letras, assim teríamos 26! Ou melhor maior que $4 * 10^{26}$ chaves possíveis.

Para este caso existe outra forma de ataque, se por um lado o intruso conhecer a língua do texto em claro, por exemplo em Português, ele poderá explorar a regularidade da língua. Este processo consiste em analisar a frequência de cada letra do texto cifrado e compara-la com a frequência das letras da suposta língua, neste caso a Portuguesa. Após esta correspondência analisa-se as palavras resultantes para ver se são legíveis. De referir que, esta análise pode ser também feita não só a letras mas também a palavras.

As cifras monoalfabéticas são fáceis de quebrar pois elas deixam transparecer a frequência das letras do alfabeto original, uma medida de prevenção para este tipo de ataque, é providenciar substituições múltiplas, conhecidas como homófonos, para cada letra. Por exemplo, uma letra "e" pode possuir cifras como 9, 76, 10 e 12, em que cada homófono é usado de forma relativa ou arbitrária [1].

4.9.1.3. Cifra Playfair

Esta é conhecida como a melhor encriptação de letra múltipla, que consiste em tratar o texto em claro como unidades simples e traduzi-las em diagramas de texto cifrado.

Este algoritmo baseia-se no uso de uma matriz quadrada de ordem 5 constituída por letras e usando uma chave ou uma palavra-chave.

Esta matriz é preenchida da esquerda para a direita e de cima para baixo, primeiro introduz-se a chave, sem elementos duplicados, e depois as restantes letras do alfabeto. As letras I e J são colocadas na mesma célula.

4.9.1.3.1. Encriptação

O texto em claro é encriptado duas letras de cada vez, isto é, aos pares, de acordo com as seguintes regras [16]:

- As letras repetidas do texto em claro que iriam gerar um par de cifras também iguais, são substituídas por uma letra pouco frequente como um x, por exemplo;
- As letras do texto em claro que figuram na mesma linha da matriz são substituídas pela respectiva letra a direita, com o primeiro elemento seguido, circularmente, o último;
- As letras do texto em claro que caem na mesma coluna são substituídas pela exactamente abaixo, com o primeiro seguido circularmente do último;
- Nos restantes casos, cada letra do texto em claro é substituída por outra que se situa na própria linha e na coluna da outra letra e vice-versa.

A Cifra Playfair é considerada mais um avanço face as cifra monoalfabéticas, isto é, como são 26 letras então teremos 26 x 26 = 676. Deste modo a identificação dos diagramas é difícil. Além do que, as frequências relativas das letras possuem um intervalo maior que os diagramas, fazendo com que a análise das frequências seja mais difícil. Por esta razão este algoritmo foi por muito tempo considerado inquebrável. Na verdade este algoritmo é fácil de quebrar pois sobrevive grande parte do texto em claro intacto. Uma forma de quebrar as cifras do playfair é demonstrado abaixo (ver Gráfico 1). Temos uma linha do texto em claro que representa a distribuição de frequências de mais de 70.000 caracteres alfabéticos do artigo sobre a criptografia da enciclopédia inglesa. Esta distribuição de frequências é também a frequência de qualquer cifra da substituição monoalfabéticas [16].

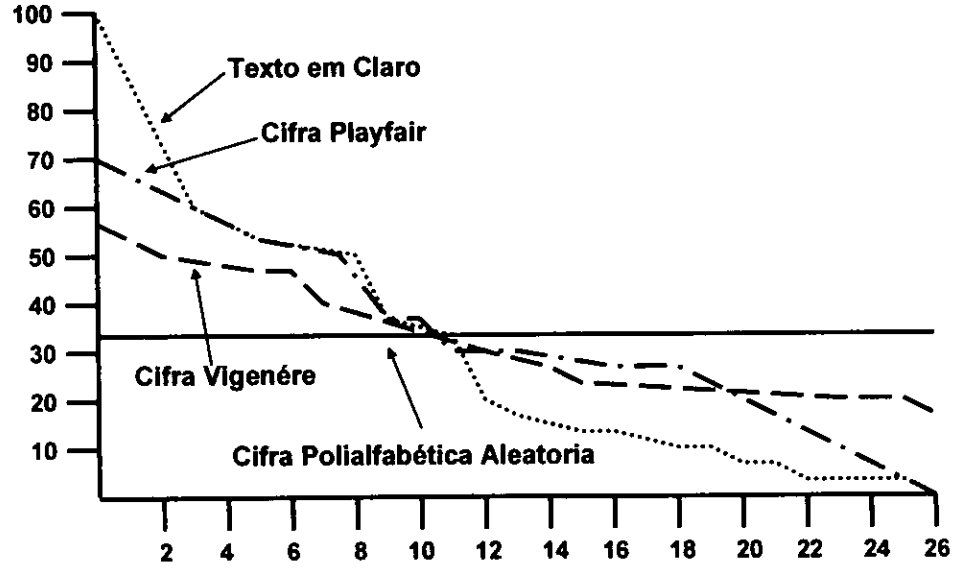


Gráfico 1 – Frequência Relativa da Ocorrência das Letras no Alfabeto Inglês [16].

O Gráfico 1 foi produzido da seguinte forma: o número de ocorrências da cada letra foi contado e dividido pelo número de ocorrências da letra "e" a mais frequente no alfabeto Inglês. Como resultado a letra "e" tem uma frequência de 1, "t" de 0.76 e assim por diante. Os pontos do eixo horizontal correspondem as letras na ordem decrescente da frequência. O Gráfico 1 mostra também a distribuição de frequências dos resultados quando o texto é encriptado usando a *Cifra Playfair*. Para normalizar o Gráfico o número de ocorrências de cada letra do texto cifrado é, outra vez, dividido pelo número de ocorrências da letra "e" no texto em claro. O Gráfico 1 mostra, também, a extensão de como a distribuição de frequências das letras, o que faz com que seja trivial resolver cifras de substituição, é mascarada pela encriptação.

Como se pode notar pelo Gráfico a linha da distribuição de frequências da cifra Playfair é estreita comparativamente a do texto em claro.

4.9.1.4. Cifra Hill

Outro algoritmo multiletra é a de Hill, desenvolvido pelo matemático Lester Hill em 1929.

4.9.1.4.1. Encriptação

No algoritmo de encriptação todas m sucessivas letras do texto em claro são substituídas por m letras do texto cifrado. A substituição é determinada por m equações lineares onde a cada carácter é atribuído um valor numérico (a=0, b=1, ..., z=25). Para m=3, o sistema seria:

$$Y_1 = (C_{11}X_1 + C_{12}X_2 + C_{13}X_3) \text{ Mod } 26 \qquad (15)$$

$$Y_2 = (C_{21}X_1 + C_{22}X_2 + C_{23}X_3) \text{ Mod } 26 \qquad (16)$$

$$Y_3 = (C_{31}X_1 + C_{32}X_2 + C_{33}X_3) \text{ Mod } 26 \qquad (17)$$

Em colunas teríamos:

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} x \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} \qquad (18)$$

ou

$$Y = CX \qquad (19)$$

Onde:

- **Y** e **X** são colunas de tamanho 3, representando o texto cifrado e o texto em claro;
- **C** é uma matriz quadrada de ordem 3 representando a chave;
- Uma operação que se usa neste algoritmo é o **Mod 26**.

Exemplo: Vamos considerar o texto em claro "criptografia" com a chave de encriptação:

$$C = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 17 \end{pmatrix} \qquad (20)$$

As primeiras três letras do texto em claro são representadas pelo vector-coluna (2 17 8) de acordo com a enumeração das letras do alfabeto, então:

$$C \begin{pmatrix} 2 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 312 \\ 462 \\ 168 \end{pmatrix} \text{ Mod } 26 = \begin{pmatrix} 0 \\ 20 \\ 12 \end{pmatrix} = \text{aum} \qquad (21)$$

Continuando assim, o texto cifrado seria "aumypubqunpa".

4.9.1.4.2. Decriptação

A decriptação requer o uso da matriz inversa de k. O inverso k^{-1} da matriz k é obtida pela equação $CC^{-1} = C^{-1}C = I^1$. Neste caso a matriz inversa é:

$$C^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \qquad (22)$$

Assim:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 17 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \text{ Mod } 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (23)$$

É visível que quando a matriz C^{-1} é aplicada ao texto cifrado, então o texto em claro é obtido.

4.9.1.5. Cifra Polialfabéticas

Outra forma de melhorar a técnica das cifras monoalfabéticas é de usar substituições monoalfabéticas diferentes de acordo com a mensagem do texto em claro. Todas as técnicas possuem as seguintes regras em comum:

- Um conjunto de regras de substituições monoalfabéticas relacionadas é usado, e;
- Uma chave determina qual das chaves é usada.

Para uma dada transformação o melhor, e mais simples, algoritmo deste género é a *Cifra de Vigenère*. Neste caso, o conjunto de regras de substituição monoalfabéticas consiste nas 26 cifras de César com de 0 a 25. Cada cifra é denotada por uma letra da chave, que é a cifra que substitui a letra do texto em claro "a". A cifra de César com deslocação 3 é denotada pelo calor da chave "d". Para demonstrar melhor este algoritmo veja a Tabela 5 conhecida como *Tabela de Vigenère*. Cada uma das 26 cifras é colocada horizontalmente com a letra da chave de cada cifra a esquerda. O alfabeto normal é colocado acima [16].

4.9.1.5.1. Encriptação

Sendo dado uma letra de chave C e uma letra do texto em claro X, a letra do texto cifrado será a intersecção da linha C com a coluna X neste caso obteremos Y.

[1] Matriz identidade em que todos os elementos são iguais a zero com a excepção dos da diagonal principal que são iguais a um.

Para encriptar uma mensagem é necessário uma chave do mesmo tamanho que a mensagem, isto é alcançado se repetirmos a palavra-chave quantas vezes o necessário.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabela 5 – A Tabela de Vigenère [16].

4.9.1.5.2. Decriptação

A decriptação é igualmente simples:

- Primeiro procuramos a linha da letra da chave, depois no topo da coluna onde se encontra a letra do texto cifrado é correspondente a letra do texto em claro.

A força desta cifra é que existem múltiplas letras do texto cifrado para cada letra do texto em claro. Deste modo, a frequência das letras é ocultada. Contudo, nem toda a informação da estrutura do texto em claro é perdida. Por exemplo, o Gráfico 1 mostra a Cifra de Vigenère com uma palavra-chave de tamanho 9. Como se vê um melhoramento é conseguido em relação a cifra Playfair, mas ainda existe uma considerável informação sobre a frequência.

Para quebrar esta cifra primeiro vamos supor que o intruso sabe que a cifra foi obtida usando uma substituição monoalfabética ou uma de Vigenère. Um teste simples pode ser feito para efectuar uma determinação. Se uma substituição monoalfabética é usada, então as propriedades estatísticas do texto cifrado deverá ser igual a da linguagem do texto cifrado. Se apenas estiver disponível uma simples mensagem para a análise, não se deve esperar uma correspondência exacta dessa pequena amostra com o *profile* estatístico da língua do texto em claro. Contudo, se é conseguido uma correspondência, podemos assumir uma substituição monoalfabética. Se, por outro lado uma cifra de Vigenère é suspeita, então o progresso depende da determinação do tamanho da palavra-chave.

Se duas sequências idênticas de letras do texto em claro ocorrem numa distância que é um múltiplo inteiro do tamanho da palavra-chave elas iriam criar cifras idênticas. Claro que nem todos trechos de texto cifrado iguais significam palavras de texto em claro iguais e encriptado com a mesma chave. Contudo, se a mensagem for longa o suficiente, irão haver um número suficiente de sequências de cifras repetidas. Resumindo, analisando os factores comuns procurando as várias sequências, o analista poderá descobrir o tamanho da palavra-chave. Se o tamanho de uma palavra-chave é N, então a cifra, consistirá de N cifras de substituição monoalfabéticas. Deste modo, podemos usar as frequências características conhecidas da mensagem texto em claro para atacar cada uma das cifras monoalfabéticas separadamente. A natureza periódica da palavra-chave pode ser eliminada usando uma palavra-chave sem repetições que seja do mesmo tamanho que a mensagem. Vigenère propôs o que chamou de *sistema de autochave*, em que uma palavra-chave é concatenada com o

próprio texto em claro para providenciar uma chave. Mesmo esta teoria é vulnerável a criptoanálise. Pois a chave e o texto em claro partilham a mesma distribuição de frequências das letras, por isso podemos usar uma técnica estatística [16].

Uma outra técnica que pode ser usada é escolher uma chave que não possui nenhuma relação estatística com o texto em claro. Este sistema funciona com dados binários em vez de letras. O sistema pode ser expressado da seguinte forma:

$$y_i = x_i \oplus c_i \qquad (24)$$

Onde:

y_i - lésima letra do texto cifrado;

x_i - lésima letra do texto em claro;

c_i - lésima letra da chave;

$\oplus$ - Operação OU-Exclusivo (XOR).

Como a cifra é gerada efectuando a operação XOR do texto em claro e da chave. Devido as propriedades do XOR, a decriptação simplesmente envolve a mesma operação lógica binária:

$$x_i = y_i \oplus c_i \qquad (25)$$

O essencial desta técnica é o meio de construção da chave. Vernam propôs o uso dum ciclo que repeti-se a chave até que a mesma alcança o tamanho do texto em claro, deste modo iríamos obter uma chave comprida. Mas apesar de a chave longa dificultar a criptoanálise, esta técnica não é eficaz pois com cifras suficientes podemos detectar as sequências repetidas.

Um militar, Mauborgne, propôs uma melhoria na Cifra de Vernam, que consistia no uso de uma chave aleatória, sem repetições, que ficou conhecida como a técnica one-time pad. O que iria produzir cifras sem relação estatística com o texto em claro, e por isso as cifras seriam inquebráveis. O único problema desta técnica é que o receptor e o emissor devem partilhar e proteger a chave, o que é difícil pois ela é gerada aleatoriamente [16].

4.9.2. Técnicas de transposição

As técnicas acima vistas são constituídas por substituições dum símbolo de cifra por um símbolo do texto em claro. Um diferente tipo de mapeamento é conseguido efectuando várias permutações das letras do texto em claro. Esta técnica é conhecida como a técnica da transposição. O mais simples algoritmo deste género é a do Rail

Force, em que o texto em claro é escrito como uma sequência de diagonais e lido como uma sequência de linhas.

Exemplo:

C I T G A I
R P O R F A

A mensagem encriptada seria:

CITGAIRPORFA

Este tipo de operação seria fácil de quebrar. Um esquema mais complexo é escrever a mensagem num rectângulo, linha por linha, e ler a mensagem coluna por coluna, mas permutando a ordem das colunas. A ordem das colunas será a chave do algoritmo. Por exemplo:

Chave: 4 3 1 2 5 6 7
Texto em claro: e s p e r e m
o p e l o t i
r o p a r a a
t a c a r e m
Texto cifrado: pepcelaaspoaeortrorretaemiam

A técnica da transposição é facilmente identificada pois a frequência das letras do texto cifrado é o mesmo do texto em claro. Para o tipo de transposição colunar efectuada acima, a criptoanálise é directa e envolve a colocação do texto cifrado numa matriz e tentando várias combinações das colunas. A tabela de frequências de diagramas e trigramas podem ser úteis. A cifra da transposição pode ser segura efectuando mais do que uma transposição. O resultado será uma permutação mais complexa que não é fácil reconstruir [16]. Deste modo, se a mensagem for encriptada usando o mesmo algoritmo teríamos, por exemplo:

Chave: 4 3 1 2 5 6 7
Texto em claro: p e p c e l a
a s p o a e o
r t r o r r e
t a e m i a m
Texto cifrado: partestapprecoomearileraaoem

Para visualizar o resultado desta dupla transposição, designando as letras na mensagem original por número que representam a posição. Com 28 letras na mensagem, teríamos:

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

Após a primeira transposição:

03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

Que possui uma estrutura regular, depois da segunda transposição, teríamos:

17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28

É uma permutação menos estruturada que é mais difícil de quebrar.

4.9.2.1. Máquinas rotoras

O exemplo agora dado sugere que múltiplos estágios de encriptação podem produzir um algoritmo que é significamente mais difícil de quebrar. Usando as cifras de substituição com as cifras de transposição antes da introdução do algoritmo DES, a mais importante aplicação dos princípios dos estágios de encriptação múltipla era um sistema conhecido como máquinas motoras.

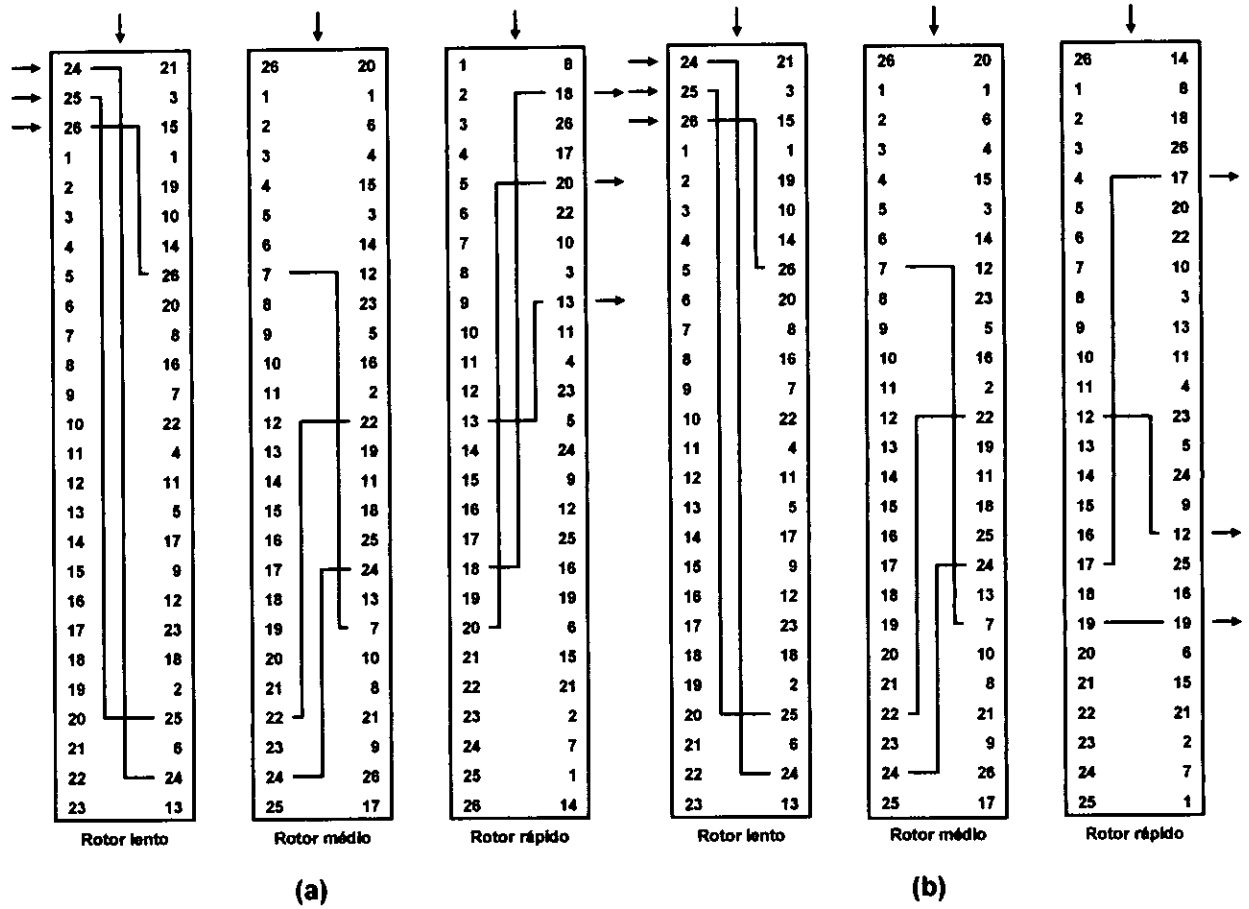


Figura 26 – Máquina Rotora (com 3 rotores): (a) Estado Inicial (b) Estado após pressionada uma tecla [16].

Este tipo de máquina é constituído por um conjunto de cilindros rotativos independentes por onde fluem fluxos electrónicos. Cada cilindro possui 26 pinos de entrada e 26 de saída, com conexões internas que ligam cada entrada a uma única saída. Para simplificar apenas três cilindros forma ilustrados na Figura 26.

Se associarmos cada pino de entrada e saída à uma letra do alfabeto então cada cilindro define uma substituição monoalfabética, no exemplo se um usuário pressiona a tecla da letra "A" um sinal eléctrico é aplicado ao 1º pino do primeiro cilindro que flui pela conexão interna para o 25º pino de saída.

Considerada uma máquina com um único cilindro. Após cada tecla ser pressionada o cilindro roda uma posição de modo que as ligações internas são trocadas de acordo. Assim, diferentes cifras de substituições monoalfabéticas são definidas. Após 26 letras do texto em claro, o cilindro regressa a posição inicial. Assim teríamos um algoritmo de substituição polialfabética de período 26. Um sistema de cilindro único não oferece muita segurança. O poder das máquinas rotoras esta no uso de cilindros múltiplos onde os pinos de output estão ligados aos pinos de entrada do próximo. A Figura 26

mostra um sistema de três cilindros. A Figura 26 (a) mostra a posição em como a entrada do primeiro pino (letra "A" do texto em claro) é conduzido pelos três cilindros e aparece na saída do segundo pino (letra "B" do texto cifrado) [16].

Com cilindros múltiplos, o cilindro mais longe do da entrada roda uma posição do pino após uma pressão. A Figura 26 (b) mostra o sistema após uma pressão. Após cada rotação completa do cilindro mais longe o do meio roda uma posição também e por cada volta completa do cilindro do meio o primeiro roda uma vez também. Este é o mesmo tipo de operação que ocorre no odómetro. O resultado é que existem 26 x 26 x 26 = 17576 diferentes substituições alfabéticas usadas antes que o sistema se repita. Adicionando um 4º ou 5º cilindro teríamos períodos de 456976 e 11881376 letras respectivamente.

Hoje em dia o princípio da máquina rotora encontra-se implementado no algoritmo DES.

4.10. Técnicas Modernas de Encriptação Convencional

4.10.1. DES (Data Encription Algoritm)

Este é o algoritmo mais usado e foi adoptado em 1977 pela IBM. No DES, os dados são encriptados em blocos de 64 bits usando uma chave de 56 bits. O algoritmo transforma 64 bits de entrada e após uma série de passos nos fornece uma saída de 64 bits. Os mesmos passos, com a mesma chave, são usados na decriptação.

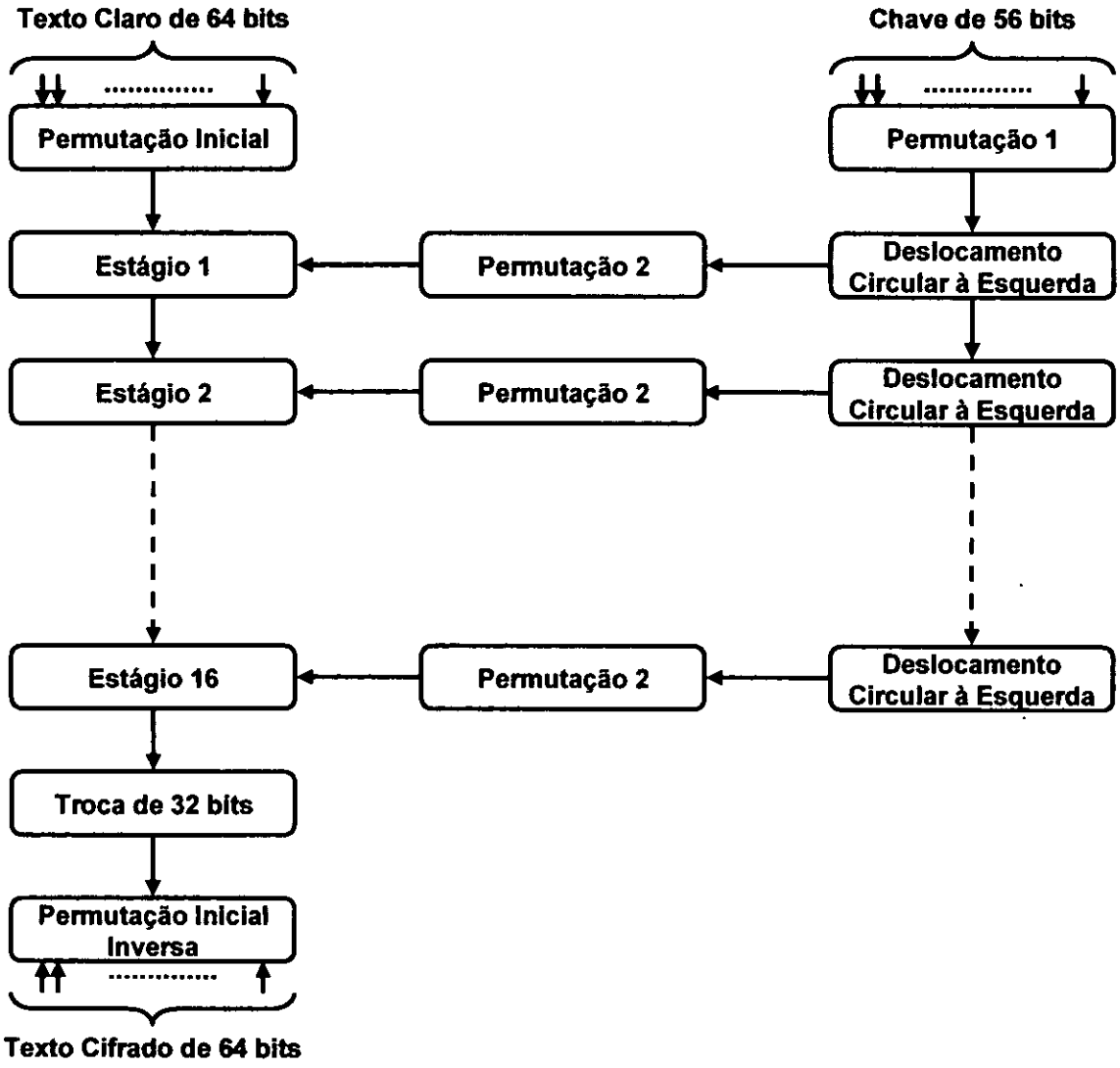


Figura 27 – Algoritmo de Encriptação DES [16].

4.10.1.1. Encriptação

A Figura 27 ilustra o esquema de encriptação DES. Como todos esquemas de encriptação, existem duas entradas para o DES: o texto em claro para ser encriptado e a chave. Neste caso, o texto em claro tem um tamanho de 64 bits e a chave tem um tamanho de 56 bits. Como se pode ver pela parte esquerda da Figura 27 o processamento do texto em claro é feito em três fases, nomeadamente [16]:

1. O texto em claro de 64 bits passa por uma Permutação Inicial (PI) que rearranja os bits para produzir a entrada permutada;
2. Em seguida ocorre uma fase composta por 16 estágios da mesma função, que envolve funções de permutação e substituição. A saída do último estágio consiste de 64 bits que é uma função de entrada do texto em claro e da chave. As metades, esquerda e direita, da saída são trocadas para produzir a *pré-saída*;

3. Finalmente a pré-saída passa por uma permutação (PI^{-1}), que é inversa a PI, para produzir o texto cifrado de 64 bits.

Com excepção da Permutação Inicial e Final, o DES possui uma estrutura idêntica a da Cifra de Fiestel (ver ANEXO D). Na parte direita da Figura 27 é ilustrada a forma como a chave de 56 bits é usada. Inicialmente, a chave passa por uma função de permutação. Após isto, para cada um dos estágios uma chave C_i é produzida através da combinação duma deslocação circular à esquerda e uma permutação. A permutação é a mesma para cada estágio, mas uma diferente subchave é produzida devido as repetidas interacções dos bits da chave.

