Universidade Eduardo Mondlane
Faculdade de Ciências
Departamento de Matemática e Informática

Trabalho de Licenciatura

Transmissão de dados através de um rádio canal utilizando um novo sistema de criptografia

Safrina Semião Zunguze
Julho 2004

Universidade Eduardo Mondlane
Faculdade de Ciências
Departamento de Matemática e Informática

Trabalho de Licenciatura

Transmissão de dados através de um rádio canal utilizando um novo sistema de criptografia

Supervisor
Prof. Dr. Yuri Petroussiuk

Co-Supervisor
Eng. Daniel Mannestig

Autora
Safrina Semião Zunguze
Julho 2004

Dedicatória

Ao meu esposo, Henrique Joaquim Macuacua e aos nossos filhos; Yanick Stefan Semião Macuacua e Kelsy R. Henrique Macuacua.

Agradecimentos

Os especiais agradecimentos à todos que contribuíram directa ou indirectamente para a elaboração deste trabalho:

Aos meus supervisores, Prof. Dr. Yuri Petroussiuk e Eng. Daniel Mannestig, toda a paciência e perseverança com que me acompanharam.

De seguida quero agradecer à minha família, em especial ao meu esposo, sem o apoio do qual não teria sido possível concluir os meus estudos. O meu muito obrigada.

Por ultimo, mas não com menos importância, agradeço aos meus colegas de faculdade pela coragem que me deram quando me sentiam a vacilar. Um especial agradecimento, ao Azarias Tomás J. Muchanga, ao Anselmo Leonardo O. Nhane, e a Atanasia Mapapa que sempre estiveram disponíveis quando precisei de ajuda.

Declaração de honra

Declaro por minha honra, que este trabalho é fruto da minha profunda investigação e não foi submetido para um outro grau que não seja o indicado, Licenciatura em Informática na Universidade Eduardo Mondlane.

Maputo, Julho de 2004

A autora

Safrina Semião Zunguze

RESUMO

A evolução das novas tecnologias de informação tem facilitado extraordinariamente a comunicação entre Empresas e pessoas no mundo inteiro, entretanto a segurança da informação constitui uma grande preocupação no ambiente de comunicação, sendo este um dos assuntos mais comentados actualmente nos meios da tecnologia da informação.

O rádio canal é um dos ambientes de comunicação, que apesar de trazer vantagens, tem alguns problemas como:

- o acesso ilegal de um *Hacker* ou *terrorista*;
- transmissão da informação sem erros;
- melhoramento das características do sistema de transmissão.

Ao longo deste trabalho foram abordados aspectos de segurança na transmissão da informação, suas vulnerabilidades. Tipo de atacantes a sistemas de informação e formas de ataques. Formas de protecção da informação contra as diferentes formas de ataques.

Neste trabalho foi proposta uma nova ideia de transmissão da informação digital através do Radio Canal usando códigos com base irracional.
O uso deste método permite utilizar na transmissão da informação o Sistema de Numeração Posicional e o Sistema de Numeração não Posicional, melhorando consideravelmente as características básicas e garantir com alta probabilidade:

- Processamento da informação sem erros;
- Transmissão da informação sem erros;
- Protecção da informação contra o acesso ilegal.

Para elaboração do presente trabalho, foi necessário realizar consultas a bibliografia (e a páginas da Internet) relacionada com a segurança e protecção da informação, e participação em algumas palestras.

Índice

Índice de Figuras e Tabelas

1 INTRODUÇÃO

Diariamente, no mundo inteiro, redes de computadores e hosts são invadidos. O nível de sofisticação destes ataques varia amplamente; enquanto geralmente se acredita que a maioria das invasões tem sucesso devido a códigos secretos fracos, há ainda um número grande de intrusões que usam técnicas mais avançadas para invadir. Pouco se sabe sobre a maioria das técnicas de invasão, porque elas podem ser de diversa natureza e então tornam-se muito mais difíceis de descobrir (Oliveira, 2001).

Até à década de 80, quando experiências iniciadas no projecto ARPANET conseguiram estabilizar um primeiro protocolo para *routing* de dados entre redes autónomas (BGP 4, que ainda faz parte do conjunto de padrões TCP/IP), a tecnologia para interligação de computadores permitia apenas redes com hierarquia fixa, que pressupõem o controlo de algum meio ou infra-estrutura de comunicação, usado para interligar os seus componentes. O projecto ARPANET foi motivado por um sentimento de insegurança e relativa paranóia em relação ao risco de ataque nuclear a que estava exposta a infra-estrutura de telecomunicações das forças armadas norte-americanas, dando início ao desenvolvimento de tecnologia para redes abertas, onde redes de computadores já operantes poderiam ser interligadas sem necessidade de controlo centralizado no processo de *routing* adaptativo para o tráfego de pacotes de dados (Oliveira, 2001).

A tecnologia de redes com hierarquias abertas para transmissão de dados permitiu que interligações entre computadores pudessem atingir escala mundial, ao evitar o colapso decorrente da explosão exponencial das tabelas *routing*, já que tal explosão seria inevitável em arquitecturas fechadas nesta escala, criando assim o potencial de interligação via TCP/IP através da infra-estrutura mundial de telecomunicações então disponível. O serviço de tipo "melhor esforço" para *routing* de pacotes IP pôde ser utilizar-se da capacidade ociosa inerente às redes de transmissão e comutação telefónica, para fornecer ligações de dados em escala mundial às redes de computadores já existentes, pela adesão aos protocolos de transportes TCP e UDP.

Este potencial de interligação relativamente simples e barato induziu a sua própria procura, forçando mudanças em cascata no perfil da procura tecnológica e de serviços nas telecomunicações (Oliveira, 2001).

Estas explosões da procura, e a transformação social que engendram, acorrem num contexto cognitivo inédito para a humanidade. Até aos anos 80 a forma de se conceberem redes de computadores, a nossa tradição cultural que legitima a autoridade dos discursos, a nossa organização social que transmite e consolida valores, moldando assim a nossa percepção e acção no mundo, sempre se haviam enquadrado em modelos hierárquicos fechados de redes de comunicação. A Internet não se enquadra, e tentar enquadrá-la por força do hábito constitui aquilo que designamos por verdadeiro *bug* do milénio. Referências à "Internet comercial" não implicam, como o termo pode sugerir, a sua posse ou controlo por alguma empresa, mas a etapa da sua evolução na qual empresas vendendo transporte e distribuição de tráfego electrónico de dados, serviços ou produtos, passam a criar associações estratégicas para desempenhar com melhor fiabilidade e eficácia as suas funções. A Internet não tem dono, gestor, comando central ou direcção. Guia-se por um método de cooperação *sui generis* para propostas e validações de novos padrões operacionais e políticas de gestão cooperada.

A Criptografia pode proteger o acesso ao valor sintáctico e a integridade das cadeias de bits nas comunicações de dados, o que é apenas um dos ângulos da questão que se esta a abordar. Precisamos confiar não apenas nos controlos de acesso a essas cadeias de bits e na sua integridade, mas principalmente no significado das mensagens que estas cadeias veiculam. Precisamos confiar no significado do que se desenha no ecrã do monitor e dos programas que se executam no CPU das máquinas, expressos através dessas cadeias de bits, sendo portanto sensato associar este outro