(a) Permutação Inicial (PI)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Permutação Inicial Inversa (PI^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(c) Expansão/Permutação (E/P)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Função de Permutação (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Tabela 6 – Tabelas de permutações do DES [16].

4.10.1.1.1. Permutação Inicial (PI)

A PI e a sua inversa, PI^{-1}, são definidas pelas Tabelas 6 (a) e (b). Para testar que PI^{-1} é inversa de PI, considere o exemplo abaixo onde temos uma entrada M de 64 bits:

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Onde M_i é um digito binário. Então, a permutação X = PI(M) é a seguinte:

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

Se após isto usarmos a permutação inversa $Y = PI^{-1}(X) = PI^{-1}(PI(M))$, podemos ver que a ordem original é restabelecida.

4.10.1.1.2. Detalhes dum Estágio

A Figura 28 mostra a estrutura da função do estágio. Começando pela parte esquerda do diagrama. A metade esquerda e direita de cada valor intermediário de 64 bits são tratadas em quantidades separadas de 32 bits, denominados E e D [16]. Deste modo, podemos generalizar o processo de estágio:

$$E_i = D_{i-1} \qquad (26)$$

$$D_i = E_{i-1} \oplus F(D_{i-1}, C_i) \qquad (27)$$

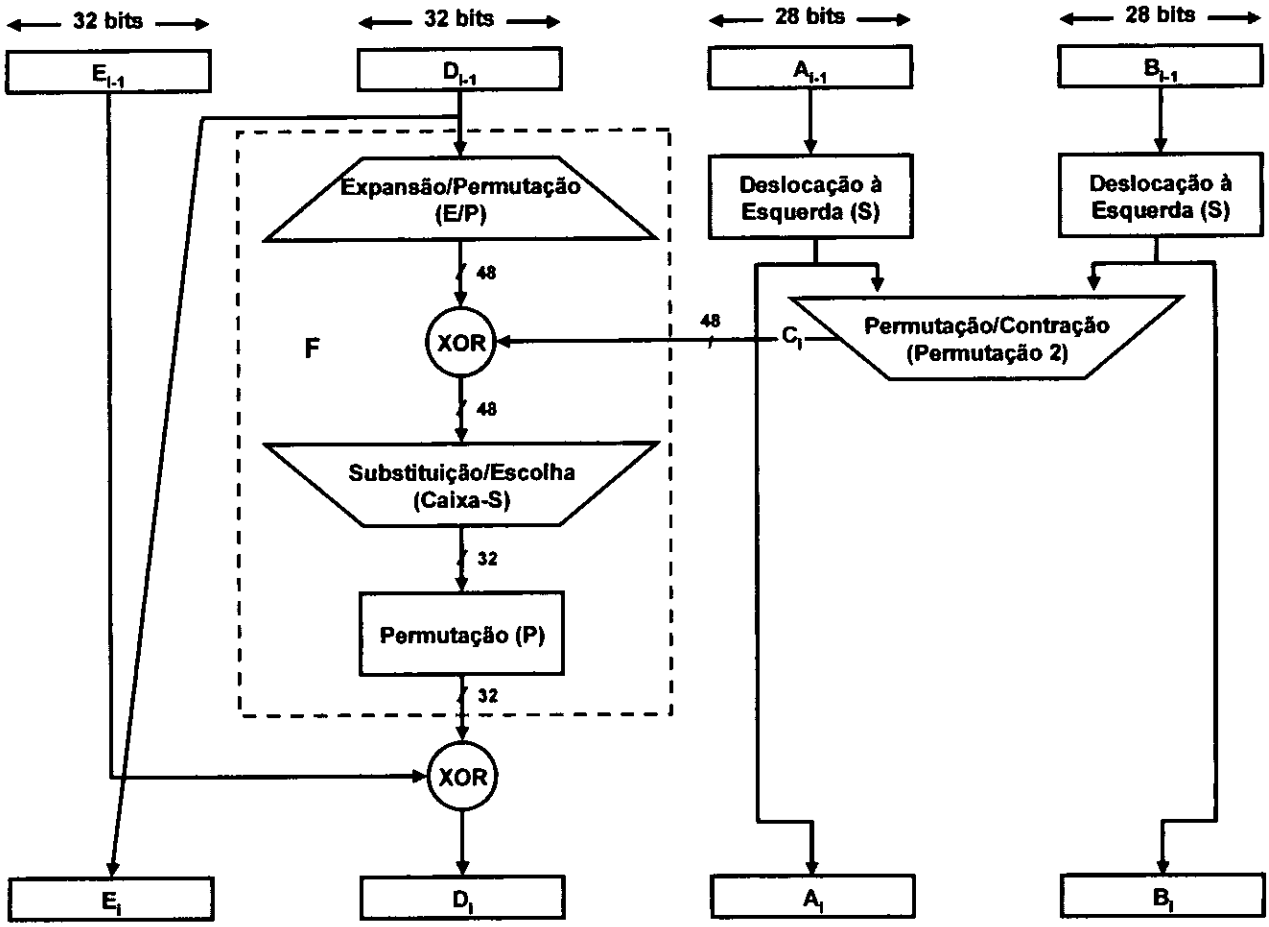


Figura 28 – Estágio Simples do Algoritmo DES [16].

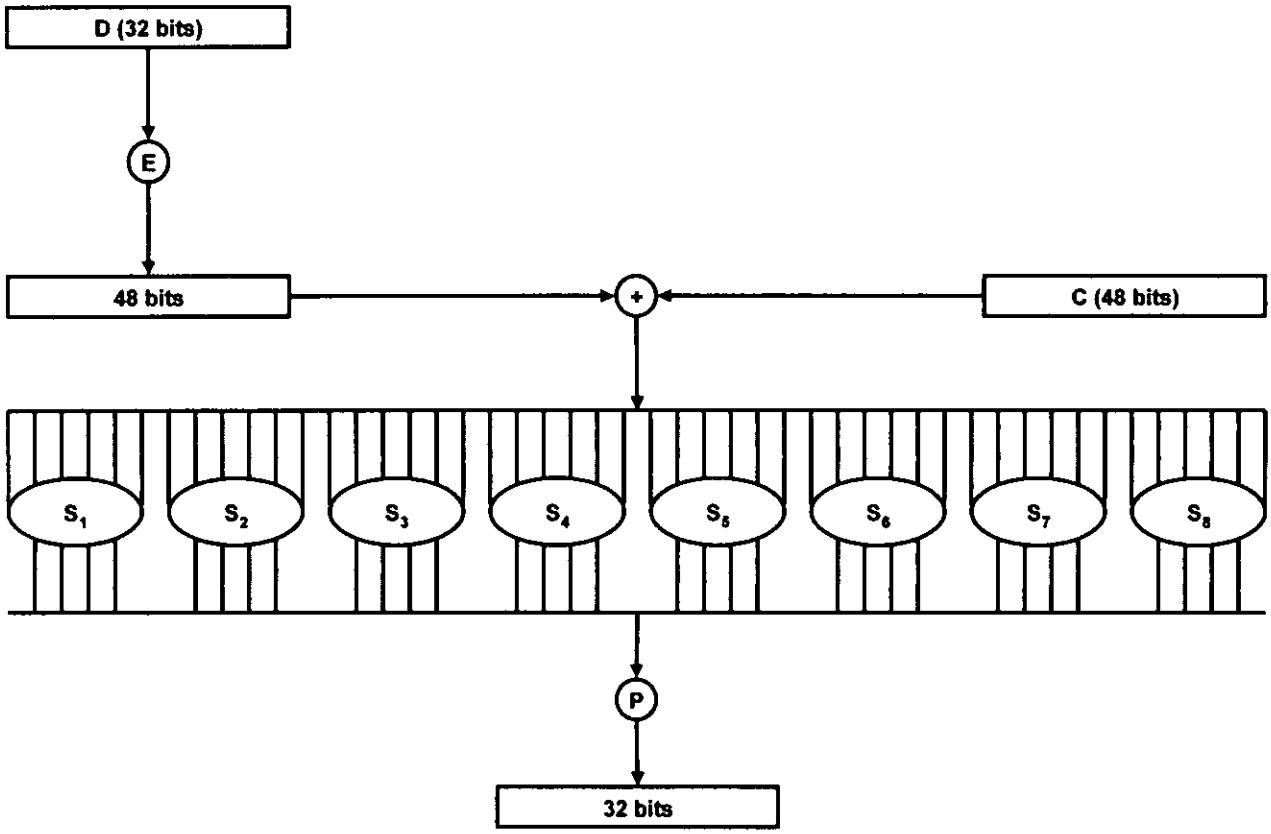


Figura 29 – Cálculo de F(D, C).

A chave do estágio C_i é de 48 bits. A entrada D_i é de 32 bits. A entrada D é primeiro expandida a 48 bits usando uma tabela que define uma permutação e uma expansão que envolve a duplicação de 16 dos bits de D (ver Tabela 6 (c)). Os 48 bits resultantes são submetidos a uma operação de OU-Exclusivo com o C_i. Estes 48 bits resultantes passam por uma função de substituição que produz uma saída de 32 bits, que é permutada como definida na Tabela 6 (d).

O papel das Caixas-S na função F é ilustrado na Figura 29. A substituição consiste num conjunto de 8 Caixas-S, em que cada uma aceita 6 bits de entrada e produz 4 bits de saída. Estas transformações são definidas na Tabela 7, que é interpretada da seguinte forma [16]:

- O primeiro e o último bit de entrada da caixa S_i formam um número binário de 2 bits para seleccionar uma das 4 substituições definidas pelas 4 linhas na tabela do S_i;
- Os 4 bits do meio seleccionam uma coluna;
- O valor decimal da célula seleccionada pela linha e coluna é convertido para a sua representação de 4 bits para produzir a saída. Por exemplo, no S_1, para a

entrada 011001, a linha é 01 (linha 1) e a coluna é 1100 (coluna 12). O valor da linha 1, coluna 12 é 9, então a saída é 1001;

- Cada linha duma Caixa-S define uma substituição geral reversível.

A saída de 32 bits das Caixas-S é então permutada, de modo que no próximo estágio cada Caixa-S afecta imediatamente as restantes.

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tabela 7 – Definição das Caixas-S [16].

4.10.1.2. Geração das chaves

Olhando para as Figura 27 e 28, vemos que a chave de 56 bits usada como entrada para o algoritmo é primeiro sujeita a uma permutação definida pela Tabela 8 (a) denominada Permutação 1. Os 56 bits resultantes são então tratados como duas metades de 28 bits, denominados C_0 e D_0. Em cada estágio, C_{i-1} e D_{i-1} são separadamente submetidos a um deslocamento circular à esquerda, ou rotação, de 1 ou 2 bits, descritos pela Tabela 8 (c). Esses valores deslocados servem de entrada para o estágio seguinte e também servem de entrada para a Permutação 2, veja a Tabela 8 (b), que produz uma saída de 48 bits que serve de entrada para a função $F(D_{i-1},C_i)$.

(a) Permutação 1 (P-1)

57	**49**	**41**	**33**	**25**	**17**	**9**
1	**58**	**50**	**42**	**34**	**26**	**18**
10	**2**	**59**	**51**	**43**	**35**	**27**
19	**11**	**3**	**60**	**52**	**44**	**36**
63	**55**	**47**	**39**	**31**	**23**	**15**
7	**62**	**54**	**46**	**38**	**30**	**22**
14	**6**	**61**	**53**	**45**	**37**	**29**
21	**13**	**5**	**28**	**20**	**12**	**4**

(b) Permutação 2 (P-2)

14	**17**	**11**	**24**	**1**	**5**	**3**	**28**
15	**6**	**21**	**10**	**23**	**19**	**12**	**4**
26	**8**	**16**	**7**	**27**	**20**	**13**	**2**
41	**52**	**31**	**37**	**47**	**55**	**30**	**40**
51	**45**	**33**	**48**	**44**	**49**	**39**	**56**
34	**53**	**46**	**42**	**50**	**36**	**29**	**32**

(c) Definição dos Deslocamentos à Esquerda

Número do Estágio	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits roteados	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tabela 8 – Tabelas usadas para o Cálculo da Chave do DES [16].

4.10.1.3. Decriptação

Como qualquer Cifra de Fiestel (ver o Anexo D) a decriptação consiste no mesmo algoritmo que a encriptação só que as chaves são usadas inversamente.

4.10.1.4. Critério de concepção do DES

O critério usado no desenho do DES baseia-se no funcionamento das Caixas-S e na função P que usa a saída das Caixas-S. O critério das Caixas-S é o seguinte:

1. Nenhum bit da saída de qualquer Caixa-S deve estar perto duma função linear do bit de entrada. Isto é, se nós seleccionarmos qualquer bit de saída e qualquer subconjunto dos 6 bits de entrada, a fracção da entrada em que cada um destes bits de saída iguala ao OU-Exclusivo desses bits de entrada não devem estar perto de 0 e 1, mas sim depende de ½;
2. Cada linha duma Caixa-S (determinado por um valor fixo dos bits de entrada mais a esquerda e direita) deve incluir todos 16 possíveis bits de entrada;
3. Se duas entradas duma Caixa-S diferem em exactamente um bit, a saída deverá diferenciar em pelo menos 2 bits;
4. Se dois bits de entrada duma Caixa-S diferem nos exactamente dois bits do meio, a saída deve diferenciar em pelo menos dois bits;
5. Se dois bits de entrada diferem nos seus dois primeiros bits e são idênticos nos restantes dois, os dois bits de saída não devem ser iguais;
6. Para qualquer diferença de 6 bits não-zero entre entradas, não mais de 8 dos 32 pares da entrada, exibindo essa diferença, pode resultar na mesma diferença na saída;
7. Este critério é similar ao anterior mas para o caso de 3 Caixas-S.

As Caixas-S são os únicos elementos no DES que não são lineares. Se elas fossem lineares todo algoritmo o seria e o mesmo seria facilmente quebrável. A linearidade foi analisada na Cifra de Hill. Os critérios restantes são usados para diminuir a Criptoanálise Diferencial (ver Anexo A) e providenciar uma boa confusão.

O critério da permutação P funciona da seguinte forma [16]:

1. Os 4 bits de saída de cada Caixa-S do estágio i são distribuídos de forma que dois deles afectam (providenciam entrada para) os "bits do meio" do estágio (i+1) e os outros dois afectam os bits do fim. Os dois bits do meio da entrada duma Caixa-S não são partilhados com Caixas-S adjacentes. Os bits do fim são

os dois bits da esquerda e os dois bits da direita, que são partilhados com Caixa-S adjacente;

2. Os 4 bits de saída de cada Caixa-S afectam as 6 diferentes Caixas-S do próximo estágio e nenhuns dois bits afectam a mesma Caixa-S;
3. Para duas Caixas-S, j e k, se um bit de saída de S_i afecta um bit do meio de S_k no próximo estágio, então um bit de saída do S_k não pode afectar um bit do meio de S_j. Isto implica que para j = k, um bit de saída de S_j não deve afectar um bit do meio de S_j.

Estes critérios são usados para aumentar a difusão do algoritmo.

4.10.1.5. Análise do DES

4.10.1.5.1. Efeito avalanche

A propriedade mais apreciável de qualquer algoritmo de encriptação é que qualquer mudança tanto no texto em claro como na chave deveria produzir uma grande mudança no texto cifrado. Particularmente uma mudança dum bit no texto em claro ou uma mudança dum bit na chave deveria produzir uma mudança em muitos bits do texto cifrado. Se a mudança é pequena, isto poderia providenciar um modo de redução do tamanho do texto em claro e da chave a ser procurada [15].

DES possui um forte efeito avalanche. Por exemplo, usaremos dois textos em claro que diferem por um bit:

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Com a chave

0000001 1001011 0100100 1100010 0011100 0011000 0011100 0110010

A Tabela 9 mostra que após três estágios, os dois blocos diferem em 21 bits. No final diferem em 34 bits. A Tabela 9 mostra um teste similar que tem como entrada um único texto em claro:

011010000 100000101 0010111 01111010 00010011 01110110 11101011 10100100

Com duas chaves que diferem em um único bit:

1110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100
0110010 1111011 1101111 0011000 0011101 0000100 0110001 11011100

(a) Mudança no Texto em Claro		(b) Mudança na Chave	
Estágio	**Número de Bits que diferem**	**Estágio**	**Número de Bits que diferem**
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

Tabela 9 – Efeito Avalanche no DES [16].

De novo, o resultado mostra que cerca de metade dos bits do texto cifrado diferem e que o efeito avalanche é sentido após alguns estágios.

4.10.1.5.2. Uso da chave de 56 bits

Com uma chave de tamanho de 56 bits, existem 2^{56} chaves possíveis o que são aproximadamente 7,2 x 10^{16} chaves. Deste modo, com este número de chaves o ataque Força-Bruta é impraticável. Assumindo que em média para se ter sucesso com a Força-Bruta deve-se tentar metade das chaves e tomando em consideração que uma simples execução do DES numa máquina leva cerca de 1 microsegundo, levaria mais de 1000 anos para quebrar a cifra. É de realçar que 1 μs por cada execução de DES é ser optimista. Pois, Diffie e Hellman em 1977 postularam que existe tecnologia para construir uma máquina paralela com um milhão de elementos de encriptação em que cada um executa uma encriptação por 1 μs o que baixaria o tempo para 10 horas. Os autores do postulado previram um custo de $ 20.000.000 em 1977 [16].

Além disso, em 1993 Wiener reportou o desenvolvimento dum chip que usa técnicas *pipelined* para chegar a uma taxa de 50 milhões de chaves/segundo. De acordo com os custos de 1993, ele concebeu um módulo que custava $ 100.000 e continha 5760 chips de procura de chaves. Com este desenho foram obtidos os resultados da Tabela 10.

Unidade do custo da máquina de procura de chaves	Tempo de espera da procura
$ 100.000	35 horas
$ 1.000.000	3,5 horas
$ 10.000.000	21 minutos

Tabela 10 – Custos e Tempo médio da máquina de Procura de Chave do DES [16].

E estimou um desenvolvimento único de $ 500.000. Em 1997 Weiner actualizou os custos da sua pesquisa e dividiu o tempo por 6, ficando, por exemplo, os $ 100.000 usados para 6 horas. Apesar do trabalho de Weiner ser de grande importância ele não foi construído [16].

Uma das mais dramáticas demonstrações de vulnerabilidade do DES foi a da chave-secreta desafiada pela RSA Laboratories. O desafio, que oferecia uma recompensa de $ 10.000, consistia em procurar uma chave DES sendo fornecido um texto cifrado para obter um texto em claro consistindo em um texto em claro desconhecido precedido por três blocos conhecidos contendo uma frase de 24 caracteres. O desafio começou em 29 de Janeiro de 1977, onde Rocke Verser, um consultor independente, desenvolveu um programa de Força-Bruta e distribuiu pela *Internet*, o projecto ligou pela *Internet* cerca de 70.000 sistemas. O projecto começou em 18 de Fevereiro de 1997 e terminou 96 dias depois quando a chave certa foi encontrada depois de examinar aproximadamente ¼ de todas possibilidades. Este desafio demonstrou a força de computadores pessoais distribuídos em atacar algoritmos criptográficos. Contudo, existe mais para um ataque de procura da chave que só tentam todas possibilidades. A não ser que o texto em claro seja fornecido, o analista deve ser capaz de identificar que o texto em claro é de facto o texto em claro. Se a mensagem for só texto em claro em Inglês, então os resultados seriam obtidos rapidamente, mas o processo de reconhecimento do Inglês deveria ser automática. Se o texto da mensagem for comprimido antes da encriptação, então o reconhecimento seria mais complicado. E se o texto fosse constituído por números a dificuldade seria maior. Resumindo, para o ataque de Força-Bruta deve-se conhecer alguma informação acerca do texto em claro

e consequentemente precisamos de alguns meios automáticos para distinguir o texto em claro do texto inútil.

Estes dois exemplos mostram que com o tempo o DES vai perdendo a sua qualidade, o que requer a procura de alternativas.

O DES é usado para aplicações pessoais e comerciais.

4.10.2. Blowfish

O Blowfish é uma cifra de bloco simétrico desenvolvido por Bruce Shneier. Blowfish foi concebido para possuir as seguintes características [16]:

- **Rápido:** Blowfish encripta dados em microprocessadores de 32 bits com uma taxa de 18 ciclos do "clock" por byte;
- **Compacto:** Blowfish pode correr com menos de 5K de memória;
- **Simples:** a estrutura simples do Blowfish é fácil de implementar e fácil é a tarefa de determinar a força do algoritmo;
- **Segurança variável:** o tamanho da chave é variável e pode ser longa até 448 bits. Isto permite uma troca entre alta velocidade e alta segurança.

Blowfish encripta blocos de texto em claro de 64 bits em blocos de texto cifrado de 64 bits. Blowfish é implementado em numerosos produtos e foi vastamente pesquisado, pelo que até agora a segurança do Blowfish é indesafiável.

4.10.2.1. Geração da subchave e Caixa-S

Blowfish usa uma chave com um intervalo de 32-448 bits (1 para 14 palavras de 32 bits). Esta chave é usada para gerar 18 subchaves de 32 bits e 4 Caixas-S_{8x32} contendo um total de 1024 entradas de 32 bits. O total de 1024 valores de 32 bits, ou 4168 bytes [16].

As chaves são armazenadas num Array-C:

$$C_1, C_2, \ldots, C_j \qquad 1 \leq j \leq 14$$

As subchaves são armazenadas no Array-P:

$$P_1, P_2, \ldots, P_{18}$$

Existem 4 Caixas-S, cada com 256 entradas de 32 bits:

$$S_{1,0}, S_{1,1}, \ldots, S_{1,255}$$

$$S_{2,0}, S_{2,1}, \ldots, S_{2,255}$$

$$S_{3,0}, S_{3,1}, \ldots, S_{3,255}$$

$S_{4,0}, S_{4,1}, \ldots, S_{4,255}$

Os passos para a geração do Array-P e das Caixas-S são os seguintes [16]:

1. Inicializar primeiro o array-P e depois as 4 Caixas-S em ordem usando os bits da parte fraccionária da constante π. Assim, os 32 bits mais a esquerda da parte fraccionária de π será P_1, e assim por diante. Por exemplo, em Hexadecimal:

   P_1 = 243F6A88

   P_2 = 85A308D3

   ...

   $S_{4,254}$ = 578FDFE3

   $S_{4,255}$ = 3AC372E6

2. Efectua-se um OU-Exclusivo do array-P e do array-C, reusando as palavras do array-C necessárias. Por exemplo, para o tamanho máximo da chave (14 palavras de 32 bits), $P_1 = P_1 \oplus C_1$, $P_2 = P_2 \oplus C_2$, ..., $P_{14} = P_{14} \oplus C_{14}$, $P_{15} = P_{15} \oplus C_1$, ..., $P_{18} = P_{18} \oplus C_4$.
3. Encriptar o bloco de 64 bits de todos zeros usando o array-P e array-S correntes, substituir P_1 e P_2 com a saída da encriptação.
4. Encriptar a saída do passo 3 usando o array-P e o array-S corrente e substituir P_3 e P_4 com o texto cifrado resultante.
5. Continue este processo para actualizar todos elementos de P e então, em ordem, todos elementos de S, usando a cada passo a saída da contínua mudança do algoritmo Blowfish.

O processo de actualização pode ser resumido da seguinte forma:

$P_1, P_2 = E_{P,S}[0]$

$P_3, P_4 = E_{P,S}[P_1 \,||\, P_2]$

...

$P_{17}, P_{18} = E_{P,S}[P_{15} \,||\, P_{16}]$

$S_{1,0}, S_{1,1} = E_{P,S}[P_{17} \,||\, P_{18}]$

...

$S_{4,254}, S_{4,255} = E_{P,S}[S_{4,252} \,||\, P_{4,253}]$

Onde:

$E_{P,S}[Y]$ é o texto cifrado produzido pela encriptação Y usando o Blowfish com os arrays P e S.

Um total de 521 execuções do algoritmo de encriptação do Blowfish é requerido para produzir os arrays P e S finais. Contudo, Blowfish não é aplicável para aplicações em que a chave secreta muda frequentemente. Além disso, para rápida execução, os arrays P e S podem ser guardados mais facilmente do que rederivados da chave a cada uso do algoritmo. Isto requer cerca de 4KB de memória. Então, Blowfish não é apropriado para aplicações com memória limitada, como são os cartões inteligentes (Smart-Cards) [16].

4.10.2.2. Encriptação

Blowfish usa duas operações primitivas:

- **Adição:** adição de palavras, denotado por +, é efectuada o módulo 2^{32}.
- **Operação OU-Exclusivo:** esta operação é denotada por $\oplus$.

O facto importante nestas duas operações é que elas não comutam. O que torna a criptoanálise mais difícil. A Figura 30 explica a operação de encriptação. O texto em claro dividido em duas partes de 32 bits EE e DE. Usamos as variáveis Ee_i e De_i para nos referirmos a parte esquerda e direita dos dados após o estágio i estar completo. O algoritmo pode ser definido pelo seguinte pseudocódigo:

For i := 1 to 16 do

$DE_i = EE_{i-1} \oplus P_i$;

$EE_i = F[DE_i] \oplus DE_{i-1}$;

$EE_{17} = DE_{16} \oplus P_{18}$;

$DE_{17} = EE_{16} \oplus P_{17}$;

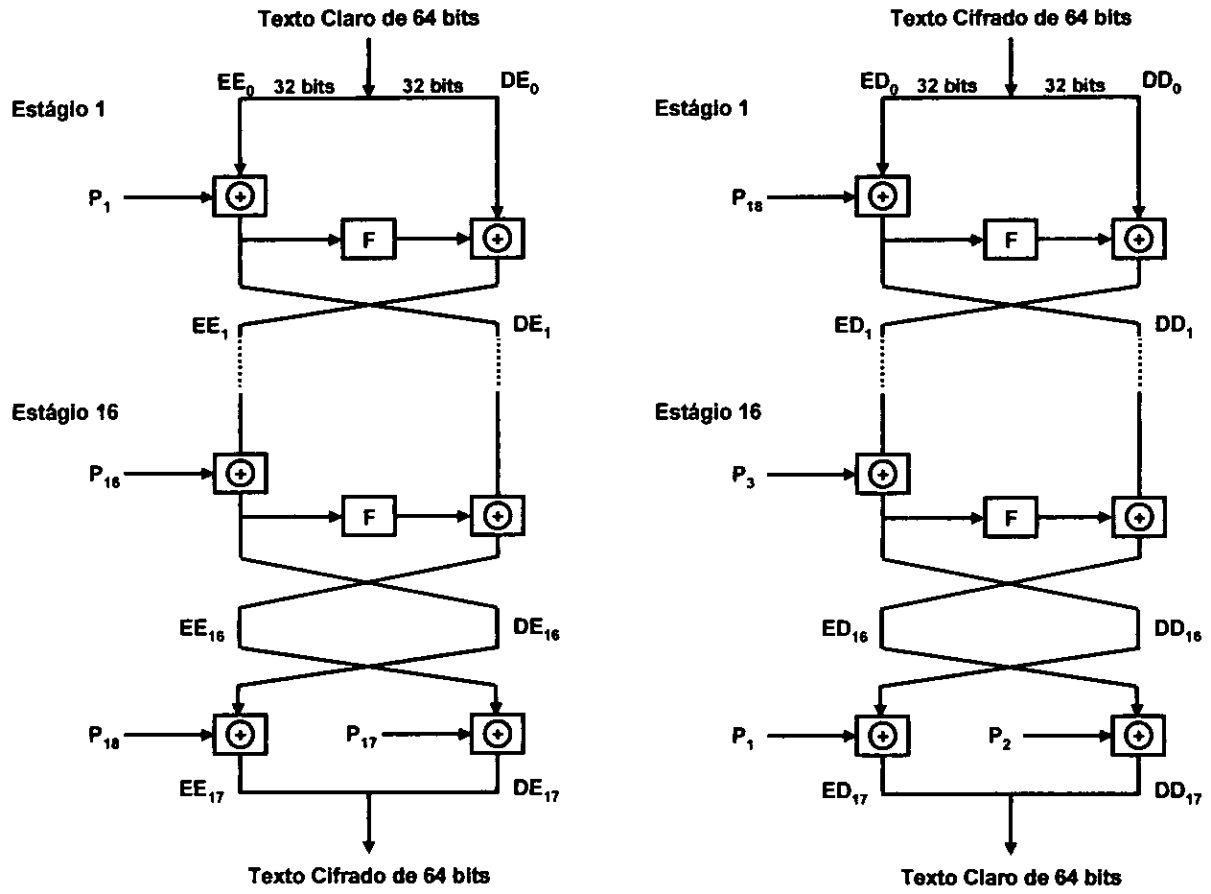


Figura 30 – Encriptação (Esquerda) e Decriptação (Direita) Blowfish [16].

O texto cifrado resultante está contido nas variáveis EE_{17} e DE_{17}. A função F é mostrada na Figura 31. Os 32 bits de entrada para F são divididos em 4 bytes. Se nomearmos os bytes a, b, c e d, então a função pode ser definida como:

$$F[a,b,c,d] = ((S_{1,a} + S_{2,b}) \oplus S_{3,c}) + S_{4,d} \qquad (28)$$

Então, cada estágio inclui o uso complexo da adição módulo 2^{32} e OU-Exclusivo, mais substituições usando Caixas-S.

4.10.2.3. Decriptação

A decriptação, como se pode ver na Figura 30, é facilmente derivada do algoritmo de encriptação. Neste caso, os 64 bits são inicialmente atribuídos as duas variáveis de uma palavra ED_0 e DD_0. Usamos as variáveis ED_i e DD_i para nos referirmos a parte esquerda e direita dos dados após o estágio i. E, como a maior parte das cifras de bloco (ver ANEXO C), a decriptação Blowfish envolve o uso de subchaves na ordem inversa. Contudo, diferente da maior parte das cifras de bloco, a decriptação Blowfish ocorre na mesma direcção algorítmica que a encriptação, em vez da inversa. O algoritmo pode ser definido com [16]:

For i = 1 to 16 do

$$DD_i = ED_{i-1} \oplus P_{19-i};$$

$$ED_i = F[DD_i] \oplus DD_{i-1};$$

$$ED_{17} = DD_{16} \oplus P_1;$$

$$DD_{17} = ED_{16} \oplus P_2;$$

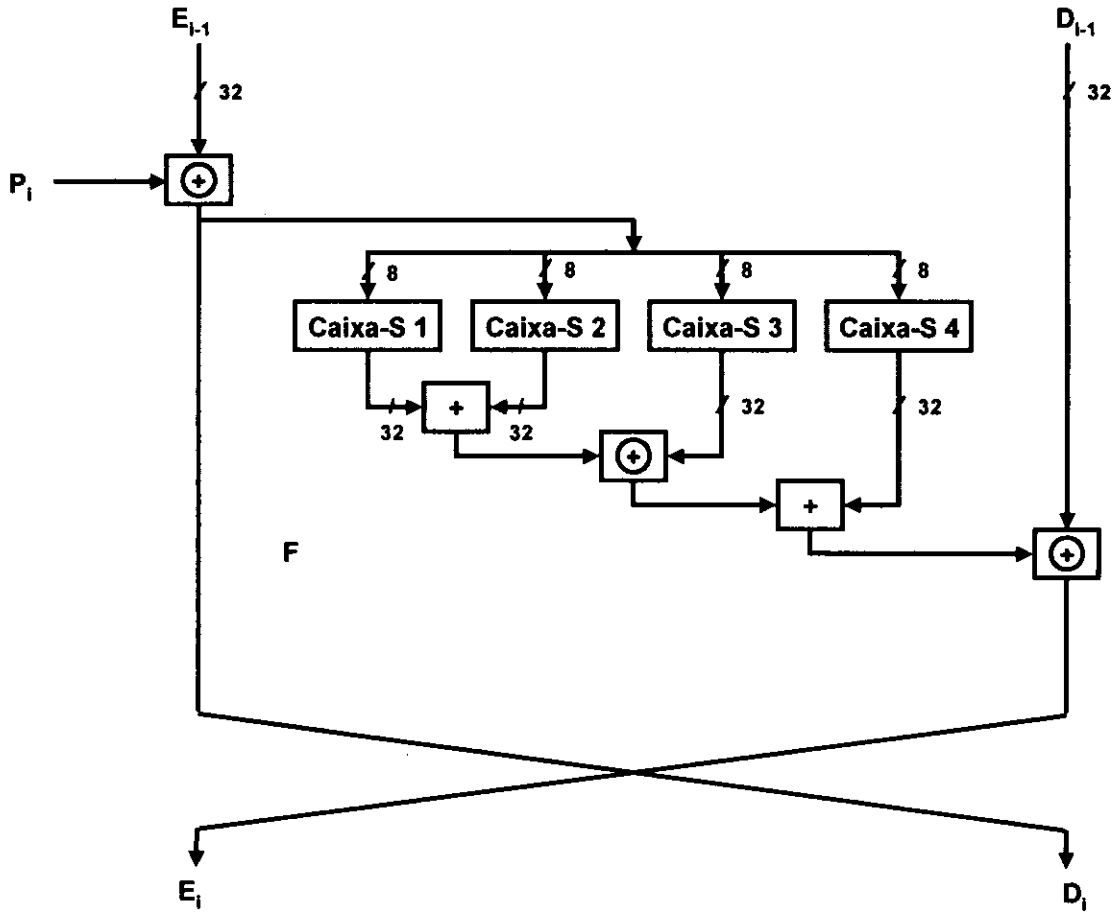


Figura 31 – Detalhe dum simples Estágio Blowfish [16].

4.10.2.4. Análise do Blowfish

Blowfish é talvez o algoritmo de encriptação convencional mais formidável. Diferentes do DES, as Caixas-S do Blowfish são dependentes da chave. Alguns dos outros algoritmos, como o RC5, são desenhados de tal forma que uma das funções executadas durante um estágio é dependente dos dados (no caso do RC5 é a rotação circular). Mas no caso do Blowfish, ambas as subchaves e Caixas-S são produzidas por um processo de repetidas aplicações do Blowfish mesmo. Isto mistura inteiramente os bits e torna a criptoanálise muito difícil.

Outra característica interessante do Blowfish é que as operações são executadas nas duas metades dos dados em cada estágio, em vez de o fazer em apenas uma metade como é no caso das Cifras de Fiestel (ver ANEXO D). Isto providencia uma grande força criptográfica mesmo quando a operação adicional é linear (OU-Exclusivo).

Quanto ao ataque de Força-Bruta, Blowfish é virtualmente invulnerável com uma adequada escolha do tamanho da chave, que pode ser de até 448 bits. Blowfish também é eficazmente rápido. A Tabela 11 compara o número de ciclos do "clock" dum Pentium para vários algoritmos implementados em C. Blowfish é claramente o mais rápido de executar.

Algoritmo	Ciclos do *Clock* por Estágio	Número de Estágios	Número de ciclos do *Clock* por byte encriptado
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50
DES-Triplo	18	48	108

Tabela 11 – Comparação de velocidades de Cifras de Bloco num Pentium [16].

4.10.2.5. Alguma consideração sobre o desenho do Blowfish:

1. Um ataque de Força-Bruta é mais difícil do que pode parecer devido ao tamanho da chave por causa do consumo de tempo do processo de geração da subchave. Um total de 522 execuções do algoritmo é requerido para testar uma simples chave;
2. A função F dá ao Blowfish o melhor efeito avalanche possível para uma rede de Fiestel (ver ANEXO D). No estágio i, todos bits de E_{i-1} afectam todos bits de D_{i-1}. Além disso, cada bit da subchave é afectado por todos bits da chave, e além disso F têm um perfeito efeito avalanche entre a chave (P_i) e a metade direita dos dados (D_i) depois de cada estágio;
3. Cada bit de entrada da função F é apenas usada como entrada para uma Caixa-S. Em contraste ao DES, muitos bits são usados como entrada para duas Caixas-S, o que reforça consideravelmente o algoritmo contra ataques diferenciais. Esta complexidade não é necessária quando se usam Caixas-S dependentes da chave;
4. Diferente da CAST, a função F no Blowfish não é dependente do estágio, pois não dá vantagens criptográficas devido ao facto da substituição do array-P já ser dependente do estágio.

4.10.3. RC5

RC5 é um algoritmo de encriptação simétrico desenvolvido por Rivest. RC5 foi concebido para ter as seguintes características [16]:

- **Adequado ao Hardware e Software:** RC5 usa apenas operações computacionais primitivas comuns em microprocessadores;
- **Rápido:** para obter isto, RC5 é um algoritmo simples e é orientado por palavras. As operações básicas trabalham em todas palavras dos dados duma vez;
- **Adaptável a processadores de diferentes tamanhos da palavra:** o número de bits em uma palavra é um parâmetro do RC5, diferentes tamanhos da palavra requerem diferentes algoritmos;
- **Número variável de estágios:** o número de estágio é o segundo parâmetro do RC5. Este parâmetro permite uma troca entre alta velocidade e alta segurança;
- **Tamanho variável da chave:** o tamanho da chave é um terceiro parâmetro do RC5. Esta característica também permite uma troca entre velocidade e segurança;
- **Simples:** a estrutura simples do RC5 é fácil de implementar e facilmente se determina a força do algoritmo;
- **Requer pouca memória:** torna o RC5 mais adequado aos cartões inteligentes (Smart-Cards) e outros elementos com memória restrita;
- **Alta segurança:** RC5 proporciona alta segurança com parâmetros adequados;
- **Rotação dependente dos dados:** RC5 incorpora rotação (deslocamento circular dos bits) cuja quantidade depende dos dados. Isto reforça o algoritmo contra a criptoanálise.

RC5 foi incorporado no RSA Data Security, Inc.'s major products, incluindo BSAFE, JSAFE e S/MAIL.

4.10.3.1. Parâmetros RC5

RC5 é actualmente uma família de algoritmos de encriptação determinada por 3 parâmetros (ver Tabela 12).

Parâmetro	Definição	Valores permitidos
W	Tamanho da palavra em bits. RC5 encripta blocos de 2 palavras	16, 32, 64
R	Número de estágios	0, 1, ...,255
B	Número de bytes de 8 bits (octetos) na chave secreta C	0, 1, ..., 255

Tabela 12 – Parâmetros do RC5 [16].

Assim, RC5 encripta blocos de texto em claro de tamanho 32, 64 ou 128 bits em blocos de texto cifrado do mesmo tamanho. O intervalo do tamanho da chave é de 0 para 2040 bits. Uma versão específica do RC5 é designada por RC5-w/r/b. Por exemplo, RC5-32/12/16 tem palavras de 32 bits (blocos de texto em claro e texto cifrado de 64 bits), 12 estágios no algoritmo de encriptação e decriptação, e a chave de 16 bytes (128 bits), esta é a chamada *versão nominal*.

4.10.3.2. Expansão da chave

RC5 executa um complexo conjunto de operações na chave secreta para produzir um total de t subchaves. Duas subchaves são usadas em cada estágio, e duas subchaves são usadas numa operação adicional que não participa em nenhum estágio, então t = 2r + 2. Cada subchave é uma palavra de w bits de tamanho. A Figura 32 ilustra a técnica usada para gerar as subchaves. As subchaves são armazenadas num array de t palavras denominado S[0], S[1], ..., S[t-1]. Usando os parâmetros r e w como entrada, este array é inicializado para um padrão particular fixo de bits pseudoaleatórios. Então a chave de b bytes, C[0 ... b-1], é convertida num array de c palavras L[0 ... c-1]. Numa máquina pequena isto é conseguido zerando o array L e copiando o texto C directamente para as posições da memória representadas por L. Se b não é um inteiro múltiplo de w, então uma porção de L da direita final permanecerá zero [16].

Finalmente, uma mistura de operações é efectuadas e aplicadas sobre o conteúdo de L para os valores inicializados de S para produzir um valor final do array S.

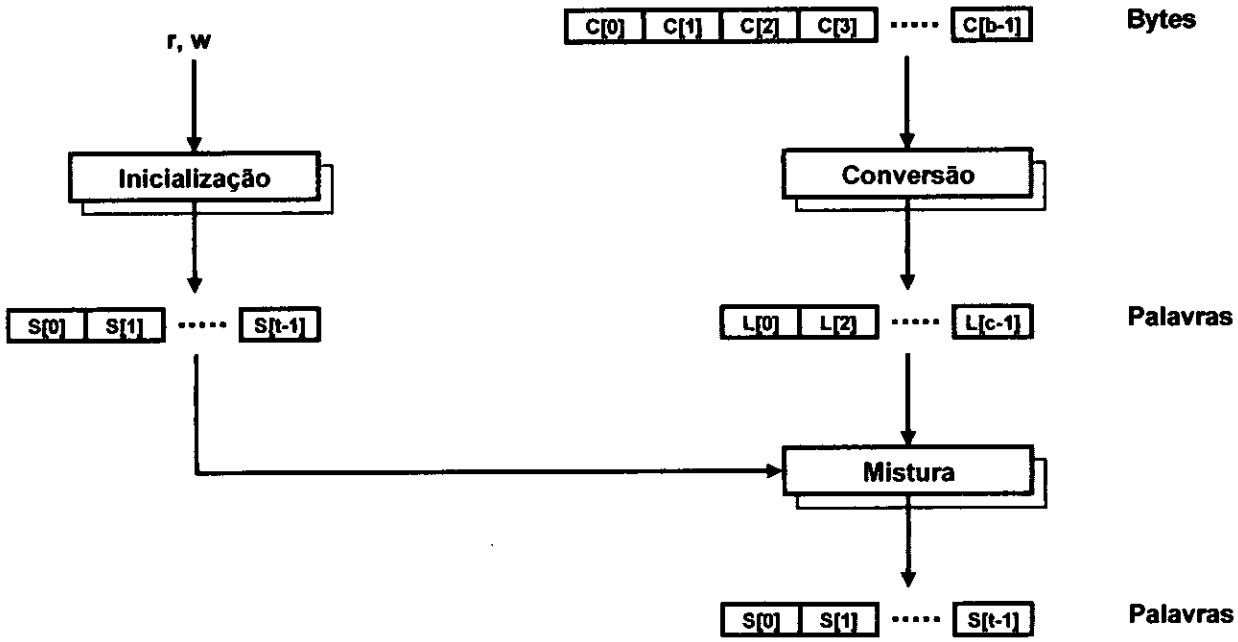


Figura 32 – Expansão da Chave RC5 [16].

Vamos olhar as operações mais detalhadamente. A operação de inicialização faz uso de duas palavras de tamanho constante definido como:

$$P_w = Odd[(e-2)2^w] \qquad (29)$$

$$Q_w = Odd[(\phi-1)2^w] \qquad (30)$$

Onde:

e = 2,718281828459... (base dos algoritmos naturais)

ϕ = 1,618033988749 (taxa doirada) = $\left(\frac{1+\sqrt{5}}{2}\right)$

Odd(x) é o inteiro impar mais próximo de x (arredondando a x, até se x for um inteiro, contudo isto não acontece aqui). Por exemplo, Odd[e] = 3 e Odd[ϕ] = 1. Usando os valores permitidos de w, as constantes são (em hexadecimal) as da Tabela 13.

W	16	32	64
P_w	B7E1	B7E15163	B7E151628AED2A6B
Q_w	9E37	9E377939	9E3779B97FIA7C15

Tabela 13 – Valores permitidos de w [16].

Usando estas duas constantes, o array S é inicializado da seguinte forma:

S[0] = P_w;
For i := 1 to t-1 do
    S[i] = S[i-1] + Q_w;

Onde a adição é efectuada módulo 2^w. O array S inicializado é então misturado com o array L da chave para produzir um array final S de subchaves. Para este propósito, três passos são executados pelo maior dos dois arrays, o array mais pequeno pode ser usado mais vezes:

```
i = j = k = 0;
Do 3 x max(t,c) times:
    S[i] = (S[i] + X + Y) <<< 3; X = S[i];
    i = (i+1) mod (t);
    L[j] = (L[j] + X + Y) <<< (X + Y);
    Y = L[j]; j = (i + 1) mod (c);
```

Rivest comentou que não é fácil determinar C do S.

4.10.3.3. Encriptação

RC5 usa 3 operações primitivas (e as suas inversões) [16]:

- **Adição:** adição de palavras, denotado por +, é efectuado o módulo 2^w. A operação inversa, denotado por -, é subtracção módulo 2^w;
- **Operação OU-Exclusivo:** esta operação é denotada por $\oplus$;
- **Rotação circular à esquerda:** a rotação circular da palavra x à esquerda por y bits é denotado por x <<< y. O inverso é a rotação circular a direita da palavra x por y bits é denotado por x >>> y.

A Figura 33 demonstra a operação de encriptação. Note que está não é uma estrutura de Fiestel (ver ANEXO D) clássica. O texto em claro é assumido para inicialmente residir nos dois registos de w bits A e B. Usaremos as variáveis EE_i e DE_i para nos referirmos a metade esquerda e direita dos dados após cada estágio i estar completo. O algoritmo pode ser definido pelo seguinte pseudocódigo:

$EE_0 = A + S[0];$

$DE_0 = B + S[1];$

For i := 1 to r do

$EE_i = ((EE_{i-1} \oplus DE_{i-1}) <<< DE_{i-1}) + S[2 \times i];$

$DE_i = ((DE_{i-1} \oplus EE_i) <<< EE_{i-1}) + S[2 \times i + 1];$

O texto cifrado resultante esta contido nas duas variáveis EE_i e DE_i. Cada um dos r estágios consiste numa substituição usando ambas as palavras dos dados, uma permutação usando as duas palavras dos dados e uma substituição que depende da chave. Note a simplicidade excepcional desta operação, que podem ser definidas por

cinco linhas de código. Note também que as duas metades dos dados são actualizadas em cada estágio. Então, um estágio do RC5 é de certa forma equivalente a dois estágios DES.

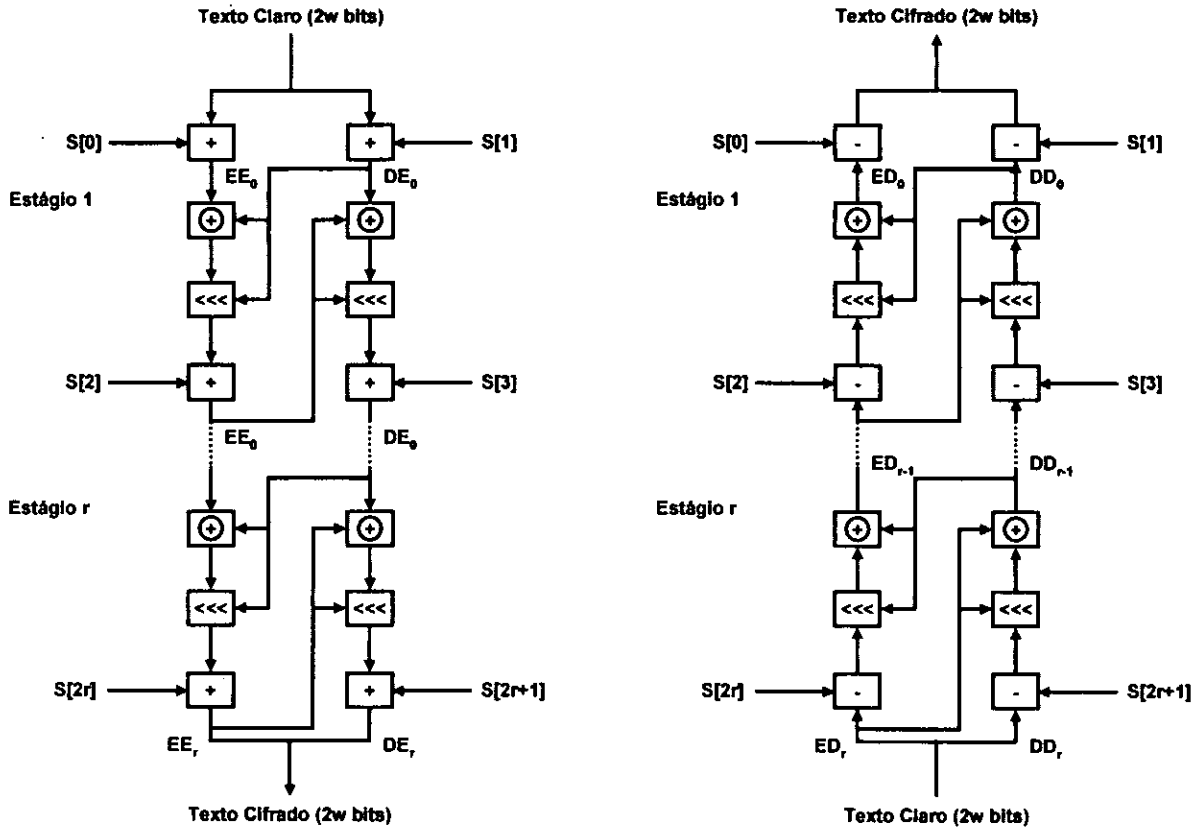


Figura 33 – Encriptação (Esquerda) e Decriptação (Direita) RC5 [16].

4.10.3.4. Decriptação

A decriptação, mostrada na Figura 33, é facilmente derivada do algoritmo de encriptação. Neste caso, os 2^w bits do texto cifrado são inicialmente atribuídos as duas variáveis duma palavra ED_r e DD_r. Usamos as variáveis ED_i e DD_i para nos referirmos a metade esquerda e direita dos dados antes do estágio começar, onde os estágios são enumerados de r para 1.

For i := r downto 1 do

$DD_{i-1} = ((DD_i - S[2 \times i + 1] >>> ED_i) \oplus ED_i);$

$ED_{i-1} = ((ED_i - S[2 \times i] >>> DD_{i-1}) \oplus DD_{i-1});$

$B = DD_0 - S[1];$

$A = ED_0 - S[0];$

4.10.3.5. Análise do RC5

As duas maiores vantagens do RC5 são a simplicidade do algoritmo e o uso de rotações dependentes dos dados. As rotações são as únicas porções não lineares do

algoritmo. Rivest sentiu que por causa da quantidade de rotações variar dependendo dos valores dos dados que circulam pelo algoritmo, a Criptoanálise Linear e Diferencial (ver ANEXO A) seriam mais complicadas.

4.10.4. CAST-128

CAST é um procedimento de desenho de algoritmos de encriptação simétricos desenvolvido por Carlisle Adams e Stafford Tavares. CAST-128 usa uma chave que varia de 40 bits à 128 bits em incrementos de 8 bits.

CAST tem uma estrutura da rede clássica de Fiestel (ver ANEXO D) com 16 estágios e operando em blocos de 64 bits de texto em claro para produzir blocos de 64 bits de texto cifrado. As duas diferenças a rede de Fiestel são que [16]:

- CAST aplica duas subchaves a cada estágio: um Km_i de 32 bits e um Kr_i de 5 bits;
- A função F depende do estágio.

CAST é resultado dum processo longo de investigação e desenvolvimento e beneficiou duma extensiva análise de Criptográficos. Foi inicialmente usado num número considerável de produtos, incluindo o PGP.

4.10.4.1. Encriptação

CAST-128 usa 4 operações primitivas:

- **Adição e subtracção:** Adição de palavras, denotado por +, é efectuado o módulo 2^{32}. A operação inversa, denotada por -, é módulo 2^{32};
- **Operação OU-Exclusivo:** esta operação é denotada por $\oplus$;
- **Rotação circular à esquerda:** a rotação circular da palavra x à esquerda por y bits é denotado por x <<< y.

O algoritmo de encriptação CAST-128 pode ser definido pelo pseudocódigo. O texto em claro é dividido em 2 metades de 32 bits E_0 e D_0. Usaremos as variáveis E_i e D_i para nos referirmos a metade esquerda e direita dos dados após o estágio estar completo. O texto cifrado é formado trocando a saída do 16º estágio, isto é, o texto cifrado é a concatenação E_{16} e D_{16}.

$E_0 \,||\, D_0$ = Texto em claro

For i=1 to 16 do

$E_i = D_{i-1}$;

$D_i = E_{i-1} \oplus F_i[D_{i-1}, Cm_i, Cr_i]$;

Texto cifrado = $E_{16} \| D_{16}$

A decriptação é idêntica a encriptação, com as chaves impostas na ordem inversa. Figura 34 mostra os detalhes dum único estágio. A função F inclui o uso de Caixas-S 48 x 32, a função de rotação circular à esquerda e quatro funções que variam dependendo do número de estágios, chamaremos essa função f_1, f_2, f_3 e f_4. Usaremos o I para nos referirmos ao valor intermédio após a função de rotação circular à esquerda, e os nomes I_a, I_b, I_c e I_d para nos referirmos aos 4 bytes de I, onde I_a é o mais significante e o I_d o menos. Com estas convenções F é definido como (ver Tabela 14):

Estágios 1, 4, 7, 10, 13, 16	$I = ((Cm_i + D_{i-1}) <<< Cr_i)$ $F = ((S1[I_a] \oplus S2[I_b]) - S3[I_c]) + S4[I_d]$
Estágios 2, 5, 8, 11, 14	$I = ((Cm_i \oplus D_{i-1}) <<< Cr_i)$ $F = ((S1[I_a] - S2[I_b]) + S3[I_c]) \oplus S4[I_d]$
Estágios 3, 6, 9, 12, 15	$I = ((Cm_i - D_{i-1}) <<< Cr_i)$ $F = ((S1[I_a] + S2[I_b]) \oplus S3[I_c]) - S4[I_d]$

Tabela 14 – Definição de F do CAST-128 [16].

Note a similaridade da estrutura da função do estágio do CAST-128 com a do Blowfish.

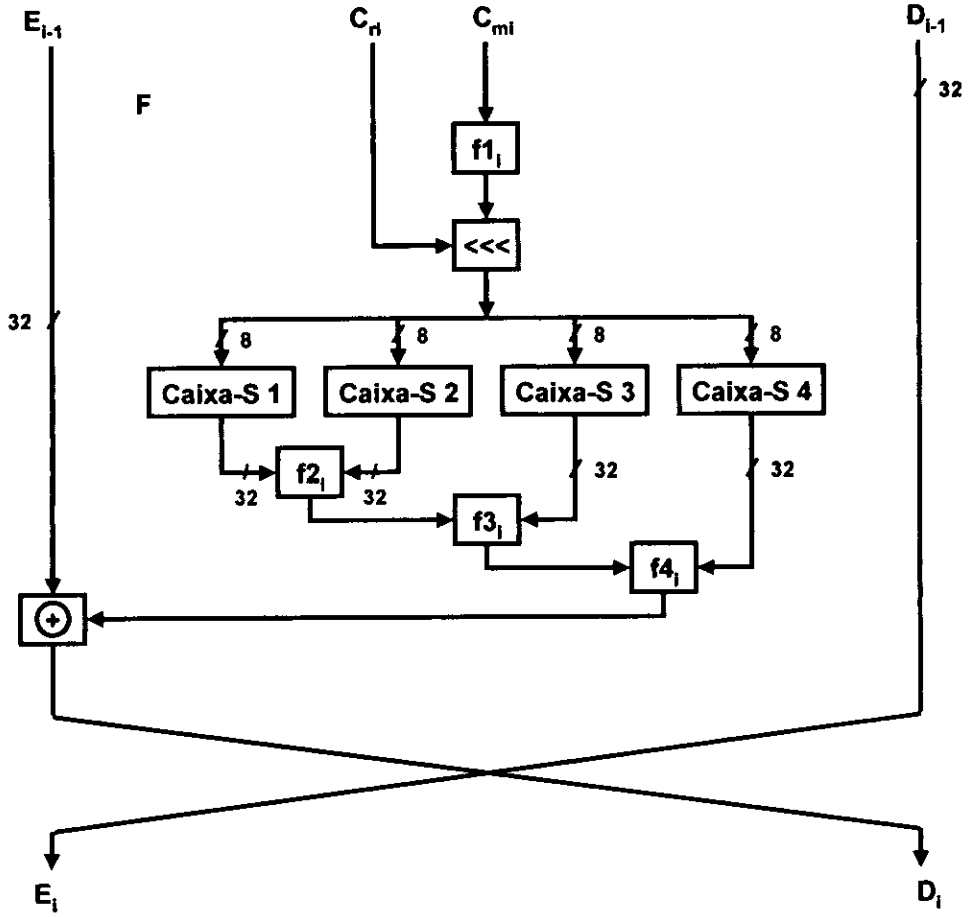


Figura 34 – Detalhe dum simples Estágio CAST-128 [16].

4.10.4.1.1. Caixas de Substituição

CAST-128 usa 8 caixas-S de 8 x 32. Quatro delas, caixa-S_1 até a caixa-S_4, são usadas no processo de encriptação e decriptação. As quatro restantes, caixa-S_5 até caixa-S_8 são usadas na geração da subchave. Cada caixa-S é um array de 32 colunas e 256 linhas. A entrada de 8 bits selecciona uma linha do array, o valor de 32 bits dessa linha é a saída. Todas caixas-S possuem valores fixos. Os autores fazem uso da teoria das funções de Bent (ver ANEXO B) [16].

4.10.4.2. Geração da chave

A geração da subchave é um processo complexo. Para começar, chamaremos os bytes da chave de 128 bytes da seguinte forma:

X0X1X2X3X4X5X6X7X8X9XAXBXCXDXEXF

Onde: X0 representa o byte mais significante e o XF o último. Também se usam as seguintes definições:

Cm_1, ..., Cm_{16} – 16 subchaves de *Masking* de 32 bits (uma por estágio);

Cr_1, ..., Cr_{16} – 16 subchaves de rotação de 32 bits (uma por estágio), onde apenas 5 bits menos significativos são usados;

z0 ... zF – Bytes intermediários (temporários);

C1, ..., C32 – Palavras de 32 bits intermediários (temporários).

Os valores C1 até C32 são calculados a partir da chave usando a caixa-S_5 até caixa-S_8. Então as subchaves são definidas como:

For I = 1 to 16 do

$Cm_i = C_i$;

$Cr_i = C_{16+i}$;

4.10.4.3. Análise do CAST

CAST faz o uso de caixas-S fixas. As caixas-S fixas com boas características não lineares são preferíveis em relação a caixas-S aleatórias que seriam obtidas se as caixas-S fossem dependentes da chave.

O procedimento usado no CAST consiste em seleccionar 32 vectores binários de Bent (ver ANEXO B) diferentes de tamanhos 256. Cada vector-coluna representa o valor dum bit de saída para qualquer entradas de dados. Os vectores são escolhidos de tal forma que a sua soma (modulo 2) é altamente não linear e de modo que elas tenham boas propriedades de avalanche. Este processo envolve a escolha de uma coluna de cada vez, efectuando um teste num conjunto de colunas já escolhidas, e depois efectuando outra escolha ou movendo para a próxima coluna.

O processo de geração das subchaves usado no CAST-128 é diferente daqueles aplicados em outros algoritmos de encriptação simétrica. Os autores do CAST se preocuparam em tornar as subchaves o mais resistentes possível a ataques criptoanáliticos e sentiram que o uso de caixas-S não lineares providencia esta força. Como se viu existem algoritmos com os mesmos objectivos, um deles é o Blowfish que usa o próprio algoritmo de encriptação para gerar as subchaves. O RC5 usa uma sequência pseudoaleatória para a inicialização seguida por um conjunto complexo de operações envolvendo rotações de tamanho variável e a adição modulo 2. É difícil dizer qual dessas abordagens é superior. Contudo, nenhuma dessas abordagens parece oferecer maior força criptográfica que a simples substituição-permutação usada no DES.

A função F é desenhada para fazer boa confusão, difusão e efeito avalanche. Usa substituições da caixa-S, adição e subtracção do módulo 2, operação OU-Exclusivo e rotações dependentes da chave. A força da função F baseia-se primariamente na força

das caixas-S, mas além disso o uso da aritmética, booleana, e operadores de rotação adicionam força.

Finalmente, F não é uniforme de estágio para estágio, como foi descrito. Esta dependência de F no número de estágios, pode providenciar mais resistência, apesar disto não ter sido demonstrado ainda.

4.10.5. RC2

RC2 é um algoritmo de encriptação simétrico desenvolvido por Ron Rivest. RC2 usa blocos de texto em claro e texto cifrado de 64 bits e uma chave de tamanho variável de 8 à 1024 bits. O algoritmo foi concebido para ser facilmente implementado em microprocessadores de 16 bits. RC2 é usado em S/MIME com chaves de 40, 64 e 128 bits [16].

4.10.5.1. Expansão da chave

RC5 efectua um conjunto de operações na chave secreta para produzir 128 bytes de subchaves. A subchave é armazenada num array de bytes denominado L[0], L[1], ...,L[127]. Para algumas operações, é conveniente referirmos ao mesmo material da subchave como um array de palavras de 16 bits C[0], C[1], ..., C[63].

Sejam T bytes da chave providenciados, com $1 \leq T \leq 128$. A geração da chave começa colocando T bytes da chave nos bytes L[0], ...,L[T]. O array L é então processado fazendo uso dum array auxiliar de bytes pseudoaleatórios P[0], ..., P[1], ..., P[255], que são baseados nos dígitos de π. O processamento é descrito como:

```
For i = T to 127 do              /* define L[T] até L[127] */
        L[i] = P[L[i - 1] + L[i - T]];
L[128 - T] = P[L[128 - T]];
For i = 127 - T down to 0 do     /* define L[0] até L[127 - T] */
        L[i] = P[L[i + 1] ⊕ L[i + T]];
```

Em geral, o primeiro estágio define cada byte da subchave expandida após os primeiros T bytes para a soma dos bytes das subchaves anteriores e os bytes da subchave T posições anteriores. O segundo estágio define cada byte da subchave exceptuando os últimos T bytes para o XOR da próxima subchave e os bytes de subchave T posições a frente.

4.10.5.2. Encriptação

RC2 usa as seguintes operações primitivas [16]:

- **Adição e subtracção:** adição de palavras, denotada por +, é efectuado módulo 2^{32}. A operação inversa, denotada por -, é subtracção módulo 2^w;
- **Operação OU-Exclusivo:** esta operação é denotada por $\oplus$;
- **Complemento Bitwise:** esta operação é denotada por ~;
- **Operação lógica AND:** esta operação é denotada por &;
- **Rotação circular à esquerda:** a rotação cíclica da palavra x à esquerda y bits é denotado por x <<< y.

Diferente de outras cifras de bloco simétricas, RC2 não usa a estrutura clássica de Fiestel (ver ANEXO D). O que o torna difícil compara-lo aos outros algoritmos.

O algoritmo de encriptação usa uma entrada de 64 bits armazenados nas palavras de 16 bits R[0], R[1], R[2], R[3], e coloca o resultado no R[0] até R[3]. O algoritmo consiste num total de 18 estágios de dois tipos: Mistura e *Mashing*. Um estágio de mistura é expressado:

```
R[0] = R[0] + C[j] + (R[3] & R[2]) + (~R[3] & R[1]);
R[0] = R[0] <<< 1;
j = j + 1;
R[1] = R[1] + C[j] + (R[0] & R[3]) + (~R[0] & R[2]);
R[1] = R[1] <<< 2;
j = j + 1;
R[2] = R[2] + C[j] + (R[1] & R[0]) + (~R[1] & R[3]);
R[2] = R[2] <<< 3;
j = j + 2;
R[3] = R[3] + C[j] + (R[2] & R[1]) + (~R[2] & R[0]);
R[3] = R[3] <<< 5;
j = j + 3;
```

Nesta permutação, C[j] é a primeira palavra da subchave que ainda não foi usada. Pode-se descrever esta operação da seguinte forma, para cada palavra R[i] são executadas as seguintes operações: a próxima palavra C[j] da subchave é adicionada a R[i]. Então R[i - 1], onde o indexe do R é módulo 3, é usado para criar uma palavra "composta" que é adicionada a R[i]. A palavra composta consiste de bits de R[i - 2] naquela posição de bits onde R[i -1] é 1 e dos bits de R[i - 3] naquela posição de bits

onde R[i - 1] é 0. Então, R[i] sofre um deslocamento circular à esquerda e j é incrementado.

Para o estágio de *Mashing*, temos:

```
R[0] = R[0] + K[R[3] & 63];
R[1] = R[1] + K[R[0] & 63];
R[2] = R[2] + K[R[1] & 63];
R[3] = R[3] + K[R[2] & 63];
```

Em palavras, para cada R[i], uma palavra da subchave é adicionada ao R[i]. O array de subchaves é indexado pela ordem mais baixa de 6 bits de R[i - 1].

RC2 pode agora ser definido como (o valor de j após cada passo é indicado em parênteses) [16]:

1. Inicialize j com zero;
2. Executa cinco estágios de Mistura (j = 20);
3. Executa um estágio de *Mashing*;
4. Executa seis estágios de Mistura (j = 44);
5. Executa um estágio de *Mashing*;
6. Executa cinco estágios de Mistura (j = 64);

Cada estágio de Mistura usa 4 palavras da subchave. Existem 16 estágios de Mistura, então todas subchaves são usadas uma vez. De salientar que, as subchaves são seleccionadas duma forma dependente dos dados para os estágios de *Mashing*.

A decriptação é executada no inverso da operação de encriptação, então os estágios são executados e as chaves são usadas na ordem inversa.

4.10.6. IDEA (International Data Encription Algoritm)

O IDEA é uma cifra de bloco (ver ANEXO C) simétrico desenvolvido por Xuejia Lai e James Massey do Instituto Tecnológico Federal da Suíça. Este algoritmo foi desenvolvido para ser resistente aos ataques da Criptoanálise Diferencial (ver ANEXO A). IDEA é um dos algoritmos de encriptação convencional que foi proposto nos últimos tempos para substituir o DES. Em termos de uso o IDEA foi uma das propostas mais bem sucedidas. Por exemplo, o IDEA é usado no PGP, que usa o algoritmo quase na totalidade [16].

4.10.6.1. Princípios de Desenho

O IDEA é uma cifra de bloco que usa uma chave de 128 bits para encriptar dados em blocos de 64 bits. Em comparação com o DES que também usa blocos de 64 bits só que com uma chave de 56 bits.

Os objectivos no desenho do IDEA podem ser agrupados naqueles relacionados com a força criptográfica e os relacionados com a fácil implementação.

4.10.6.2. Força criptográfica

As características do IDEA relacionadas com a força criptográfica são:

1. **Tamanho do bloco:** o bloco deve ser longo o suficiente para deter a análise estatística (isto é, negar ao oponente qualquer vantagem que alguns blocos apareçam mais que outros). Por outro lado, a complexidade na implementação duma função de encriptação eficiente cresce exponencialmente com o tamanho do bloco. O uso dum bloco de 64 bits é geralmente conhecido como suficientemente forte.
2. **Tamanho da chave:** o tamanho da chave deve ser longo o suficiente para prevenir as buscas exaustivas da chave. Com uma chave de 128 bits o IDEA é suficientemente seguro presentemente e futuramente.
3. **Confusão:** o texto cifrado deve depender do texto em claro e da chave duma forma complicada e envolvida. O objectivo é complicar a determinação de como as estatísticas do texto cifrado dependem das estatísticas do texto em claro. IDEA alcança este objectivo usando 3 operações diferentes, o que contrasta com o DES que usa a operação OU-Exclusivo e pequenas Caixas-S não lineares.

4. **Difusão:** todo bit do texto em claro deve influenciar todo bit do texto cifrado, e cada bit da chave deve influenciar todos bits do texto cifrado. A alteração dum único bit do texto em claro altera muitos bits do texto cifrado e esconde assim a estrutura estatística do texto em claro. IDEA é muito eficiente neste aspecto.

Vamos focar-nos um pouco nos últimos dois pontos, a confusão é obtida misturando 3 operações. Cada operação é efectuada em duas entradas de 16 bits que produz uma única saída de 16 bits, as operações são:

- **Bit-por-bit OU-Exclusivo**, denotado por $\oplus$.
- **Adição módulo inteiro** 2^{16} (módulo 65536), com entradas e saídas tratadas como inteiros de 16 bits. Esta operação é denotada por $\boxplus$.
- **Multiplicação módulo de inteiro** $2^{16}+1$ (módulo 65537), com entradas e saídas tratadas como inteiros de 16 bits, exceptuando que o bloco com todos zeros é tratado como representação 2^{16}. Esta operação é denotada por $\odot$. Por exemplo:

  $$0000000000000000 \odot 1000000000000000 = 1000000000000001$$

  Pois,

  $$2^{16} \times 2^{15} \bmod (2^{16}+1) = 2^{15}+1 \qquad (31)$$

A Tabela 15 mostra os valores de 3 operações operando em número de 2 bits (em vez de 16 bits). Estas três operações são incompatíveis de modo que:

1. Nenhum par das três operações satisfazem uma regra distributiva, isto é:

   $$a \boxplus (b \odot c) \neq (a \boxplus b) \odot (a \boxplus c) \qquad (32)$$

X	Y	X ⊞ Y	X ⊙ Y	X ⊕ Y
0 00	0 00	0 00	1 01	0 00
0 00	1 01	1 01	0 00	1 01
0 00	2 10	2 10	3 11	2 10
0 00	3 11	3 11	2 10	3 11
1 01	0 00	1 01	0 00	1 01
1 01	1 01	2 10	1 01	0 00
1 01	2 10	3 11	2 10	3 11
1 01	3 11	0 00	3 11	2 10
2 10	0 00	2 10	3 11	2 10
2 10	1 01	3 11	2 10	3 11
2 10	2 10	0 00	0 00	0 00
2 10	3 11	1 01	1 01	1 01
3 11	0 00	3 11	2 10	3 11
3 11	1 01	0 00	3 11	2 10
3 11	2 10	1 01	1 01	1 01
3 11	3 11	2 10	0 00	0 00

Tabela 15 – Funções usadas no IDEA (para um operando com 2 bits de tamanho) [16].

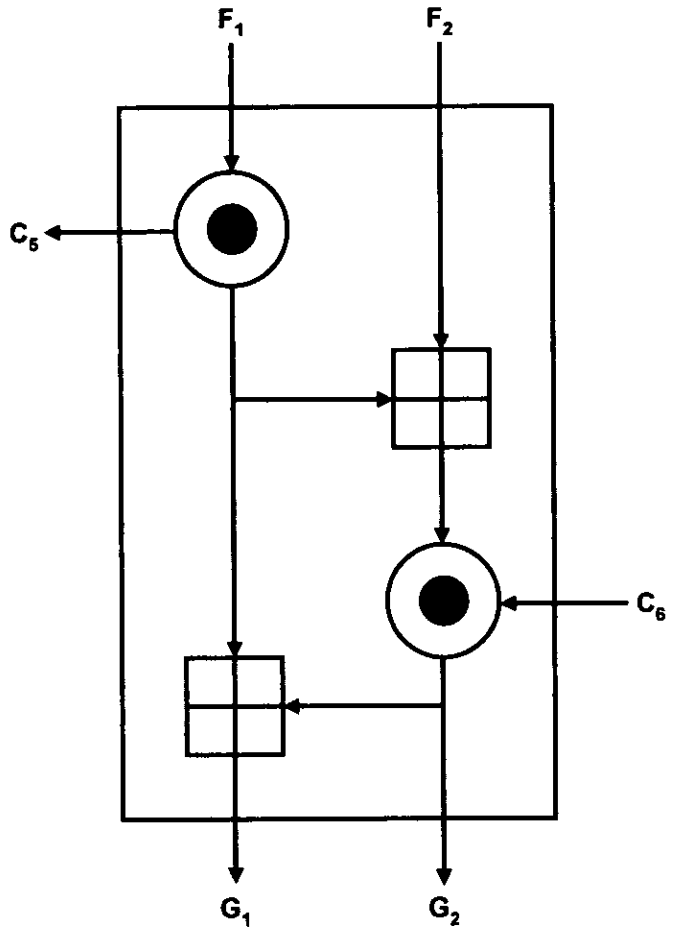


Figura 35 – Estrutura Multiplicação/Adição (M/A) [16].

2. Nenhum par das três operações satisfazem uma regra associativa, isto é:

$$a \boxplus (b \oplus c) \neq (a \boxplus b) \oplus c \qquad (33)$$

O uso dessas três operações separadas em combinação providencia uma complexa transformação da entrada, tornando a criptoanálise mais difícil que com um algoritmo como o DES, que usa a função OU-Exclusivo.

No IDEA, a difusão é providenciada pela construção básica do bloco do algoritmo, conhecida como a Estrutura Multiplicação/Adição (MA) (ver Figura 35). Esta estrutura tem como entrada dois valores de 16 bits que derivam do texto em claro e duas subchaves de 16 bits derivadas da chave e produz uma saída de 16 bits. Uma procura exaustiva computarizada determinou que cada bit de saída do primeiro estágio depende de todos bits da entrada derivados do texto em claro e de todos bits das subchaves. Esta estrutura particular é repetida 8 vezes ao longo do algoritmo, providenciando uma difusão eficaz. Além disso, como se pode ver esta estrutura usa menos número de operações (quatro) necessárias para adquirir uma difusão completa.

4.10.6.3. Consideração de implementação

IDEA é desenhado para facilitar ambas implementações do Software e Hardware. Implementação de Hardware, tipicamente em VLSI, é concebida para adquirir alta velocidade. Implementação de Software tem a vantagem de ser flexível e de baixo custo.

4.10.6.3.1. Implementação em Software:

- **Usa subblocos:** operações da cifra devem operar em subblocos que são "naturais" ao Software, como de 8, 16 ou 32 bits. IDEA usa subblocos de 16 bits;
- **Usa operações simples:** operações da cifra devem ser facilmente programáveis usando a Adição, deslocamento e assim por diante. Os 3 elementos básicos do IDEA cumprem estes requisitos. A mais difícil dos três, a multiplicação modular ($2^{16}+1$), pode ser facilmente construída por operações primitivas.

4.10.6.3.2. Implementação em Hardware:

- **Similaridade entre a encriptação e decriptação:** a encriptação e decriptação devem diferir apenas na forma de uso da chave de modo que o mesmo aparelho possa ser usado para ambos processos o de encriptação e decriptação. Como DES, IDEA possui uma estrutura que satisfaz este requisito;
- **Estrutura regular:** a cifra deve ter uma estrutura modular regular para facilitar a implementação do VLSI. IDEA é construído por dois módulos básicos de construção de blocos repetidos múltiplas vezes.

4.10.6.4. Encriptação

O esquema do IDEA é ilustrado na Figura 36. Como todo esquema de encriptação, existem duas entradas para a função de encriptação: o texto em claro para ser encriptado e a chave. Neste caso o texto em claro é de 64 bits e a chave é de 128 bits.

Olhando para a parte esquerda da Figura 36, vemos que IDEA é constituído por 8 estágios seguidos por uma função de transformação final. O algoritmo divide a entrada em 4 subblocos de 16 bits. Cada um dos estágios toma os quatro subblocos de 16 bits como entrada e produz 4 blocos de saída de 16 bits. A transformação final também produz 4 blocos de 16 bits, que são concatenados para formar o texto cifrado de 64 bits. Cada um dos estágios faz uso de 6 subchaves de 16 bits, onde a transformação

final usa 4 subchaves, para um total de 52 subchaves. A parte direita da Figura 36 indica que essas 52 subchaves são todas geradas da chave original de 128 bits [16].

4.10.6.4.1. Detalhes dum estágio

Na Figura 37 mostra-se o algoritmo do 1º estágio, pois os restantes têm a mesma estrutura. Podemos ver que o IDEA desvia-se um pouco da estrutura clássica de Fiestel (ver ANEXO D). O estágio começa com uma transformação que combina os 4 subblocos de entrada, usando as operações de multiplicação e adição. Esta transformação é destacada pelo rectângulo sombreado mais acima. Os 4 blocos de saída desta transformação são então combinados usando a operação OU-Exclusivo para formar dois blocos de 16 bits que são as entradas da estrutura MA (ver Figura 35) que é mostrada pelo rectângulo sombreado mais abaixo. A estrutura MA também usa duas subchaves como entrada e combina essas entradas para produzir duas saídas de 16 bits.

Finalmente, os 4 blocos de saída da transformação superior são combinados com os dois blocos de saída da estrutura MA usando o OU-Exclusivo para produzir os 4 blocos de saída deste estágio. Note que as duas saídas que são parcialmente geradas pela segunda e terceira entrada (X_2 e X_3) são relacionados para produzir a segunda e terceira saída (W_{12} e W_{13}). Isto incrementa a mistura dos bits que estão a ser processados e torna o algoritmo mais resistente a criptoanálise diferencial (ver ANEXO A).

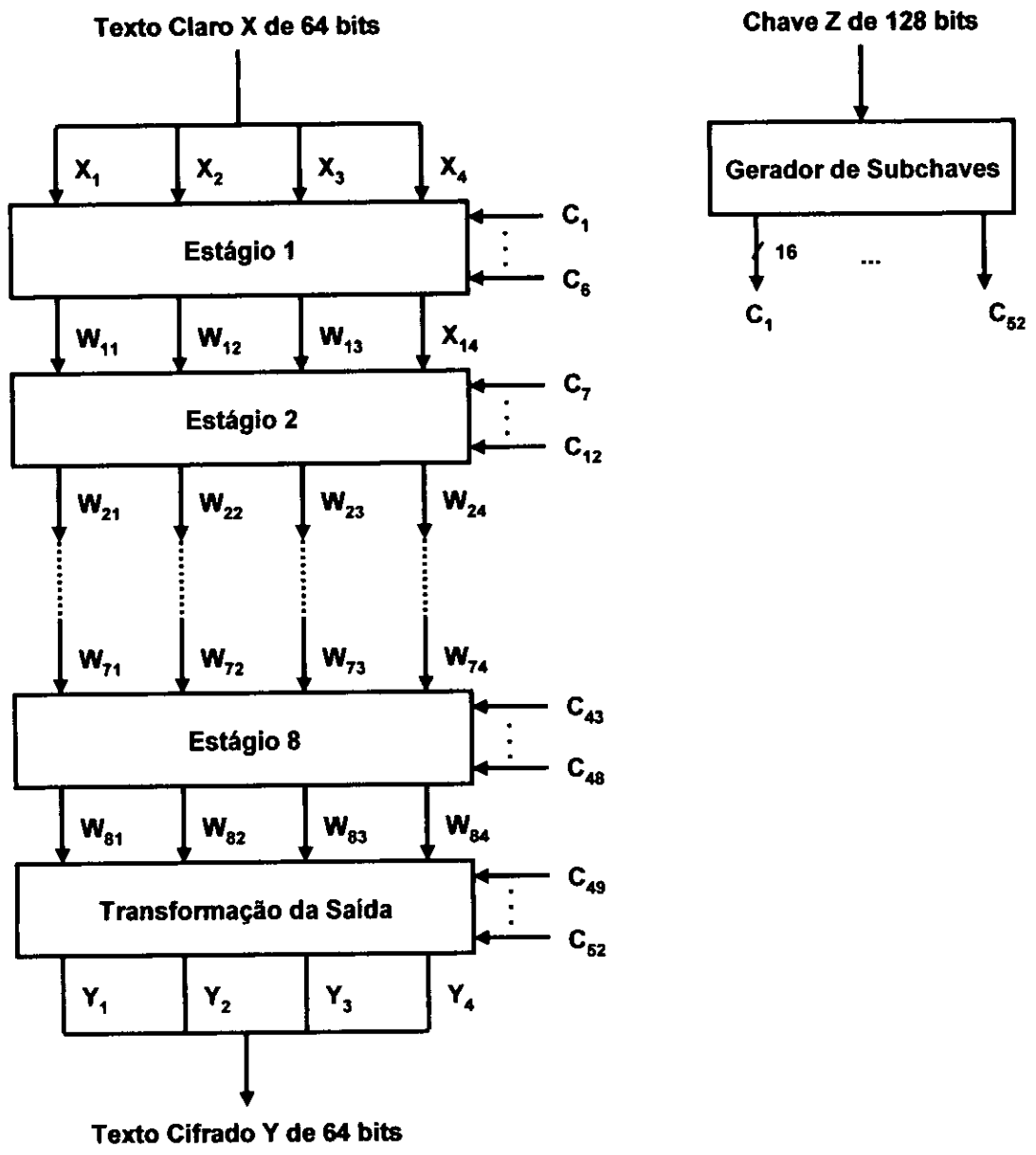


Figura 36 – Estrutura IDEA [16].

O nono estágio do algoritmo, denominado como estágio da transformação da saída da Figura 36 é mostrado na Figura 38. Note que possui a mesma estrutura que as porções sombreadas acima dos estágios precedentes (ver Figura 37). A única diferença é que a segunda e terceira entrada são inter-relacionadas antes de serem aplicadas as unidades operacionais. De facto, isto tem o efeito de desfazer o inter-relacionamento no fim do oitavo estágio. A razão para este inter-relacionamento extra é de que a decriptação tem a mesma estrutura que a encriptação como veremos. Note que este nono estágio requer apenas 4 subchaves de entrada, comparativamente as 6 subchaves de entrada para cada um dos primeiros 8 estágios.

4.10.6.5. Geração da subchave

Retornando a Figura 36, vemos que são geradas 52 subchaves de 16 bits da chave de encriptação de 128 bits. O esquema da geração é o seguinte: as primeiras 8 subchaves denominadas Z_1, Z_2, ..., Z_8, são tiradas directamente da chave, com Z_1 a ser igual aos primeiros 16 bits (mais significantes), Z2 corresponde aos próximos 16 bits, e assim por diante [16].

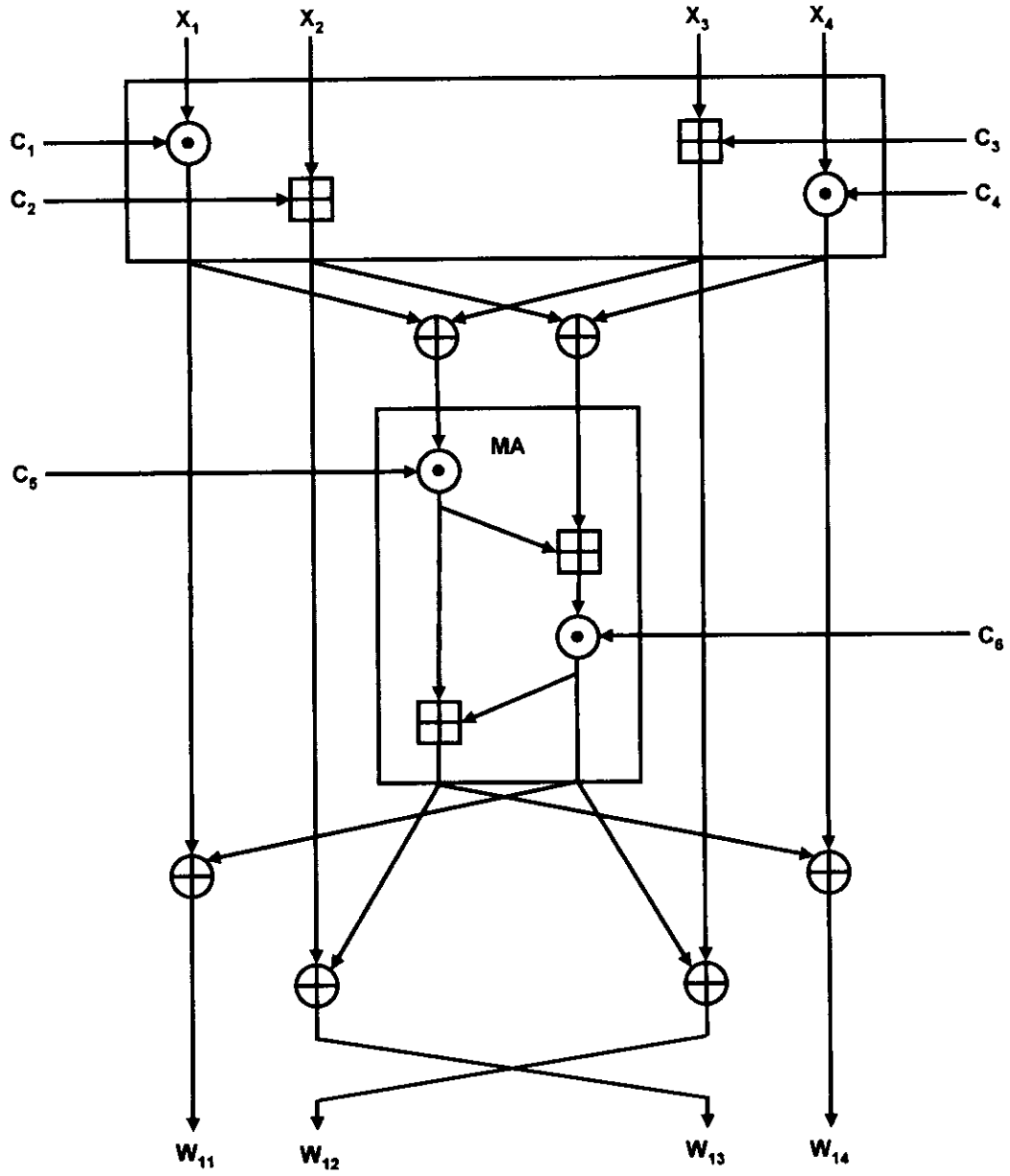


Figura 37 – Estágio Simples do IDEA (Primeiro Estágio) [16].

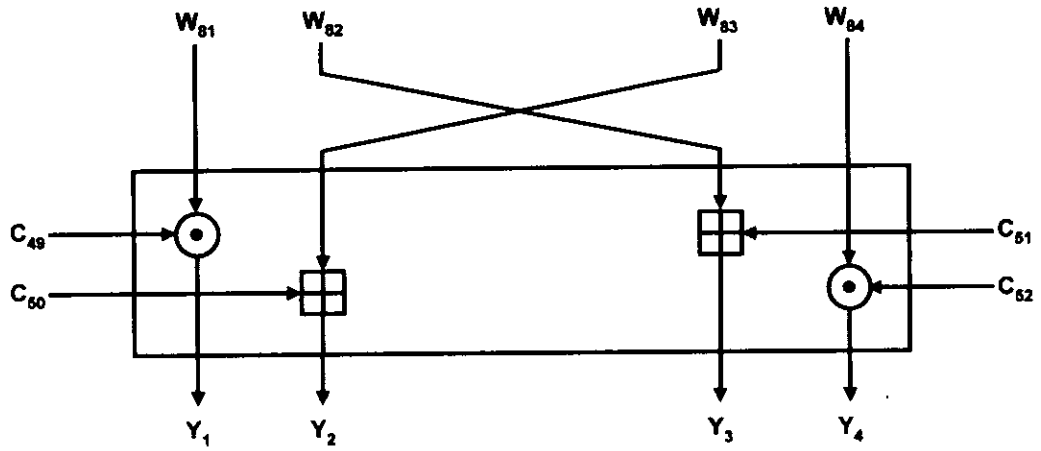


Figura 38 – Estágio da Transformação da Saída do IDEA [16].

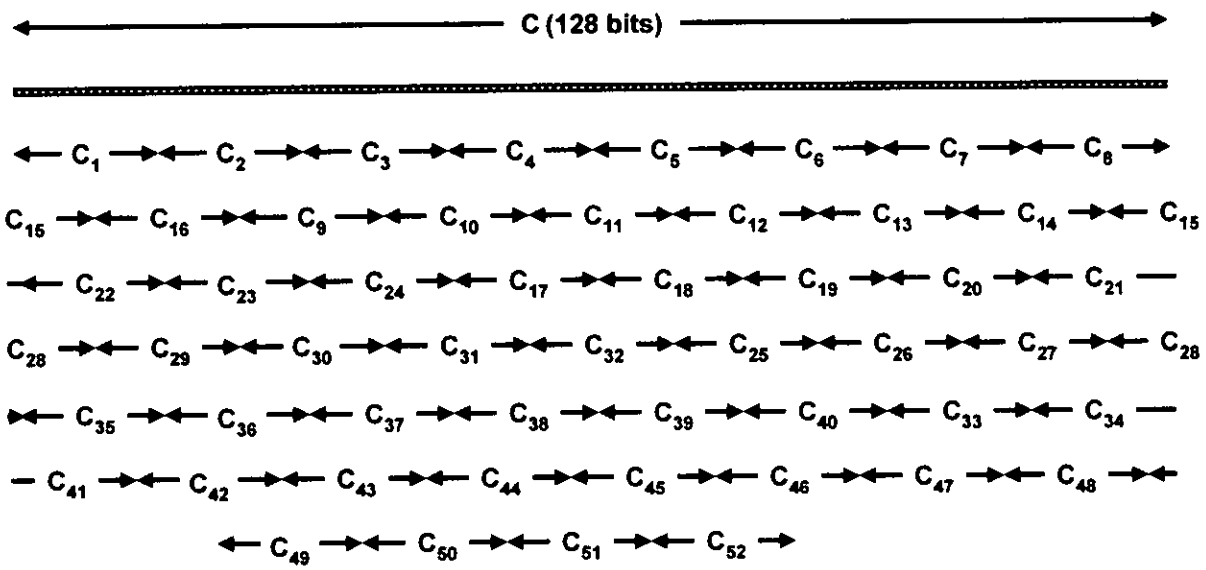


Figura 39 – Subchaves do IDEA.

Após isto, uma deslocação circular a esquerda de 25 posições de bits é aplicado a chave, e as próximas 8 subchaves são extraídas. Este procedimento é repetido até que tenhamos as 52 subchaves. A Figura 39 indica todos os bits de todas as subchaves relativamente a chave original. Este esquema providencia uma técnica eficiente para variar os bits da chave usados para as subchaves nos 8 estágios. Note que a primeira subchave usada em cada estágio usa um conjunto de bits diferente da chave. Se a chave como um todo é denominada C[1..28], então a primeira chave dos 8 estágios teria os seguintes bits:

C_1 = C[1..16]

C_7 = C[94..112]

C_{13} = C[90..105]

C_{19} = C[83..98]

C_{25} = C[76..91]

C_{31} = C[44..59]

C_{37} = C[34..52]

C_{43} = C[30..45]

Os 96 bits das subchaves usados para um estágio são, com a excepção do 1º e 8º estágio, descontínuos, de modo que não há sequer uma simples relação dos deslocamentos entre as subchaves dum estágio e outras dos outros. A razão deste fenómeno é que apenas 6 subchaves são usadas em cada estágio, onde 8 subchaves são extraídas em cada rotação da chave.

4.10.6.6. Decriptação

O processo de decriptação é essencialmente o mesmo que o algoritmo de encriptação. A decriptação é efectuada usando o texto cifrado como entrada para a mesma estrutura IDEA, mostrada na Figura 36, mas com uma selecção das subchaves diferente. As subchaves da decriptação U_1, ..., U_{52} são derivadas das chaves da encriptação da seguinte forma:

1. As primeiras 4 subchaves do estágio i da decriptação são derivadas das primeiras 4 subchaves do estágio (10-i) da encriptação, onde o estágio da transformação é considerado estágio 9. A primeira e quarta subchave da decriptação são iguais ao módulo multiplicativo inverso (2^{16}+1) da correspondente primeira e quarta subchave da encriptação. Para estágios de 2 à 8, a segunda e terceira subchave de decriptação são iguais ao módulo aditivo inverso (2^{16}) da correspondente segunda e terceira segunda subchaves de encriptação;
2. Para os primeiros 8 estágios, as últimas duas subchaves do estágio i da decriptação são iguais as últimas duas subchaves do estágio (9-i) da encriptação.

A Tabela 16 resume estas relações. Para o multiplicativo inverso, é usada a notação Z_j^{-1}, então temos:

$$C_j \odot C_j^{-1} = 1 \qquad (34)$$

Porque $2^{16}+1$ é um número primo, cada inteiro $Z_j \leq 2^{16}$ não zero tem um único módulo multiplicativo inverso $(2^{16}+1)$. Para o módulo aditivo inverso 2^{16}, usa-se a notação $-Z_j$, então temos:

$$-C_j \boxplus C_j = 0 \qquad (35)$$

Para verificar que o mesmo algoritmo com as subchaves de decriptação produz o resultado correcto, considere a Figura 40, que mostra o processo de encriptação a decorrer no lado esquerdo e de decriptação no direito. Cada um dos 8 estágios é mostrado de forma detalhada pelos dois subestágios de transformação que é referido como subencriptação. O subestágio da transformação corresponde ao rectângulo sombreado mais elevado da Figura 37, e o estágio da subencriptação refere-se ao resto do processamento daquele estágio. Considere as caixas debaixo dos dois diagramas. No lado da encriptação, as seguintes relações esperam pela saída da transformação:

$$Y_1 = W_{81} \odot C_{49}$$
$$Y_2 = W_{83} \boxplus C_{50}$$
$$Y_3 = W_{82} \boxplus C_{51}$$
$$Y_4 = W_{84} \odot C_{52}$$

O primeiro subestágio do primeiro estágio do processo de decriptação possui a seguinte relação:

$$J_{11} = Y_1 \odot U_1$$
$$J_{12} = Y_2 \boxplus U_2$$
$$J_{13} = Y_3 \boxplus U_3$$
$$J_{14} = Y_4 \odot U_4$$

Substituindo:

$$J_{11} = Y_1 \odot Z_{49}^{-1} = W_{81} \odot C_{49} \odot Z_{49}^{-1} = W_{81}$$
$$J_{12} = Y_2 \boxplus -Z_{50} = W_{83} \boxplus C_{50} \boxplus -Z_{50} = W_{83}$$
$$J_{13} = Y_3 \boxplus -Z_{51} = W_{82} \boxplus C_{51} \boxplus -Z_{51} = W_{82}$$
$$J_{14} = Y_4 \odot Z_{52}^{-1} = W_{84} \odot C_{52} \odot Z_{52}^{-1} = W_{84}$$

Estágio	Encriptação		Decriptação	
	Designação	Equivalente á	Designação	Equivalente á
Estágio 1	$C_1C_2C_3C_4C_5C_6$	C[1..96]	$U_1U_2U_3U_4U_5U_6$	$C_{49}^{-1} - C_{50} - C_{51}\ C_{52}^{-1}\ C_{47}\ C_{48}$
Estágio 2	$C_7C_8C_9C_{10}C_{11}C_{12}$	C[97..128; 26..89]	$U_7U_8U_9U_{10}U_{11}U_{12}$	$C_{43}^{-1} - C_{45} - C_{44}\ C_{46}^{-1}\ C_{41}\ C_{42}$
Estágio 3	$C_{13}C_{14}C_{15}C_{16}C_{17}C_{18}$	C[90..128; 1..25; 51..82]	$U_{13}U_{14}U_{15}U_{16}U_{17}U_{18}$	$C_{37}^{-1} - C_{39} - C_{38}\ C_{40}^{-1}\ C_{35}\ C_{36}$
Estágio 4	$C_{19}C_{20}C_{21}C_{22}C_{23}C_{24}$	C[83..128; 1..50]	$U_{19}U_{20}U_{21}U_{22}U_{23}U_{24}$	$C_{31}^{-1} - C_{33} - C_{32}\ C_{34}^{-1}\ C_{29}\ C_{30}$
Estágio 5	$C_{25}C_{26}C_{27}C_{28}C_{29}C_{30}$	C[76..128; 1..43]	$U_{25}U_{26}U_{27}U_{28}U_{29}U_{30}$	$C_{25}^{-1} - C_{27} - C_{26}\ C_{28}^{-1}\ C_{23}\ C_{24}$
Estágio 6	$C_{31}C_{32}C_{33}C_{34}C_{35}C_{36}$	C[44.75; 101..128; 1..36]	$U_{31}U_{32}U_{33}U_{34}U_{35}U_{36}$	$C_{19}^{-1} - C_{21} - C_{20}\ C_{22}^{-1}\ C_{17}\ C_{18}$
Estágio 7	$C_{37}C_{38}C_{39}C_{40}C_{41}C_{42}$	C[37..100; 126..128; 1..29]	$U_{37}U_{38}U_{39}U_{40}U_{41}U_{42}$	$C_{13}^{-1} - C_{15} - C_{14}\ C_{16}^{-1}\ C_{11}\ C_{12}$
Estágio 8	$C_{43}C_{44}C_{45}C_{46}C_{47}C_{48}$	C[30..125]	$U_{43}U_{44}U_{45}U_{46}U_{47}U_{48}$	$C_7^{-1} - C_9 - C_8\ C_{10}^{-1}\ C_5\ C_6$
Transformação	$C_{49}C_{50}C_{51}C_{52}$	C[23..86]	$U_{49}U_{50}U_{51}U_{52}$	$C_1^{-1} - C_2 - C_3\ C_4^{-1}$

Tabela 16 – Subchaves da Encriptação e Decriptação [16].

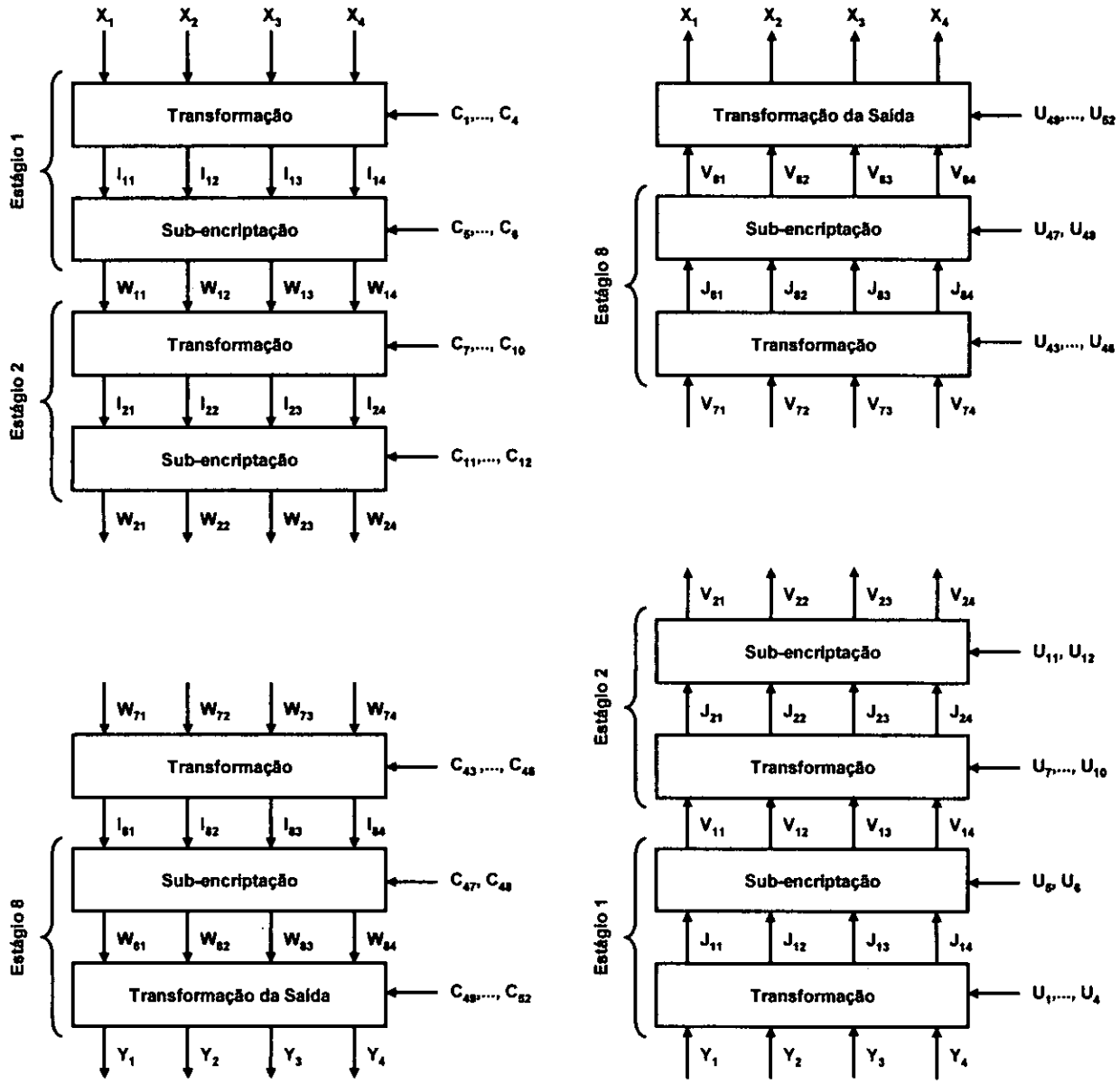


Figura 40 – Encriptação e Decriptação IDEA [16].

Assim, a saída do primeiro subestágio do processo de decriptação é igual a entrada do último estágio o processo de encriptação, exceptuando o intercâmbio do 2º e 3º bloco. Agora considere as seguintes relações, que pode ser derivado da Figura 37:

$$W_{81} = I_{81} \oplus MA_D\,(I_{81} \oplus I_{83},\ I_{82} \oplus I_{84})$$

$$W_{82} = I_{82} \oplus MA_D\,(I_{81} \oplus I_{83},\ I_{82} \oplus I_{84})$$

$$W_{83} = I_{83} \oplus MA_E\,(I_{81} \oplus I_{83},\ I_{82} \oplus I_{84})$$

$$W_{84} = I_{84} \oplus MA_E\,(I_{81} \oplus I_{83},\ I_{82} \oplus I_{84})$$

Onde:

MA_D (X, Y) é a saída da direita da estrutura MA com entradas X e Y e MA_E (X, Y) é a saída da esquerda da estrutura MA com entradas X e Y. Agora [16]:

$$V_{11} = J_{11} \oplus MA_D (J_{11} \oplus J_{13}, J_{12} \oplus J_{14}) = W_{81} \oplus MA_D (W_{81} \oplus W_{83}, W_{82} \oplus W_{84}) = I_{81} \oplus MA_D (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MA_D [I_{81} \oplus MA_D (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{83} \oplus MA_E (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}), I_{82} \oplus MA_D (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus I_{84} \oplus MA_E (I_{81} \oplus I_{83}, I_{82} \oplus I_{84})] = I_{81} \oplus MA_D (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) \oplus MA_D (I_{81} \oplus I_{83}, I_{82} \oplus I_{84}) = I_{81}$$

Similarmente temos:

$$V_{12} = I_{82}$$

$$V_{13} = I_{83}$$

$$V_{14} = I_{84}$$

Então a saída do segundo subestágio do processo de decriptação é igual a entrada do próximo-para-último subestágio do processo de encriptação exceptuando o caso da inter-relação do 2º e 3º blocos. Usando a mesma derivação, esta relação pode ser mostrada para guardar a cada ponto correspondente na Figura 40, até que teremos:

$$V_{81} = I_{11}$$

$$V_{82} = I_{12}$$

$$V_{83} = I_{13}$$

$$V_{84} = I_{14}$$

Finalmente, porque a transformação da saída do processo de decriptação é igual ao primeiro subestágio do processo de encriptação excepto no caso do intercâmbio do 2º e 3º blocos, tem-se a saída de todo processo de encriptação igual a entrada do processo de encriptação.

CAPÍTULO V

NÚMEROS DE FIBONACCI

- Fórmula Geral
- A Secção Doirada
- Vantagens do Uso dos Códigos de Fibonacci na Criptografia
- Operação Lógica do Tipo-R
- Operação Lógica do Tipo-S
- Conversão do Sistema Binário para Fibonacci e Vice-Versa
- Álgebra Booleana

5. NÚMEROS DE FIBONACCI

O Sistema de Fibonacci é um sistema de numeração Posicional com base irracional que permite realizar operações aritméticas e lógicas e utiliza só dois números 0 e 1 que são designados por *bit* (binary digit). Pressupõe-se que ele tenha surgido através dum desafio colocado pelo Imperador Frederico II, no século XIII, em que o matemático italiano *Leonardo Fibonacci* (ver Figura 41) participou, o desafio consistia em solucionar o seguinte problema [35]:

Um fazendeiro cria coelhos. Cada coelho dá origem a um coelho quando ele completa 2 meses de idade, e daí em diante a um coelho a cada mês. Os coelhos nunca morrem, e ignoramos os machos. Quantos coelhos terá o fazendeiro no n-ésimo mês, se ele começar com um coelho recém-nascido?

Figura 41 – Leonardo Fibonacci [35].

De acordo com o suposto, Fibonacci começou analisando o resultado para um número pequeno de valores, através desta análise ele foi obtendo uma sequência de números e logo viu necessidade de deduzir um termo geral para a sequência. Com os resultados da análise Fibonacci estipulou que a sequência começa com 0 e 1, pelo que, a regra para a geração dos restantes números seria [38]:

"Adicionar os dois últimos números para obter o seguinte"

Sendo assim, teríamos:

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Deste modo, os números de Fibonacci podem ser são definidos como:

$$F_n = F_{n-2} + F_{n-1} \qquad (36)$$

Onde:

$F_1 = 1$

$F_2 = 1$

$n \geq 3$

A Tabela 17 ilustra alguns Números Decimais representados na Codificação de Fibonacci.

5.1. Formula Geral dos Códigos de Fibonacci

Para generalizar a recursividade da sua regra, Fibonacci definiu a Formula [11]:

$$F_p(n) = F_p(n-1) + F_p(n-p-1) \qquad (37)$$

Onde:

$p \in \{1, 2, 3, ...\}$ é parâmetro de código irracional

$F(1) = ... = F(p+1) = 1$

$n > p + 1$

A Formula (37) pode ser vista como uma Família de sequências dos Códigos de Fibonacci, pois para cada valor de p obtemos uma sequência de valores diferentes. Neste trabalho irei trabalhar apenas com a família p=1.

Exemplo:

- Para $p = 1 \Rightarrow F_1(n) = F_1(n-1) + F_1(n-2)$, é o caso da Formula (36).
- Para $p = 2 \Rightarrow F_2(n) = F_2(n-1) + F_2(n-3)$, gera-se o valor seguinte somando o último e o antepenúltimo valor da sequência, então a sequência seria:

  1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, ...
- Para $p = 3 \Rightarrow F_3(n) = F_3(n-1) + F_3(n-4)$, gera-se o valor seguinte somando o último e o ante antepenúltimo valor da sequência, então a sequência seria:

  1, 1, 1, 1, 2, 3, 4, 5, 7, 10, 14, 19, 26, 36, 50, 69, ...

	F(13)	F(12)	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	233	144	89	55	34	21	13	8	5	3	2	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	1	0
2	0	0	0	0	0	0	0	0	0	0	1	0	0
3	0	0	0	0	0	0	0	0	0	1	0	0	0
4	0	0	0	0	0	0	0	0	0	1	0	1	0
5	0	0	0	0	0	0	0	0	1	0	0	0	0
6	0	0	0	0	0	0	0	0	1	0	0	1	0
7	0	0	0	0	0	0	0	0	1	0	1	0	0
8	0	0	0	0	0	0	0	1	0	0	0	0	0
9	0	0	0	0	0	0	0	1	0	0	0	1	0
10	0	0	0	0	0	0	0	1	0	0	1	0	0
11	0	0	0	0	0	0	0	1	0	1	0	0	0
12	0	0	0	0	0	0	0	1	0	1	0	1	0
13	0	0	0	0	0	0	1	0	0	0	0	0	0
14	0	0	0	0	0	0	1	0	0	0	0	1	0
15	0	0	0	0	0	0	1	0	0	0	1	0	0
16	0	0	0	0	0	0	1	0	0	1	0	0	0
17	0	0	0	0	0	0	1	0	0	1	0	1	0
18	0	0	0	0	0	0	1	0	1	0	0	0	0
19	0	0	0	0	0	0	1	0	1	0	0	1	0
20	0	0	0	0	0	0	1	0	1	0	1	0	0

Tabela 17 – Representação de alguns Número Decimais usando a codificação de Fibonacci (p=1).

5.2. A secção doirada

A secção doirada é um valor especial relacionado com a série de Fibonacci. Este valor é obtido dividindo dois valores sucessivos. Produzindo o gráfico desses valores pode-se reparar que o mesmo tende a uma limite (ver Gráfico 2), esse limite é a raiz positiva duma equação quadrática e é denominada *secção doirada* denotada por φ (PHI) [29].

$$D(n) = \frac{F(n-1)}{F(n-2)} \qquad (38)$$

Onde:

$n > 2$

Se tomarmos dois números sucessivos da série, a e b, e a + b, então:

$$\frac{b}{a} \cong \frac{a+b}{b} \cong \frac{a}{b} + 1 \qquad (39)$$

Definimos a secção doirada, φ, como sendo o limite de $\frac{b}{a}$, então:

$$\begin{aligned} \phi &= \frac{\phi}{1} + 1 \\ \phi^2 - \phi - 1 &= 0 \qquad (40) \\ \phi &= \frac{1+\sqrt{5}}{2} \approx 1.618 \end{aligned}$$

Para elucidar melhor o valor do limite de $\frac{b}{a}$, vamos olhar para a Tabela 18 onde são mostrados alguns Códigos de Fibonacci e a divisão entre eles.

n	F(n) = F(n-1) + F(n-2)	D(n) = F(n-1) / F(n-2)
1	1	-
2	1	1
3	2	2
4	3	1,5
5	5	1,666666667
6	8	1,6
7	13	1,625
8	21	1,615384615
9	34	1,619047619
10	55	1,617647059
11	89	1,618181818
12	144	1,617977528
13	233	1,618055556
14	377	1,618025751
15	610	1,618037135
16	987	1,618032787
17	1597	1,618034448
18	2584	1,618033813
19	4181	1,618034056
20	6765	1,618033963

Tabela 18 – Divisão de alguns Códigos de Fibonacci.

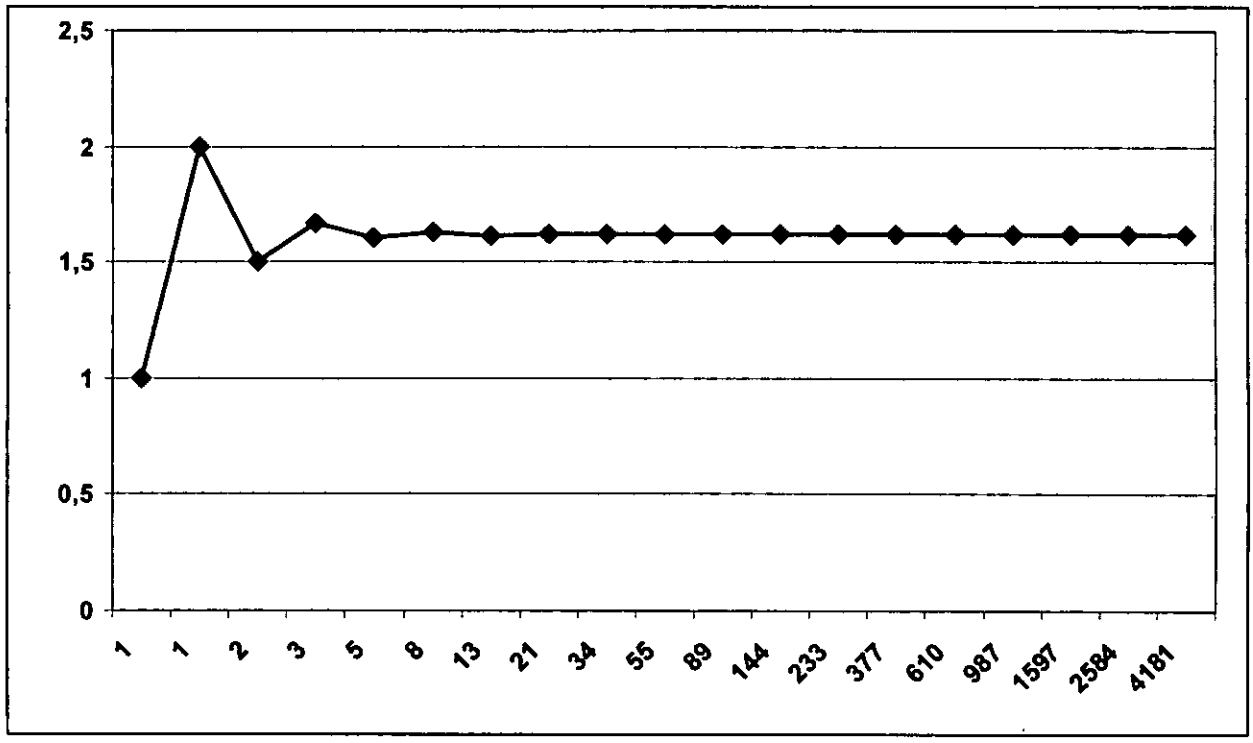


Gráfico 2 – Gráfico das divisões entre os Códigos de Fibonacci.

5.3. Vantagens do uso dos Códigos de Fibonacci na Criptografia

Incorporando os Números de Fibonacci num sistema criptográfico permite-nos, além da criptografia/decriptografia:

- Determinar e corrigir os erros que podem ocorrer durante a transmissão da informação digital através do meio de transmissão, e;
- Compactar os Códigos Binários dos algoritmos criptográficos.

5.4. Operação Lógica do Tipo-R

Pode-se definir a operação Lógica do Tipo-R como uma decomposição de um bit, n, com valor "1" da codificação de Fibonacci em dois bits, n-1 e n-2, com valor lógico "1" que antecedem a n, de realçar que, esta operação só pode ter lugar se os bits n-1 e n-2 tiverem o valor lógico "0" (ver a Tabela 19).

	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	**89**	**55**	**34**	**21**	**13**	**8**	**5**	**3**	**2**	**1**	**1**
101	1	0	0	0	0	1	0	1	0	1	0
101	0	1	1	0	0	1	0	1	0	1	0
101	0	1	0	1	1	1	0	1	0	1	0

Tabela 19 – Exemplo da Operação do Tipo-R.

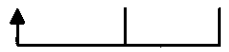
A operação Lógica do Tipo-R é simbolizada por  .

5.5. Operação Lógica do Tipo-S

A operação Lógica do Tipo-S é inversa a do Tipo-R, isto é, dois bits, n-1 e n-2, com valor "1" geram um bit, n, com valor lógico "1", claro que o bit n deve possuir valor lógico "0" (ver Tabela 20).

	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	**89**	**55**	**34**	**21**	**13**	**8**	**5**	**3**	**2**	**1**	**1**
101	0	1	0	1	1	1	0	1	0	1	0
101	0	1	1	0	0	1	0	1	0	1	0
101	1	0	0	0	0	1	0	1	0	1	0

Tabela 20 – Exemplo da Operação do Tipo-S.

A operação Lógica do Tipo-R é simbolizada por  .

A operação do Tipo-S permite-nos obter a forma mínima da codificação de Fibonacci. Na forma mínima uma codificação de Fibonacci possui os bits com valor lógico "1" separados minimamente de ambos lados por um bit de valor lógico "0". É esta característica que permite-nos detectar erros e corrigir alguns que ocorrem durante a transmissão [11].

Por exemplo, suponhamos que o carácter A possui a combinação 10010101 na codificação de Fibonacci, ao transmitir-se este carácter pode ocorrer um erro e o quinto

bit ser alterado para o valor lógico "1", neste caso o receptor iria receber 10011101 em vez de 10010101, de acordo com o critério estipulado ao se encontrar dois bits com valor lógico "1" seguidos podemos afirmar que ocorreu um erro e em certos casos podemos até tentar recuperar a informação original.

5.6. Conversão do Sistema Binário para Fibonacci e Vice-Versa

A maior parte dos algoritmos criptográficos baseiam-se no sistema de numeração binário, daí a necessidade de se descrever o processo de conversão do sistema binário para o de Fibonacci e vice-versa.

5.6.1. Conversão do Sistema Binário para Fibonacci

Para fazer a conversão do Sistema Binário para o Fibonacci, primeiro temos que converter os números do Sistema Binário para o Decimal e por fim de Decimal para Fibonacci.

5.6.1.1. Conversão do Sistema Binário para Decimal

Existem vários métodos para efectuar esta conversão, um deles consiste em:

1. Contar o número de bits, n, da palavra binária;
2. Preencher a equação (41):

$$ND = B_n*2^{n-1} + B_{n-1}*2^{n-2} + \ldots + B_1*2^0 \quad (41)$$

   Onde B_i é o valor binário do Bit, podendo ser "1" (um) ou "0" (zero).
3. Calcular a Formula (41).

Exemplo: Suponhamos que o úmero binário seja $(10010101)_2$, transformando para o Sistema Decimal teríamos:

$$ND = 1*2^7 + 0*2^6 + 0*2^5 + 1*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0$$

$$ND = 128 + 0 + 0 + 16 + 0 + 4 + 0 + 1$$

$$ND = 149$$

Então, $(10010101)_2 = (149)_{10}$

5.6.1.2. Conversão do Sistema Decimal para Fibonacci

Para a conversão de Números do Sistema Decimal para Fibonacci, deve-se:

1. Percorrer a sequência de Fibonacci, da Tabela 21, da esquerda para a direita a procura do valor mínimo maior ou igual ao Número Decimal a ser codificado;

2. Ao encontrar o valor subtrai-se o mesmo ao número decimal, com o resultado dessa subtracção repete-se o Passo 1 e 2, até diferença ser nula, ou igual a "0" (Zero);
3. Preenche-se com zero os restantes espaço vazios.

Exemplo: Vamos codificar o número $(149)_{10}$, pelo que o valor mínimo maior que 149 é 144. Efectuando a diferença temos 149 – 144 = 5. Repetindo o processo, agora com 5, vemos que o valor mínimo igual a 5 é 5. Calculando a diferença vemos que 5 – 5 = 0, e então terminamos o processo (ver Tabela 21).

	F(13)	F(12)	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	233	144	89	55	34	21	13	8	5	3	2	1	1
149	0	1	0	0	0	0	0	0	1	0	0	0	0

Tabela 21 – Exemplo da Conversão do Sistema Decimal para Fibonacci.

Deste modo, podemos afirmar que $(10010101)_2 = (100000010000)_F$.

5.6.2. Conversão dos Números de Fibonacci para o sistema Binário

Para fazer a conversão dos Números de Fibonacci para o Sistema Binário, primeiro temos que converter os números de Fibonacci para o Sistema Decimal e por fim de Decimal para Binário.

5.6.2.1. Conversão dos Números de Fibonacci para o sistema Decimal

Para fazer esta conversão deve-se:

1. Contar o número de bits, n, da palavra binária;
2. Preencher a equação (42):

$$ND = B_n*F(n) + B_{n-1}*F(n-1) + \ldots + B_1*F(1) \quad (42)$$

Onde B_i é o valor binário do Bit, podendo ser "1" (um) ou "0" (zero) e F(i) é o número i da sequência de Fibonacci.

3. Calcular a Formula (42).

Exemplo: Usando o exemplo anterior vamos converter o número $(100000010000)_F$, transformando para o Sistema Decimal teríamos:

ND = 1*F(12) + 0*F(11) + 0*F(10) + 0*F(9) + 0*F(8) + 0*F(7) + 0*F(6) + 1*F(5) + 0*F(4) + 0*F(3) + 0*F(2) + 0*F(1)

ND = 1*144 + 0*89 + 0*55 + 0*34 + 0*21 + 0*13 + 0*8 + 1*5 + 0*3 + 0*2 + 0*1 + 0*1

ND = 144 + 0 + 0 + 0 + 0 + 0 + 0 + 5 + 0 + 0 + 0 + 0

ND = 149

Então, $(100000010000)_F = (149)_{10}$

5.6.2.2. Conversão do Sistema Decimal para Binário

Para a conversão de Números Decimais para Fibonacci, deve-se:

1. Dividir o Número Decimal por 2;
2. Se o resultado da divisão acima for diferente de "0" (zero) ou "1" (um) então repete-se o Passo 1; se for "0" ou "1" forma-se o Número Binário concatenando o resultado da última divisão e os restos das divisões efectuadas começando da última até a primeira.

Exemplo: Vamos, agora, codificar o número $(149)_{10}$, iniciamos o processo dividindo o 149 por 2, e assim sucessivamente (ver Figura 42).

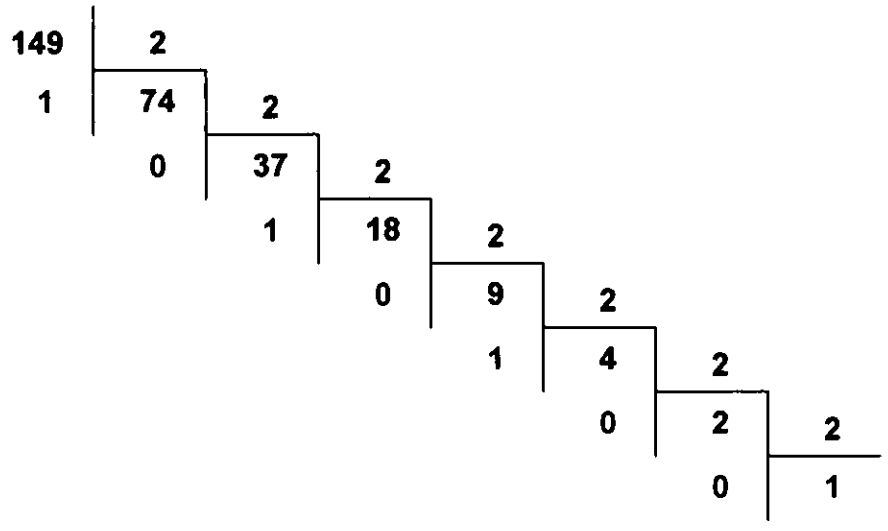


Figura 42 – Exemplo de conversão do Sistema Decimal para Binário.

Deste modo, podemos afirmar que $(149)_{10} = (10010101)_2$.

5.7. Álgebra Booleana para os Números de Fibonacci

5.7.1. Operadores Lógicos

5.7.1.1. AND

Pela tabela de verdade que se segue nota-se que a saída é 1 só quando ambas entradas são iguais a 1 (ver Tabela 22).

Entrada		Saída
A	B	S
0	0	0
0	1	0
1	0	0
1	1	1

Tabela 22 – Tabela de Verdade da Operação Lógica AND.

5.7.1.2. OR

Pela tabela de verdade que se segue nota-se que a saída é 1 sempre que uma das entradas for 1, o que em notação algébrica podemos definir como soma lógica (ver Tabela 23).

Entrada		Saída
A	B	S
0	0	0
0	1	1
1	0	1
1	1	1

Tabela 23 – Tabela de Verdade da Operação Lógica OR.

5.7.1.3. NOT

Da tabela de verdade em baixo nota-se que a saída de circuito é sempre inverso da entrada (ver Tabela 24).

Entrada	Saída
A	S
0	1
1	0

Tabela 24 – Tabela de Verdade da Operação Lógica NOT.

5.7.1.4. NAND

Como o nome diz este circuito é a negação do circuito AND (ver Tabela 25).

Entrada		Saída
A	B	S
0	0	1
0	1	1
1	0	1
1	1	0

Tabela 25 – Tabela de Verdade da Operação Lógica NAND.

5.7.1.5. NOR

A descrição que se pode fazer sobre a formação desta função é idêntica a do caso da função NAND, sendo a diferença a de usar as funções OR e NOT (ver Tabela 26).

Entrada		Saída
A	B	S
0	0	1
0	1	0
1	0	0
1	1	0

Tabela 26 – Tabela de Verdade da Operação Lógica NOR.

5.7.1.6. EXOR (OR EXCLUSIVO)

Embora composta por várias portas lógicas o circuito EXOR pode ser considerado um circuito básico, devido a sua grande utilidade prática, por exemplo dos circuitos de soma binária (1 + 1 = 0, veja a tabela) (ver Tabela 27).

Entrada		Saída
A	B	S
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 27 – Tabela de Verdade da Operação Lógica EXOR.

5.7.1.7. EXOR NOT

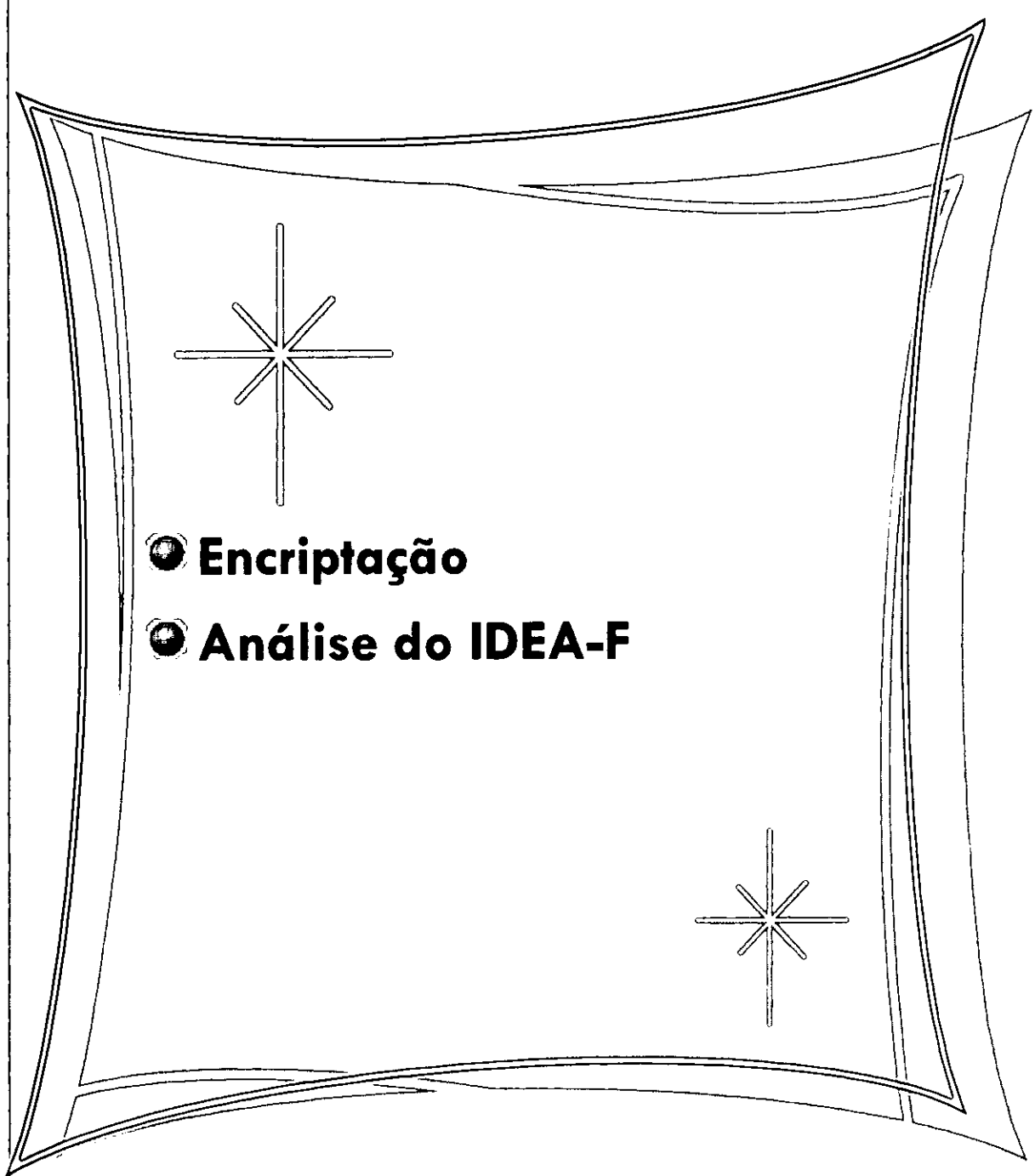
O circuito NÃO-OU-EXCLUSIVO, é também como comparador digital ou circuito coincidência (ver Tabela 28).

Entrada		Saída
A	B	S
0	0	1
0	1	0
1	0	0
1	1	1

Tabela 28 – Tabela de Verdade da Operação Lógica EXOT NOT.

CAPÍTULO VI

ALGORITMO IDEA-F



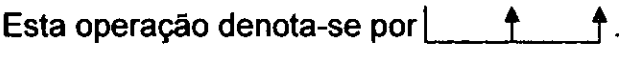
- Encriptação
- Análise do IDEA-F

6. ALGORITMO IDEA-F

O IDEA-F é um sistema de Criptografia Convencional concebido a partir do algoritmo Simétrico IDEA. Ele opera em blocos de texto de 64 bits e usa uma chave de 128 bits. Uma das características que o difere do IDEA é o facto de ele produzir Texto Cifrado de tamanho variável, isto é, ele recebe Texto em claro de 64 bits mas produz Texto cifrado de tamanho 2 à 98 bits, o que dificulta a criptoanálise pois o tamanho da palavra transmitida é variável.

O IDEA-F faz uso dos Números de Fibonacci (parâmetro 1) o que lhe permite detectar e corrigir possíveis erros que possam ocorrer durante a transmissão.

Em termos de implementação, o IDEA-F contempla as seguintes operações:

- **Bit-por-bit OU-Exclusivo**, denotado por $\oplus$.
- **Adição módulo inteiro** 2^{16} (módulo 65536), com entradas e saídas tratadas como inteiros de 16 bits. Esta operação é denotada por $\boxplus$.
- **Multiplicação módulo de inteiro** $2^{16}+1$ (módulo 65537), com entradas e saídas tratadas como inteiros de 16 bits, exceptuando que o bloco com todos zeros é tratado como representação 2^{16}. Esta operação é denotada por $\odot$.
- **Operação do Tipo-S**, para obtenção da forma Mínima dos Códigos de Fibonacci. Esta operação denota-se por  .
- **Operação do Tipo-R**, para obtenção da forma não Mínima dos Códigos de Fibonacci. Esta operação denota-se por  .

6.1. Encriptação

Dum modo geral, a encriptação do IDEA-F (ver Figura 43) consiste em receber o texto em claro de 64 bits (X) e a chave de 128 bits (C) e produzir o texto cifrado intermédio de 64 bits (L) usando o algoritmo IDEA. Após a obtenção do texto cifrado intermédio este passa por um processo de conversão para a codificação de Fibonacci, visto que o IDEA processa o texto no Sistema Binário. Uma vez terminada a conversão, o texto cifrado intermédio (LF), agora na codificação de Fibonacci e na sua Forma Mínima (FM), é submetido a um Dispositivo Lógico que transforma o mesmo da Forma Mínima para a Forma Não Mínima (ÑFM), produzindo assim o texto resultante (Z). O IDEA-F possibilita, ainda, a escolha dos diferentes textos cifrados intermediários, isto é, o emissor pode optar por enviar a cifra que resulta do algoritmo IDEA (Texto Cifrado

Intermédio) em código Binário, ou enviar o da conversão de Binário para Fibonacci (Texto Cifrado Intermédio na Codificação de Fibonacci) e, por fim, o do Dispositivo Lógico (Texto Comprimido). Esta escolha é controlada pelo uso do Dispositivo de Comando. Todos estes processos são depois concatenados no Porto de Saída que produz o Texto Cifrado (Y) final que é depois enviado ao respectivo receptor.

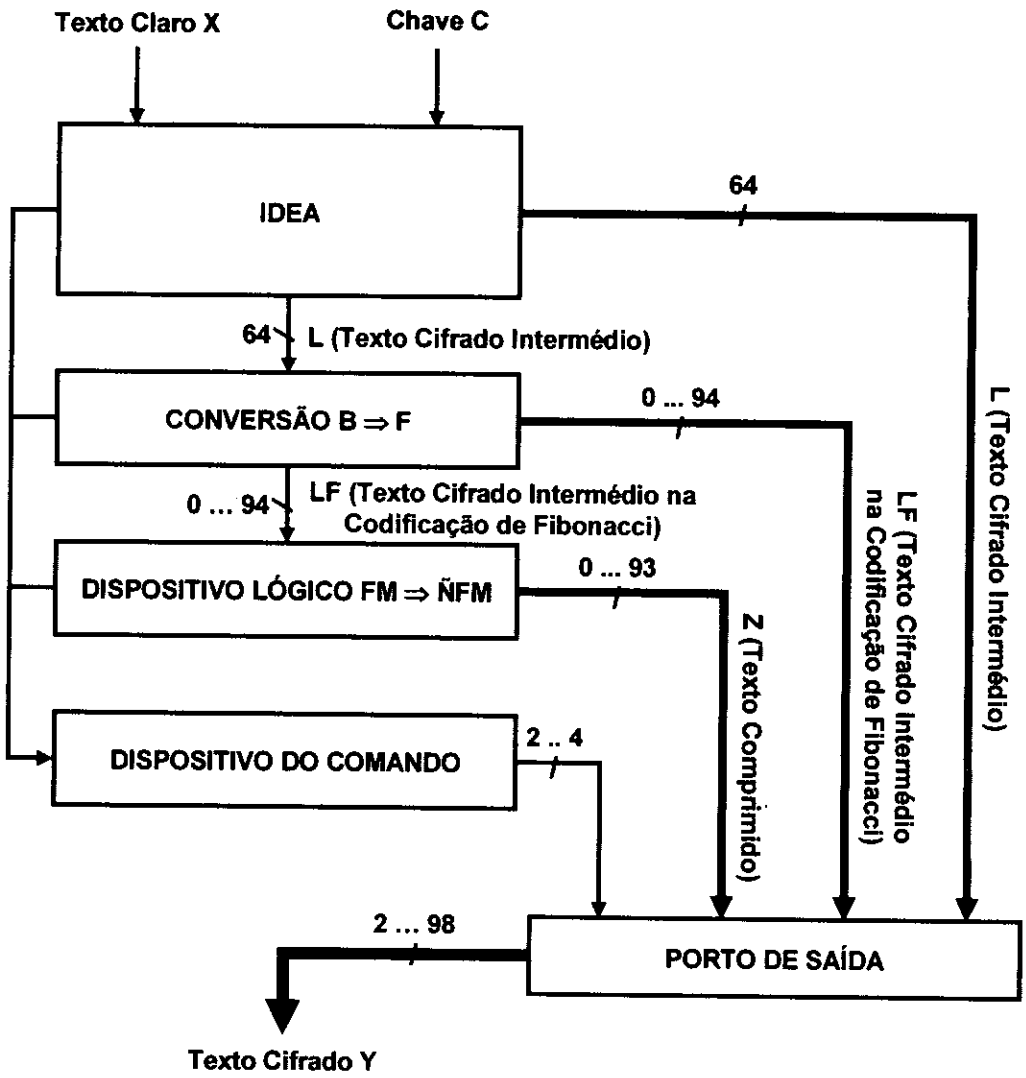


Figura 43 – Esquema de encriptação do IDEA-F.

6.2. Análise do IDEA-F

Vamos agora analisar as fases inerentes neste algoritmo.

6.2.1. IDEA

Como se pode ver pela Figura 43, o IDEA possui duas entradas, uma para o bloco do texto em claro de 64 bits e outra para a chave de 128 bits. Como se pôde ver no Capitulo anterior o IDEA é constituído por 8 estágios seguidos por uma função de transformação final. O algoritmo divide a entrada em 4 subblocos de 16 bits. Cada um

dos estágios toma os quatro subblocos de 16 bits como entrada e produz 4 blocos de saída de 16 bits. A transformação final também produz 4 blocos de 16 bits, que são concatenados para formar o texto cifrado intermédio de 64 bits (L). Cada um dos estágios faz uso de 6 subchaves de 16 bits, onde a transformação final usa 4 subchaves, para um total de 52 subchaves. Como se pode ver pela descrição, o IDEA produz um bloco de 64 bits, de tamanho fixo, que permite representar 2^{64} = 18.446.744.073.709.551.616 números que vão de 0 à $2^{64} - 1$ = 18.446.744.073.709.551.615.

Se o emissor optar por enviar a cifra resultante do IDEA, não obterá vantagem alguma, pois o tempo de envio continuará longo visto que o tamanho da palavra continuará sendo de 64 bits, não será possível detectar erros, que advêm da transmissão, pois a cifra estará na forma Binária.

6.2.2. Conversão B ⇒ F

Permite a conversão do Texto Cifrado Intermédio (L) de 64 bits, que é o resultado do IDEA, do Sistema Binário para a codificação de Fibonacci, produzindo assim o Texto Cifrado Intermédio na Codificação de Fibonacci (LF) de blocos de tamanho variável com 0 á 94 bits. De realçar que, após a conversão, o número na codificação de Fibonacci encontra-se na sua Forma Mínima (FM).

Se o emissor optar por enviar esta cifra ele terá algumas vantagens, nomeadamente:

- Por apresentar um tamanho variável, *minimiza o uso do meio de transmissão* e ocupa-o apenas com bits significativos, o que diminui, também, a *probabilidade de ocorrência de erros* e *aumenta a velocidade de transmissão;*
- Como se pode ver pela Tabela 29, os Números de Fibonacci na sua forma Mínima possuem padrões de "0" (Zeros) e "1" (uns) próprios, por exemplo, não possuem dois "1" (uns) consecutivos, isto é, entre dois "1" (uns) existe sempre um ou mais zeros. Com base neste padrão podem-se *detectar erros de transmissão, aumentando assim a veracidade da informação.*

	F(14)	F(13)	F(12)	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	**377**	**233**	**144**	**89**	**55**	**34**	**21**	**13**	**8**	**5**	**3**	**2**	**1**	**1**
4											1	0	1	0
20								1	0	1	0	1	0	0
32							1	0	1	0	1	0	0	0
401	1	0	0	0	0	0	1	0	0	0	1	0	0	0
123				1	0	1	0	0	0	0	0	0	0	0
246		1	0	0	0	0	0	1	0	0	0	0	0	0
351		1	0	1	0	0	1	0	1	0	0	0	0	0
527	1	0	1	0	0	0	0	0	0	1	0	0	1	0
95				1	0	0	0	0	0	1	0	0	1	0
89				1	0	0	0	0	0	0	0	0	0	0

Tabela 29 – Representação de alguns Códigos de Fibonacci na forma Mínima.

6.2.3. Dispositivo Lógico FM ⇒ ÑFM

O Dispositivo Lógico recebe como *input* o Texto Cifrado Intermédio na Codificação de Fibonacci (LF) resultado do processo de conversão que apresenta blocos variáveis de 0 á 94 bits, processa-os e produz o Texto Comprimido (Z) de blocos de tamanho variável de 0 á 93 bits.

O Processamento do dispositivo lógico consiste em:

1. Transformar o código de Fibonacci da Forma Mínima para a Forma Não Mínima, usando para tal a operação Tipo-R dos Números de Fibonacci. Aplicando-a continuamente, até não poder mais, para o caso dos números da Tabela 29 obteríamos o resultado na Tabela 30;
2. Dado que os códigos de Fibonacci de parâmetro 1 possuem dois 1 (uns), aplicar uma operação de troca entre os últimos dois bits dos números que terminam com os bits "10" obtendo, assim, "01" de modo que todos números terminem com 1. Por exemplo, se o número for

$$4 = (1010)_F \qquad (43)$$

Como o número (43), não termina com o bit 1, então vamos aplicar a troca, obteremos:

$$4 = (1010)_F = (1001)_F \qquad (44)$$

	F(14)	F(13)	F(12)	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	**377**	**233**	**144**	**89**	**55**	**34**	**21**	**13**	**8**	**5**	**3**	**2**	**1**	**1**
4											1	0	1	0
20									1	1	1	1	1	1
32								1	1	1	1	1	1	0
401		1	0	1	0	1	1	1	0	1	1	1	1	0
123					1	1	1	0	1	0	1	0	1	1
246			1	0	1	0	1	1	1	0	1	0	1	1
351			1	1	1	1	0	1	1	1	0	1	1	0
527		1	1	1	0	1	0	1	1	0	1	1	1	0
95					1	0	1	0	1	1	1	1	1	0
89					1	0	1	0	1	0	1	0	1	1

Tabela 30 – Representação de alguns Códigos de Fibonacci na forma Não Mínima.

3. Aplicar, novamente, a operação Tipo-R. Deste modo, obteríamos o mostrado pela Tabela 31.

	F(14)	F(13)	F(12)	F(11)	F(10)	F(9)	F(8)	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
N.D.	**377**	**233**	**144**	**89**	**55**	**34**	**21**	**13**	**8**	**5**	**3**	**2**	**1**	**1**
4												1	1	1
20									1	1	1	1	1	1
32								1	1	1	1	1	0	1
401		1	0	1	0	1	1	1	0	1	1	1	0	1
123					1	1	1	0	1	0	1	0	1	1
246			1	0	1	0	1	1	1	0	1	0	1	1
351			1	1	1	1	0	1	1	1	0	1	0	1
527		1	1	1	0	1	0	1	1	0	1	1	0	1
95					1	0	1	0	1	1	1	1	0	1
89					1	0	1	0	1	0	1	0	1	1

Tabela 31 – Representação de alguns Números de Fibonacci na forma Não Mínima.

Os passos 2 e 3 permitem comprimir a palavra e definir o primeiro e último bit como "1" (um).

O Texto Comprimido (Z) é o principal texto cifrado do IDEA-F, dado que se pode optar pelos outros intermediários.

Para o caso em o emissor opta por enviar esta cifra ele terá as seguintes vantagens:

- Por apresentar um tamanho variável, *minimiza o uso do meio de transmissão* e ocupa-o apenas com bits significativos, o que diminui, também, a *probabilidade de ocorrência de erros* e *aumenta a velocidade de transmissão*. De salientar que, pelo tratamento que se dá ao bloco neste processo ele se apresenta mais comprimido do que LF;
- Como se pode ver pela Tabela 31, os Números de Fibonacci na sua forma Não Mínima não possuem dois "0" (zeros) consecutivos, isto é, entre dois "0" (zeros) existe sempre um ou mais "1" (uns). Com base neste padrão podem-se *detectar erros de transmissão, aumentando assim a veracidade da informação*.

6.2.4. Dispositivo de Comando

Para um bloco dum dado texto em claro o IDEA-F pode produzir três tipos de cifra distintos, nomeadamente:

- Texto Cifrado Intermédio (L);
- Texto Cifrado Intermédio na Codificação de Fibonacci (LF);
- Texto Comprimido (Z).

Deste modo, podemos definir dois modos de utilização do IDEA-F o *homogéneo* e o *heterogéneo*. No homogéneo o emissor opta por encriptar todos os blocos do texto usando o mesmo tipo de cifra, enquanto que no heterogéneo são usados todos tipos de cifras para encriptar os blocos dum mesmo texto em claro. De referir que, o tipo de cifra a aplicar num dado bloco é escolhida aleatoriamente.

O Dispositivo de Comando possui mecanismos que *indicam o tipo de texto cifrado* que o emissor optou e que *controlam o início e fim de cada bloco* visto que algumas cifras possuem blocos de tamanho variáveis.

Na Tabela 32 são descritos os tipos de cifras produzidas pelo IDEA-F.

Número	Nome	Características	Exemplo
1	Texto Cifrado Intermédio (L)	• Possui um tamanho fixo de 64 bits.	0000000001101010 0010100000001010 1010110010101001 0010001111000000
2	Texto Cifrado Intermédio na Codificação de Fibonacci (LF)	• Possui um tamanho variável de 0 à 94 bits; • Não possui dois "1" (uns) consecutivos; • O bloco começa com um bit de valor lógico "1" (um) e termina com um bit de valor lógico "0" (zero).	101000100
3	Texto Comprimido (Z)	• Possui um tamanho variável de 0 à 93 bits; • Não possui dois "0" (zeros) consecutivos; • O bloco começa com um bit de valor lógico "1" (um) e termina com um bit de valor lógico "1" (um).	101111101

Tabela 32 – Tipos de Cifras do IDEA-F.

Como se disse acima uma das funções do Dispositivo de Comando é o de controlar o início e fim de cada bloco, para tal vamos analisar as combinações possíveis que se encontram num texto cifrado do IDEA-F. Tomando em consideração que o IDEA-F pode produzir 3 (três) tipos de cifras distintas e que todas elas podem ser aplicadas a um mesmo texto em claro, podemos calcular o número de combinações possíveis dos três tipos de cifra, usando para tal a análise combinatória. Calculando o arranjo com repetição de 3 elementos agrupados dois a dois, teríamos:

$$A_n^K = n^K \qquad (45)$$

Aplicando a formula (45), teríamos:

$$A_3^2 = 3^2 = 9 \qquad (46)$$

De acordo com o resultado obtido na fórmula (46) podemos concluir que podem surgir 9 (nove) combinações possíveis.

Para cada combinação devem ser definidos bits específicos para destacar a separação das cifras. A Tabela 33 mostra esses mesmos bits (os bits vermelhos representam os de separação).

Combinação de 2 (duas) Cifras		Bits de Separação	Exemplo
Primeira	Segunda		
1	2	10	00000000011010100010100000010101010100101010010001000111100000101010001000
1	3	11	00000000011010100010100000010101010100101010010001000111100000011101111101
1	1	00	00000000011010100010100000010101010100101010010001000111100000000000000000011010100010100000001010101011001010100100010001111000000
2	1	1100	10100010011000000000001101010001010000001010101011001010100100100011110000000
2	2	1111	101000100111110100010
2	3	1110	10100010011101011111101
3	2	0001	10111110100011010001000
3	1	0011	10111110100110000000001101010001010000001010101011001010100100100011110000000
3	3	0000	10111110100001011111101

Tabela 33 – Bits de separação das combinações dos tipos de Cifra do IDEA-F.

Além dos bits de separação, o IDEA-F prevê, também, o uso de bits iniciais que são usados para o primeiro bloco (ver Tabela 34, os bits azuis representam os iniciais).

Tipo de Cifra	Bits Iniciais	Exemplo
1	10	1000000000011010100010100000001010101011001010100100010001111000000
2	00	00101000100
3	11	11101111101

Tabela 34 – Bits iniciais dos tipos de Cifra do IDEA-F.

6.2.5. Porto de Saída

O Porto de Saída tem a função de concatenar o bloco do texto cifrado resultante do IDEA-F, os bits de separação e os iniciais, formando assim o Texto Cifrado (Y) de tamanho variável com tamanho 2 à 98 bits.

CAPÍTULO VII

CONCLUSÃO E RECOMENDAÇÕES

7. CONCLUSÃO E RECOMENDAÇÕES

Como se pode concluir, a invenção do computador fez com que o Mundo altera-se a sua forma de trabalhar, pois os seus benefícios, como o rápido processamento, fizeram com que o mesmo fosse aplicado tanto para as actividades económicas como para o uso doméstico. Esta rápida expansão do computador fez com que houve necessidade de os interligar, como forma de obter uma ligação a baixo custo, e com esta necessidade surgiram as redes de computadores.

O desenvolvimento das redes de computadores culminou com o surgimento da Internet, que veio dinamizar, ainda mais, a forma como as Organizações actuam, visto que deu origem a chamada *Aldeia Global*, onde existem tantas possibilidades de negócio como no Mundo Real. Esta nova forma de fazer negócio fez com que as Organizações expandissem facilmente as suas actividades e, consequentemente, gerar mais receitas; de maneira que, toda Organização quer se ver representada neste novo Mundo, o que implicou mudanças tanto na tomada de decisão, como na publicitação dos seus Produtos, e principalmente na forma de comunicação. Estas mudanças foram, grandemente, motivadas pelo desenvolvimento de ferramentas que permitem as pessoas se expressar mais facilmente *online*.

Além dos benefícios que este novo mundo trouxe, a utilização da *Internet* ou uma rede de computadores para a comunicação faz com que a informação fique vulnerável, tanto durante a transmissão, pois a mesma circula por vários locais através do meio de transmissão, como a para a informação armazenada a um computador, pois um computador que pertence a uma rede pode ser acedido remotamente. Estes factores permitiram a criação de uma nova forma de crime, como extorsões, falcatruas, terrorismo, espionagem e violação de privacidade, em que o principal objectivo do crime é a *informação*. Deste modo, devem-se definir mecanismos tanto para combater como para punir os responsáveis, o que é uma tarefa muito complicada visto que no mundo Virtual é difícil encontrar os responsáveis por tais actos, pois os mesmos perpetuam estes actos através dum computador (que pode pertencer a um Internet-Café) que pode se encontrar em qualquer parte do Globo, o que dificulta a sua localização no Mundo Real, daí que, é quase impossível, caracteriza-los fisicamente ou conhecer a sua identidade.

Este exemplo, de como a Internet pode representar um perigo aplica-se também as Intranets, pois o acesso ilegal pode ser perpetrado por um dos funcionários da Organização, que por trabalhar na mesma, tem acesso a rede interna. Por outro lado, um intruso pode se introduzir nas instalações onde opera a Organização e ter acesso a rede e até aos próprios computadores. Deste modo, os mecanismos de segurança devem contemplar tanto as *instalações* como a *transmissão* em si. O que nos faz concluir que as redes seguras são as que se desconhecem a sua localização física e não são públicas, ou por outra, não são penetradas por qualquer pessoa, o que para a maior parte das Organizações não é viável [19].

Ao longo deste trabalho foram analisados aspectos a ter em conta para garantirmos uma segura transmissão de informação, o que comporta a escolha dum meio de transmissão adequado, detecção de possíveis vulnerabilidades do Sistema de Informação, identificação de eventuais intrusos tanto internos como externos a Organização e que métodos usar para proteger a informação, levando em consideração os métodos de violação.

Com a expansão dos Sistemas de Informação em áreas chave como a Saúde, a Educação, o Sector Público e Privado e a integração destes Sistemas, as TIC´s passaram a determinar o desenvolvimento económico e social dum País, e impulsionaram bastante a economia Mundial chegando a ser consideradas como um Indicador de Crescimento Económico. Em países em desenvolvimento, como é o caso de Moçambique, em que as TIC´s são uma novidade, a questão da segurança da informação durante a sua transmissão tem sido esquecida, pois a maior parte dos gestores dessas mesmas instituições não tem consciência da facilidade com que um intruso pode ter acesso a informação durante a sua transmissão. A má utilização ou deficiente aplicação das TIC's, pode provocar muitos danos que podem ocorrer desde perda, roubo e destruição de informação, o que têm posto em causa os benefícios deste novo modo de operar, e aumenta a resistência em adoptar as TIC´s, principalmente em Moçambique em que a maior parte da População não tem acesso a um computador e teme pelos seus postos de trabalho, visto que não domina o uso do computador.

Em termos de analogia, pode-se comparar um Sistema de Informação ao funcionamento dum Banco, cujos intervenientes são a *Informação* e o *Dinheiro*, respectivamente. Para ambos os casos, devem ser implementadas medidas de segurança tanto nas Instalações, em que os mesmos operam, como para o Transporte.

Para o primeiro caso, são usados mecanismos como o uso de guardas, o controlo de acessos, a colocação de câmaras de vigilância, o armazenamento de objectos em cofres, etc.; para o segundo caso, já não podem ser usados os mesmos mecanismos pois o tipo de objecto a ser transportado define as vias a serem usadas, deste modo, para o dinheiro (representada no estado físico) são usados guardas, carros blindado, etc.; já para informação (representada no estado electrónica) é usada, geralmente, a *criptografia* por ser a forma mais barata e que exige pouca intervenção Humana. Neste trabalho foram descritos os algoritmos criptográficos simétricos mais conhecidos, o objectivo dessa descrição é fornecer uma base de comparação entre eles analisando assim as suas fraquezas e qualidades.

A grande dificuldade que a maior parte dos Gestores enfrenta é a de avaliar a *Informação*, ou melhor, saber quanto ela vale e quanto se deve gastar para protege-la, pois é um bem abstracto e intangível estando esse mesmo valor associado a um contexto, o que já não é o caso do *Dinheiro* em que o seu valor é bastante evidente. Esta dificuldade é mais acentuada em países como Moçambique, em que a Políticas de Informática[2] é recente e os crimes informáticos não estão bem definidos na Legislação, pelo que, não são reportados e nem investigados como tal. Por estes motivos, é difícil para qualquer Gestor avaliar o Risco a que a Informação esta sujeito, pois não sabe o que combate, nem quem combate e nem que armas usar para combater, por outro lado, este esta consciente de que a perda de dados ou registos, resultante duma catástrofe natural ou uma acção humana propositada, pode levar uma Organização a encerrar a sua actividade.

Como se pôde ver ao longo deste trabalho, o sucesso dum algoritmo criptográfico depende da sua Força Criptográfica que comporta, principalmente, o tamanho do bloco, o tamanho da chave a confusão e a Difusão da velocidade de transmissão do texto cifrado resultado desse mesmo algoritmo. Com o aumento do nível de exigência dos SI, factores como o tempo de transmissão de uma dada mensagem, que comporta o tempo de "mascarar" e "desmascarar" a informação e o tempo de envio da mesma, começam a sobrepor os mecanismos de segurança, pois as Organizações sabem que um atraso no funcionamento do Sistema, provocado em grande parte pelas medidas de segurança, pode resultar num péssimo desempenho do mesmo. Este aspecto criou um paradoxo no campo na Criptografia, pois enquanto que por um lado algoritmos complexos que produzem textos com blocos de tamanho considerável como 64 bits e

[2] A Política de Informática, em Moçambique, foi aprovada em de 12 de Dezembro de 2000

usam chaves igualmente compridas, significa maior segurança da informação, por outro lado aumentam o tempo de envio da informação, condicionando assim o sucesso das operações que dependem dessa mesma informação, sem contar que ocupam maior largura de banda da infra-estrutura de comunicação, aumentando assim os custos da comunicação e dificultando o acesso aos serviços por parte de outros usuários da mesma.

Com os avanços científicos e tecnológicos que se tem verificado nos últimos tempos, e que têm colmatado com a proliferação das aplicações Multimédia, cuja informação processada não é só a alfanumérica, que é representada por números e caracteres, mas sim um diversificado tipo de informação que incluem além da própria alfanumérica, áudio, vídeo, imagens, etc. Devido a natureza da informação Multimédia, ela é mais volumosa, o que faz com que o seu processamento consuma mais os recursos computacionais e a sua transmissão ocupe uma maior largura de banda passante. Deste modo, a velocidade de processamento e transmissão deste tipo de informação condicionam o bom funcionamento dos Sistemas, por consequência os algoritmos criptográficos tem de ser redesenhados por forma a acompanharem a estas novas exigências do mercado.

Ao longo deste trabalho, apresentou-se uma nova versão do IDEA, o IDEA-F, que faz uso dos Códigos de Fibonacci para, além de garantir a segurança da informação transmitida, reduzir o tamanho dos blocos do texto, possibilitando uma transmissão menos morosa e à menos custos, visto que paga-se por cada *bit* transmitido, detectar e, em certos casos, corrigir erros que podem ocorrer durante a transmissão.

Nos últimos tempos têm-se notado que a maior parte dos gestores e utilizadores das TIC's já se consciencializaram para a necessidade de se defenderem de softwares maliciosos, como é o caso do vírus, e de acessos ilegais, pois de alguma forma já foram prejudicados pelos mesmos. O mesmo já não acontece com a transmissão da informação, em que estes nem sabem se já foram atacados ou se já foram atribuíram as culpas, pela perda de informação, a um outro factor. Isto acontece principalmente porque este nível de segurança depende da definição duma política interna por parte da Organização, daí que, aconselha-se os Gestores das Empresas, a olharem para a Segurança dos seus SI's, não como um factor isolado ou de suporte da sua actividade mas sim um factor decisivo para o seu funcionamento. Além disso, esta política deve abranger tanto o nível físico como o lógico da Organização e não deve lesar o funcionamento da Organização e muito menos prejudicar o Cliente, deste modo os

mecanismos a serem adoptados devem levar em consideração tanto os aspectos organizacionais como financeiros da Instituição.

ANEXOS

- Criptoanálise Diferencial e Linear
- Função Bent
- Cifração de Bloco
- Estrutura da Cifra de Fiestel

ANEXO A - CRIPTOANÁLISE DIFERENCIAL E LINEAR

A maior preocupação com o DES era o ataque de Força-Bruta devido a sua chave de 56 bits. Com o desenvolvimento das novas cifras de bloco com cumprimentos de chave superiores apareceram dois métodos de criptoanálise o Diferencial e o Linear (ver ANEXO A).

A.1. Criptoanálise Diferencial

O ataque de criptoanálise diferencial é complexo. Vamos simula-lo no DES, começemos por mudar a notação do DES. Considerando que o bloco de texto em claro original X é constituído por duas metades X_0 e X_1. Cada estágio do DES mapeia a parte direita da entrada para dentro da parte esquerda da saída e define a parte direita da saída para ser uma função da parte direita da entrada e a subchave do estágio. Deste modo, em cada estágio, apenas um novo bloco de 32 bits é criado. Se chamarmos a cada bloco novo m_i ($2 \leq i \leq 17$), então as metades da mensagem intermédia são relatadas como [16]:

$$X_{i+1} = X_{i-1} \oplus f(X_i, C_i); \quad i = 1,2, \ldots,16 \qquad (47)$$

Na criptoanálise diferencial, começamos com duas mensagens, X e X', com uma diferença XOR conhecida $\Delta X = X \oplus X'$, e consideramos a diferença entre as metades da mensagem intermediárias $\Delta X = X_i \oplus X'_i$. Então teremos:

$$\Delta X_{i+1} = X_{i+1} \oplus X'_{i+1} = [X_{i-1} \oplus f(X_i, C_i)] \oplus [X'_{i+1} \oplus f(X'_i, C_i)] = \Delta X_{i-1} \oplus [f(X_i, C_i) \oplus f(X'_i, C_i)] \qquad (48)$$

Suponha que muitos pares de entradas de f com a mesma diferença produzem a mesma diferença na saída se a mesma chave for usada. Para ser mais preciso suponhamos que X causa Y com a probabilidade p, se para uma fracção p de pares onde a entrada XOR é X, e a saída XOR é Y. Nós queremos supor que há uma quantidade de valores de X que tem uma grande probabilidade de criar uma diferença na saída em particular. Contudo, se nós conhecemos ΔX_{i-1} e ΔX_i com uma grande probabilidade, deste modo saberemos ΔX_{i+1} com grande probabilidade. Contudo, se um número com estas diferenças é determinado, é lógico determinar a subchave usada na função f.

A estratégia geral da criptoanálise diferencial é baseada nas considerações dum único estágio. O procedimento é de iniciar com duas mensagens texto em claro m e m' com uma dada diferença após cada estágio para produzir uma probabilidade da diferença

do texto cifrado. Na verdade, existem duas diferenças prováveis para as duas metades de 32 bits ($\Delta X_{17}|| \Delta X_{16}$). A seguir submete-se m e m' para encriptação para determinar a diferença actual sobre a chave desconhecida e comparar o resultado com a diferença provável. Se existir uma igualdade:

$$E_C(X) \oplus E_C(X') = (\Delta X_{17}|| \Delta X_{16}) \qquad (49)$$

Então suspeitamos que todos padrões possíveis de todos estágios intermediários estão correctos. Com esta suposição, podemos fazer algumas deduções sobre os bits da chave. Este procedimento deve ser repetido muitas vezes para determinar todos bits da chave.

A.2. Criptoanálise Linear

Um método mais recente é o da Criptoanálise Linear, vamos descreve-la aplicando-a ao DES; ela baseia-se em procurar uma aproximação Linear para descrever a transformação efectuada. Este método pode encontrar uma chave do DES dando 2^{47} textos em claro conhecidos, comparando com 2^{47} texto em claro escolhidos para a criptoanálise diferencial. Apesar disto ser um melhoramento pequeno, pois é mais fácil produzir texto em claro conhecido que o texto em claro escolhido, ainda deixa a criptoanálise linear impraticável no DES.

A criptoanálise linear actua da seguinte forma. Para uma cifra com blocos de texto em claro e texto cifrado de n-bits e uma chave de m-bits, seja o bloco de texto em claro chamado de X[1], X[2], X[3], ..., X[n], o bloco de texto cifrado Y[1], Y[2], Y[3], ..., y[n] e a chave C[1], C[2], C[3], ..., C[n] e define-se:

$$A[I, j, \ldots, k] = A[i] \oplus A[j] \oplus \ldots \oplus A[k] \qquad (50)$$

O objectivo da Criptoanálise Linear é de encontrar uma equação linear eficaz da forma:

$$X[\alpha_1, \alpha_2, \ldots, \alpha_a] \oplus Y[\beta_1, \beta_2, \ldots, \beta_b] = C[\gamma_1, \gamma_2, \ldots, \gamma_c] \qquad (51)$$

Onde:

$1 \leq a, b \leq n$, $1 \leq c \leq m$ e α, β, γ são termos que representarão locais de bits únicos fixos que tem a probabilidade de $p \neq 0{,}5$. Quanto mais distante p for de 0,5, mais eficaz será a equação. Uma vez proposta uma relação, o procedimento é calcular os resultados da parte esquerda da equação precedente para um grande número de pares texto em claro-texto cifrado. Se o resultado for "0" a maior parte das vezes, assume-se $C[\gamma_1, \gamma_2, \ldots, \gamma_c] = 0$. Se for 1 a maior parte do tempo, assume-se que $C[\gamma_1, \gamma_2, \ldots, \gamma_c] = 1$. Isto dá-nos uma

equação linear dos bits da chave. Tenta-se arranjar mais relações possíveis para que se possa descobrir os bits das chaves. Porque estamos usando equações lineares, o problema pode ser tratado por um estágio do texto cifrado de cada vez, com resultados combinados [16].

ANEXO B - FUNÇÃO BENT

Considerando a função f(x) que mapeia um inteiro de n bits em um simples bit, isto é expresso como f: $\{0,1\}^n \rightarrow \{0,1\}$; o argumento X pode ser representado pelo algarismo de n bits (X_{n-1}, ..., X_2, X_1). Por exemplo, para n=3, uma função poderia ser enumerada como {g(000) = 0; g(001) = 1; g(010) = 1; g(011) = 0; g(100) = 1; g(101) = 0; g(110) = 1; g(111) = 0}. Como uma função pode ser representada por um vector-coluna em como a k-ésima entrada na coluna corresponde ao g(k). Por exemplo,

$$g = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

A transformação Walsh da função f: $\{0,1\}^n \rightarrow \{0,1\}$ é definida por:

$$W_f(w) = \sum_{x=0}^{2^n-1} (-1)^{f(x)+w.x} \qquad (52)$$

Onde:

$$w.x = w_{n-1}x_{n-1} \oplus \ldots \oplus w_0x_0$$

E onde w é um inteiro $0 \leq w \leq 2^{n-1}$. Note que cada termo do somatório toma um valor +1 ou –1. E para um valor dado w, $W_f(w)$ toma um inteiro de $-2^n \leq W_f(w) \leq 2^n$. Pode-se mostrar que f(x) pode ser expressado na forma inversa de Walsh [53]:

$$f(x) = \frac{1}{2^n} \sum_{w=0}^{2^n-1} W_f(w)(-1)^{w.x} \qquad (53)$$

E f(x) pode ser expresso como uma soma de funções de w.

O conjunto de funções Bent, com n igual, é o conjunto de funções f: $\{0,1\}^n \rightarrow \{0,1\}$ que:

$$W_f(w) = \pm 2^{\frac{n}{2}}, \quad \forall \quad w \in \{0,1\}^n \qquad (54)$$

Uma função Bent é um vector binário onde a transformação Walsh tem uma certa importância.

A relação entre as funções Bent e as Caixas-S é que uma Caixa-S mapeia uma entrada de n bits para uma saída de m bits. Como se mencionou antes, uma Caixa-$S_{n \times m}$ consiste em 2^n linhas de m bits cada. Os n bits de entrada seleccionam uma das linhas da Caixa-S e m bits dessa linha é a saída. Pode-se ver as Caixas-S como um conjunto de m vectores colunares $[C_{m-1}(x) \ldots C_1(x)\ C_0(x)]$, onde x é a entrada de n bits e $C_i(x)$ é a i-ésima coluna da Caixa-S. E cada coluna da Caixa-S pode ser vista como uma função C_i: $\{0,1\}^n \rightarrow \{0,1\}$. Isto nos permite construir e usar as Caixas-S onde as colunas são funções Bent.

As funções Bent possuem uma enorme não linearidade e um perfeito SAC.

ANEXO C - CIFRAÇÃO DE BLOCO

C.1. Princípios de concepção de Cifras de Bloco

Apesar dos grandes avanços que ocorreram no desenvolvimento de cifras de bloco, os princípios nunca mudaram. Vamos agora analisar os três aspectos críticos na concepção de cifras de bloco, nomeadamente, o número de estágios, o desenho da função F e a geração das chaves.

C.1.1. Número de estágios

Quanto maior o número de estágios S, mais difícil será a criptoanálise, mesmo para o caso de uma função F fraca. No geral, o critério deveria ser de maneira que o número de estágios é escolhido de forma que o esforço da criptoanálise seja maior que o esforço dum ataque de procura de chave, Força-Bruta [15].

Este critério é atractivo pois torna simples avaliar a força do algoritmo e compara-lo aos diferentes algoritmos.

C.1.2. Desenho da função F

O elemento principal duma cifra de Fiestel (ver ANEXO D) é a função F, e esta função usa as Caixas-S.

C.1.2.1. Critério de desenho de F

A função F providencia a confusão numa Cifra de Fiestel (ver ANEXO D). Uma das principais características da função F é a não *linearidade*. Quanto menos linear for F mais difícil será qualquer ataque criptográfico. Isto é, quanto mais difícil for aproximar a função F a um conjunto de equações lineares, mais F não será linear. Pode-se considerar muitos outros aspectos na concepção da função F. Pois deseja-se que o algoritmo tenha um bom efeito avalanche. Uma versão mais forte do efeito avalanche é o *Strict Avalanche Criterion* (SAC) que diz que qualquer bit j duma Caixa-S deveria mudar com probabilidade ½ quando qualquer bit de entrada i é invertido para todos i, j. Apesar de SAC ser aplicado a Caixas-S poderíamos também aplica-lo a função F.

Outro critério proposto é o *Bit Independence Criterion* (BIC) que diz que os bits de saída j e k deveriam mudar independentemente quando qualquer bit simples de entrada é invertido para todos i, j e k. O SAC e BIC são duas funções de confusão fortes.

C.1.2.2. Desenho das Caixas-S

No geral, deseja-se que qualquer mudança no vector de entrada duma Caixa-S resulte em mudanças aparentemente aleatórias na saída. A relação não deve ser linear e difícil de aproximar a funções lineares.

Uma característica óbvia duma Caixa-S é o seu tamanho. Uma Caixa-S_{nxm} tem n bits de entrada e m bits de saída. DES tem 6 X 4 Caixas-S. Blowfish e o CAS têm 8 X 32 Caixas-S.

As Caixas-S mais largas são mais resistentes a criptoanálise Linear e Diferencial. Por outro lado, quanto maior o n maior será a tabela. Deste modo, por razões práticas aconselha-se o que o n seja 8 ou 10.

Outra consideração é que quanto maior for a Caixa-S mais difícil é concebe-la. Uma Caixa-$S_{n \times m}$ consiste em 2^n linhas de m bits cada. Os n bits de entrada seleccionam uma das linhas da Caixa-S e m bits dessa linha são a saída. Por exemplo, numa Caixa-S_{8x32}, se a entrada é 00001001, a saída consistirá em 8 bits da linha 9 (a primeira linha é denominada 0) [16].

Mister e Adams estipularam que as Caixas-S deveriam satisfazer o SAC e o BIC. E também sugeriram que todas combinações lineares das colunas das Caixas-S devem ser Bent (Ver ANEXO B).

As funções Bent são uma classe especial de funções booleanas que são altamente não lineares de acordo com certos critérios matemáticos.

Um outro critério relacionado com as Caixas-S é a *Avalanche Garantida* (AG) que diz, uma Caixa-S satisfaz AG na ordem γ se para uma mudança dum bit na entrada pelo menos γ bits da saída mudam. Para Caixas-S grandes, como 8 x 32, a questão é escolher o melhor método de seleccionar as entradas da Caixa-S de modo a cumprir os critérios discutidos.

Nyberg, que escreveu bastante sobre a concepção das Caixas-S, sugeriu [16]:

- **Aleatoriedade:** usa-se um gerador de números pseudo-aleatórios ou uma tabela de números aleatórios para gerar as entradas da Caixa-S. Isto pode levar a resultados indesejados em caixas pequenas mas aceitáveis em caixas grandes;
- **Testar a aleatoriedade:** escolher aleatoriamente as entradas da Caixa-S e depois testa-las de modo que as indesejáveis não sejam usadas;

- **Desenvolvido pelo Homem:** é a aproximação mais ou menos manual que usa apenas a matemática. Esta aproximação é difícil de efectuar em Caixas-S grandes;
- **Elaborado matematicamente:** gerar Caixas-S de acordo com princípios matemáticos. Usando a construção matemática, as Caixas-S podem ser produzidas oferecendo uma segurança comprovada contra a criptoanálise Linear e Diferencial e com boa difusão. Esta é a técnica do CAST.

Uma variação da primeira técnica é de usar Caixas-S que são aleatórias e dependentes da chave. Este é o caso usado no Blowfish. Uma grande vantagem das Caixas-S dependente da chave é que elas não são fixas, e é impossível analisar as Caixas-S para analisar fraquezas.

C.2. Características das Cifras de Bloco

Virtualmente, todas cifras de bloco simétrico são similares em muitos aspectos ao DES e a Estrutura Básica de Cifra de Bloco de Fiestel (ver ANEXO D). Com a evolução da criptoanálise e com a necessidade dum Software de encriptação rápidos foram feitos avanços. Nesta secção serão descritas algumas características da chave encontradas em alguns algoritmos mas não no DES:

- **Tamanho da chave variável:** se um algoritmo de encriptação é concebido para ser extremamente resistente a criptoanálise, então a sua força é determinada pelo tamanho da chave, quanto mais longa for a chave, mais longo será o ataque de procura da chave, Força-Bruta. Blowfish, RC5, CAST-128 e RC2 possuem esta característica;
- **Operadores Misturados:** o uso de mais dum operador aritmético e/ou booleano complica a criptoanálise, especialmente se estes operadores não satisfazem as regras associativas e distributivas. Esta característica providencia não linearidade como alternativa às caixas-S. Todos algoritmos aqui retractados usam Operadores Misturados, com a excepção do DES Triplo;
- **Rotação dependente dos dados:** outra alternativa às caixas-S é usar rotações dependentes dos dados. Com suficiente número de estágios, isto pode provocar excelente *confusão* e *difusão*. Além disso, as rotações são dependentes dos blocos de dados movendo pelos estágios, em vez das subchaves. Isto torna a recuperação das subchaves mais difícil. O RC5 usa rotações dependentes de dados;

- **Rotação dependente da chave:** uma rotação pode depender da chave do que dos dados, isto acontece no CAST-128;
- **Caixa-S dependente da chave:** em vez de conceber caixas-S fixas com elementos criptográficos desejáveis, como acontece em DES e CAST-128, o conteúdo das caixas-S pode ser dependente da chave. Uma chave diferente cria uma caixa-S diferente. Esta característica, especialmente em caixas-S largas (ex: 8 x 32) significa resultados de alta não linearidade e dificulta a criptoanálise. Blowfish usa caixas-S dependente da chave;
- **Algoritmo de definição do tamanho da chave:** esta é uma táctica ingénua usada no Blowfish. A geração das subchaves leva muito mais que uma simples encriptação e decriptação. O resultado é que o esforço dum ataque Força-Bruta é altamente difícil;
- **F variável:** o uso duma função F que varia de estágio para estágio pode complicar o problema da criptoanálise. CAST-128 usa uma função F variável.
- **Tamanho do bloco de texto em claro/texto cifrado variável:** um bloco de maior tamanho oferece maior força criptográfica. Também, um bloco de tamanho variável pode providenciar uma medida de conveniência, permitindo o algoritmo ser anexado a uma aplicação. RC5 adopta esta estratégica;
- **Número variável de estágios:** outra característica importante é que um aumento do número de estágios incrementa a força criptográfica. Claro que, um incremento no número de estágios aumenta o tempo da encriptação e decriptação. Permitindo um número variável de estágios permite ao usuário fazer uma troca entre segurança e rapidez de execução. RC5 providencia um número variável de estágios;
- **Operações nas duas metades dos dados em cada estágio:** na Clássica Cifra de Fiestel (ver ANEXO D), apenas uma metade dos dados é alterada em cada estágio. Se uma simples operação foi efectuada na metade em que caso contrário não é alterada, a segurança poderia ser aumentada com um aumento mínimo do tempo de execução. IDEA, Blowfish e RC5 operam nas duas metades dos dados em cada estágio.

O trabalho desenvolvido nesta área tenta refinar a Cifra de Fiestel (ver ANEXO D) e DES em vez de desenhar uma nova estrutura. Pois a estrutura de Fiestel não tem demonstrado fraquezas.

C.3. Cifração de Fluxo Vs. Cifração de Bloco

A Cifração de Fluxo é aquela que encripta um fluxo de dados digitais por bit ou byte por vez. Um dos exemplos de encriptação é a cifra de Vigenère de autochave e a cifra de Vernam. A Cifração de Bloco é aquela em que um bloco do texto em claro é tratado como um todo e é usado para produzir um bloco de texto cifrado de tamanho igual. Usualmente, usam-se blocos de 64 bits. Em geral, as cifras de bloco são mais aplicáveis que as cifras em fluxo. A maior parte das aplicações das redes que usam a Criptografia Convencional usam as cifras de bloco [16].

ANEXO D - ESTRUTURA DA CIFRA DE FIESTEL

A Figura 44 mostra a estrutura proposta por Fiestel. A entrada do algoritmo de encriptação é um bloco de texto em claro de 2w bits e a chave C. O bloco do texto em claro é dividido em duas metades E_0 e D_0. As duas metades dos dados passam por n estágios e depois é combinado para produzir o bloco de texto cifrado. Cada estágio I tem como entrada E_{i-1} e D_{i-1}, derivados do estágio anterior, assim como C_i derivada do C inicial. Em geral, C_i é diferente do C e dos outros C_i.

Todos estágios têm a mesma estrutura. Uma substituição é efectuada na metade à esquerda dos dados.

Isto é feito aplicando a função de estágio F na metade direita dos dados e depois usando o OU-Exclusivo da saída daquela função e da metade esquerda dos dados. A função de estágio possui a mesma estrutura geral para cada estágio mas é parametrizada pelo estágio da subchave C_i. Após a substituição efectua-se uma Permutação que consiste no intercâmbio de duas metades dos dados.

A realização da rede Fiestel depende da escolha dos seguintes parâmetros []:

- **Tamanho do bloco:** quanto maior tamanho dos blocos significa maior segurança mas reduz a velocidade da Encriptação/Decriptação. Um bloco de tamanho de 64 bits é razoável para os algoritmos de Cifra de Bloco (ver ANEXO C);
- **Tamanho da chave:** quanto maior a chave maior será a segurança mas irá decrementar a velocidade da Encriptação/Decriptação. Chaves de tamanho de 64 bits ou menos são largamente consideradas como inadequadas, o mais usado são os de 128 bits;
- **Número de estágios:** a essência da cifra de Fiestel é que um simples estágio oferece pouca segurança mas múltiplos estágios oferecem mais segurança. O ideal são 16 estágios;
- **Algoritmo de geração de chaves:** quanto mais complexo for o algoritmo mais difícil será a criptoanálise;
- **Função de estágio:** neste caso também, quanto mais complexa for a função maior resistência haverá para a criptoanálise;
- **Software de Encriptação/Decriptação rápido:** em vários casos a encriptação é incorporada nas aplicações ou utilidades, deste modo, a velocidade de execução do algoritmo deve ser tomado em consideração;

- **Facilidade de analisar:** apesar de querermos fazer o algoritmo mais difícil possível de quebrar, há um grande benefício em fazer o algoritmo fácil de analisar. Isto é, se o algoritmo pode ser facilmente explicado, é mais fácil analisar o algoritmo para vulnerabilidades criptoanalíticas e desenvolver um algoritmo mais seguro. DES, por exemplo, não tem uma funcionalidade fácil de analisar.

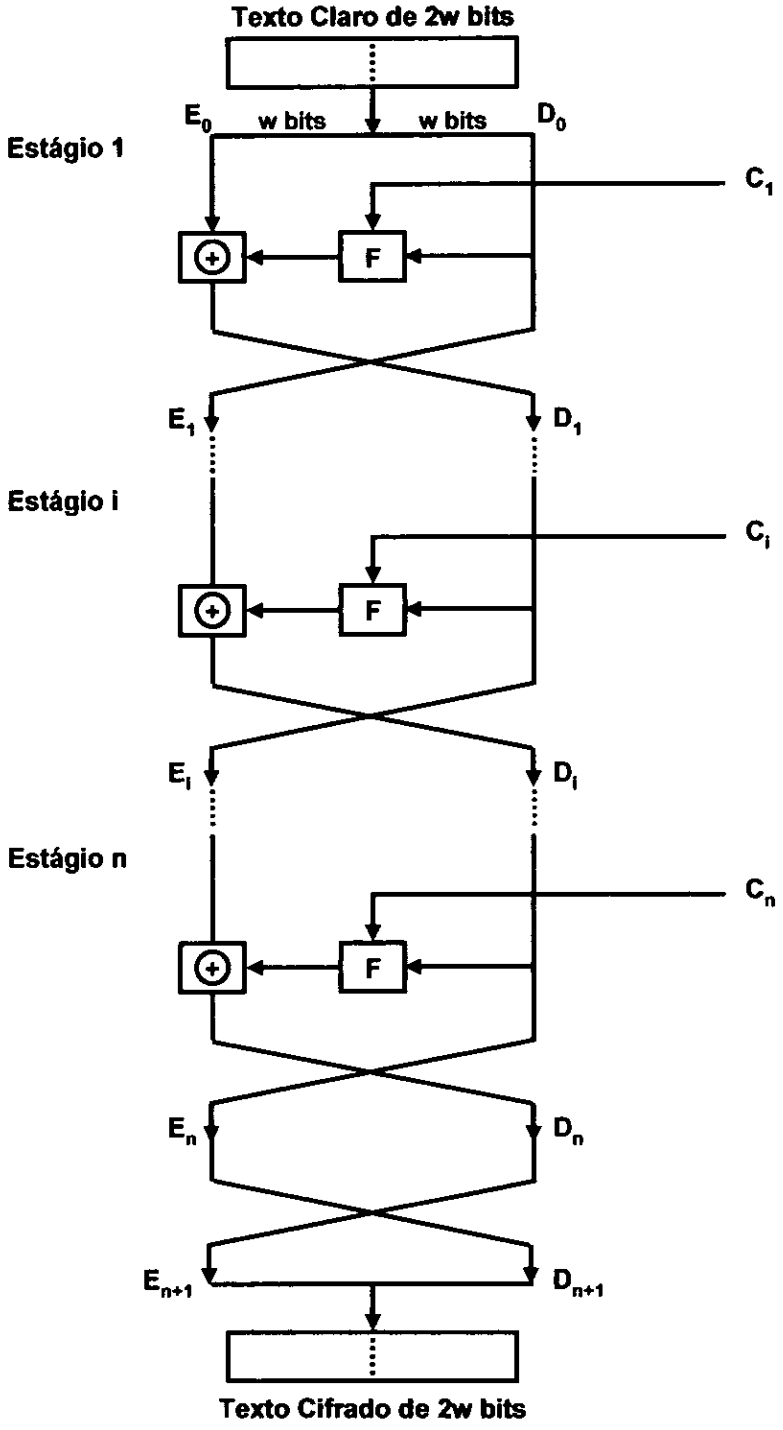


Figura 44 – Rede Clássica de Fiestel [16].

D.1. Algoritmo de Decriptação de Fiestel

É essencialmente idêntico ao processo de encriptação. A regra é a seguinte, usa-se o texto cifrado como entrada para o algoritmo, mas usa-se as subchaves C_i na ordem inversa. Isto é, usa-se o C_n no primeiro estágio, C_{n-1} no segundo, e assim por diante até C_1 que é usado no último estágio. Para vermos que este algoritmo produz o texto em claro, vejamos a Figura 45, que mostra o algoritmo de Encriptação e Decriptação com 16 estágios, EE_i e DE_i para os dados que fluem no algoritmo de encriptação e ED_i e DDi para os dados que fluem na Decriptação. O diagrama mostra que em qualquer estágio, os valores intermédios do processo de decriptação é igual ao valor correspondente ao processo de encriptação com as duas metades dos valores trocadas. Vendo por outro lado, seja , EE_i || DE_i (E_i concatenado com D_i) a saída do iésimo estágio do algoritmo, então a entrada correspondente para o (16-i)ésimo estágio de decriptação é , DD_i || ED_i.

Olhando para a Figura 45, após a última iteração do processo de encriptação, as duas metades da saída são trocadas, de modo que o texto cifrado é DE_{16} || EE_{16}. A saída daquele estágio é o texto cifrado. Agora use este texto cifrado como entrada no mesmo algoritmo. A entrada do primeiro estágio é DE_{16} || EE_{16} que é igual a troca de 32 bits da saída do 16º estágio do processo de encriptação.

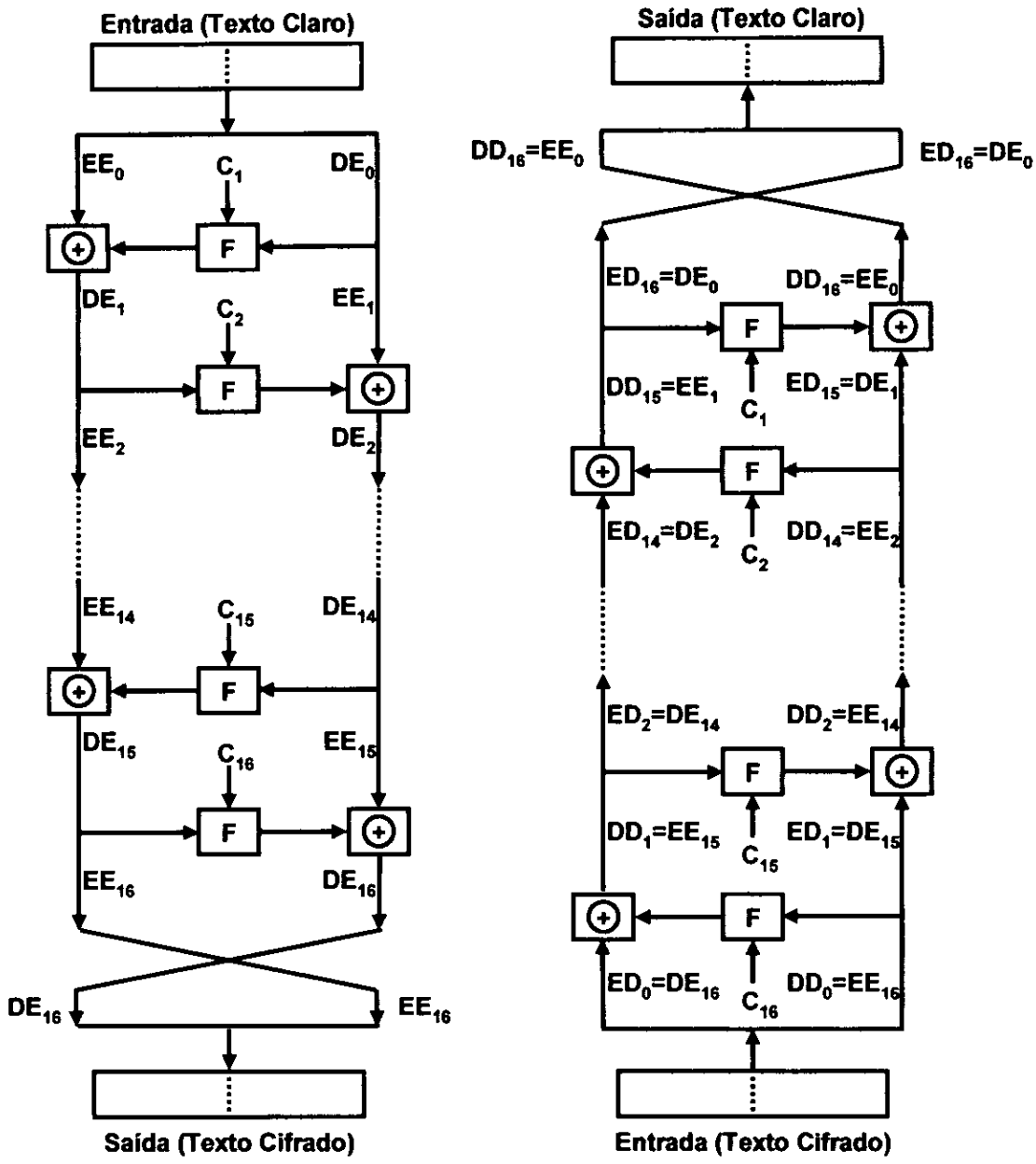


Figura 45 – Encriptação e Decriptação de Fiestel [16].

Agora vemos que a saída do primeiro estágio do processo de decriptação é igual a troca de 32 bits da entrada do 16º estágio do processo de encriptação. Primeiro consideramos o processo de encriptação, vemos que:

$$EE_{16} = DE_{15}$$

$$DE_{16} = EE_{15} \oplus F(DE_{15}, C_{16})$$

No lado da decriptação:

$$ED_1 = DD_0 = EE_{16} = DE_{15}$$

$$DD_1 = ED_0 \oplus F(DD_0, C_{16})$$

$$= DE_{16} \oplus F(DE_{15}, C_{16})$$

$$= [EE_{15} \oplus F(DE_{15}, C_{16})] \oplus F(DE_{15}, C_{16})$$

O OU-Exclusivo tem as seguintes propriedades:

$$[A \oplus B] \oplus C = A \oplus [B \oplus C]$$

$$D \oplus D = 0$$

$$E \oplus 0 = E$$

Então temos, $ED_1 = DE_{15}$ e $DD_1 = EE_{15}$. Contudo, a saída do primeiro estágio do processo de decriptação é $EE_{15} \,||\, DE_{15}$, que é a troca de 32 bit de entrada do 16º estágio da encriptação. Esta correspondência guarda todo percurso até o fim das 16 iterações. Em termos gerais, a iésima iteração do algoritmo de encriptação:

$$EE_i = DE_{i-1}$$

$$DE_i = EE_{i-1} \oplus F(DE_{i-1}, C_i)$$

Rearrajando os termos, teremos:

$$DE_{i-1} = EE_i$$

$$EE_{i-1} = DE_i \oplus F(DE_{i-1}, C_i) = DE_i \oplus F(EE_i, C_i)$$

Então, teremos descrito a entrada da iésima iteração como função das saídas, e estas equações confirmam as atribuições feitas na parte direita da Figura 45.

Finalmente, vemos que a saída do último estágio do processo de decriptação é $DE_0 \,||\, EE_0$. Uma troca de 32 bits recupera o texto original. Demonstrando a validade do processo de decriptação de Fiestel. Note que, a derivação não requer que F seja uma função reversível. Para vermos isso, use um caso limitado em que F produz uma saída constante (por exemplo: todos), apesar dos valores dos dois argumentos. A equação ainda serve.

D.2. Difusão

É a estrutura estatística do texto em claro é dissipada dentro das estatísticas do texto cifrado.

D.3. Confusão

Torna a relação entre as estatísticas do texto cifrado e o valor da chave de encriptação o mais complexo possível.

D.4. Algoritmo de geração da chave

Na cifra de bloco de Fiestel a chave é usada para gerar subchaves em cada estágio. Em geral, deve-se seleccionar subchaves para maximizar a dificuldade de deduzir as

subchaves e de retornar a chave principal. Hall sugeriu que pelo menos a geração da chave deve garantir o critério SAC e BIC da chave/texto cifrado.

BIBLIOGRAFIA

Livros e Folhetos

[1] AMARAL, Pedro Paulo do. Segurança de Dados e Criptografia. 1998. 15 p.Tese, Licenciatura, União Pioneira de Integração Social, 1998. 15 p.

[2] BECKET, Brian. Introduction to Cryptology and PC Security. London: McGraw-Hill Publishing Company, 1997. 345 p.

[3] CARRIÇO, José António da Silva, CARRIÇO, António João Chambel da Silva. *Computadores, Tecnologias e Sistemas de Informação*: Periféricos, Internet e Multimédia. Lisboa: CTI, 1997. 94 p.

[4] CARRIÇO, José António da Silva, CARRIÇO, António João Chambel da Silva. *Computadores, Tecnologias e Sistemas de Informação*: O Núcleo do Sistema. Lisboa: CTI, 1997. 96 p.

[5] CISCO NETWORKING ACADEMY. Network Basics. s.l.: s.n., 2000. p. 123-168.

[6] Conselho de Ministros. Política de Informática, Aprovada pela resolução Nº 28/2000 de 12 de Dezembro, 56 p.

[7] DEITEL, Harvey M., DEITEL, Barbara. Computers and Data Processing. Florida: Academic Press, 1985. 627 p.

[8] *História dos Grandes Inventos*. Porto: Selecções do Reader´s Digest., 1983. 368 p.

[9] KAHN, David. *The Story of Secret Writing*. New York: Macmillan, 1967.

[10] KAHN, David. *The Codebreakers*. New York: Macmillan, 1967.

BIBLIOGRAFIA

[11] PETROSSUIK, Yuri, MANNESTIG, Daniel. Códigos de Reflexão Irracional, 2005. Número 2. p. 73-80.

[12] RAEL, Joacilio Basilio. Criptografia: Segurança lógica de Dados. Brasilia: s.n., 1998. 40 p.

[13] SANTOS, Jorge M.L. Dias dos, LEMOS, Maria Helena Vieira S. *Iniciação a Actividade Administrativa*: Práticas Administrativa 7, 8, 9 anos de Escolaridade. 4ª Edição (actualizada). Lisboa: Edições Asa, 1990. 221 p.

[14] SOARES, Luiz Fernando Gomes, LEMOS, Guido, COLCHER, Sérgio. *Redes de Computadores*: Das LANs, MANs e WANs às redes ATM. 2ª Edição. Rio de Janeiro: Editora Campos, 1995. 576 p.

[15] STALLINGS, William. *Network Security Essentials*: Applications and Standards. New Jersey: Prentice Hall, 2000. 365 p.

[16] STALLINGS, William. *Cryptography and Network Security*: Principles and Practice. Second Edition. New Jersey: Prentice Hall, 1998. 571 p.

[17] STALLINGS, William. *Local and Metropolian Area Networks*. 5ª Edição. New Jersey: Prentice Hall, 1997.

[18] TANENBAUM, Andrew S. *Redes de Computadores*. Rio de Janeiro: Editora Campus, 1994. 786 p.

Revistas

[19] FARIA, João Pedro. Entrevista (com Eugene Kaspersky). PC Guia, Outubro, 2005, vol. 9, Nº 119, p. 94-96.

[20] Guia Completo para a segurança Informática. PC Guia, Dezembro, 2005, vol. 9, Nº 121, p. 26-51.

[21] SHEFFI, Yossi. Os Riscos são Imprevisíveis. ExecutiveDigest, Julho, 2006, Nº4 II Série, p. 11-16.

Sites

[22] A Short History of Cryptography.
http://www.all.net/books/ip/chp2.html (17/Abr/2006)

[23] Arquitectura de Computadores.
http://mega.ist.utl.pt/~ic-ac/colect-prob.pdf (01/Mar/2006)

[24] CID, Daniel. Conceitos de Criptografia. UNDERLINUX, 24 Mar. 2005. Segurança.
www.underlinux.com.br/modules.php?name=News&file=article&sid=4318
(20/Nov/2005)

[25] Criptografia.
http://www.marinha.pt/extra/revista/ra_jan2004/pag_10.html (28/Jul/2006)

[26] Criptografia e Certificação.
http://www.training.com.br/ipmaia/pub_seg_cripto.htm (20/Nov/2005)

[27] Cryptography Timeline.
http://world.std.com/~cme/html/timeline.html (17/Abr/2006)

[28] Early Cryptology.
http://home.hiwaay.net/~paul/cryptology/history.html (17/Abr/2006)

[29] Fibonacci Number.
http://mathworld.wolfram.com/fibonaccinumber.html (01/Mar/2006)

[30] Fibonacci Number.
http://pessoal.sercomtel.com.br/matematica/alegria/fibonacci/seqfib1.htm
(01/Mar/2006)

[31] Indicadores de Ciência e Tecnologia em Moçambique.
http://www.govnet.gov.mz/informacao/ciencia_e_tecnologia/indicadores_c_t_moc.pdf (10/Mai/2006)

[32] História da Criptologia.

http://www.numaboa.com.br/ criptologia/historia/index.php (17/Abr/2006)

[33] Movimento Gravitacional.
Educar.sc.usp/fisica/movgrav.html (7/Jul/2006)

[34] Mozambique's Soft ICT Infrastructure - A Pilot Study.
http://www.schoolnetafrica.net/fileadmin/resources/Moz_soft_infra_reportFIN.pdf (10/Abr/2006)

[35] Números de Fibonacci.
http://www.cin.ufpe.br/~if670/1-2003/lovasz-capitulo4.pdf (01/Mar/2006)

[36] Scan ICT Mozambique - Final Report.
http://www.uneca.org/aisi/scanghana/documents/3.%20Scan%20ICT%20Mozambique.pdf (10/Abr/2006)

[37] The Basics of Cryptography.
http://fisher.osu.edu/~muhanna_1/pdf/crypto.pdf (10/Nov/2005)

[38] The Life and Numbers of Fibonacci.
http://plus.maths.org/issue3/fibonacci/feat.pdf (01/Mar/2006)

[39] UniCERT – Brasil.
www.unicert.com.br (20/Nov/2005)

[40] www.wikipedia.org

Conferências

[41] CHEMANE, Lourino. Mozambique ICT Policy Implementation Strategy and e-Government: Challenges and Opportunities. Regional Workshop on Building e-Governance capacity in Africa, ca. 2002.
http://unpan1.un.org/intradoc/groups/public/documents/CAFRAD/UNPAN006472.pdff (11/Jul/2006)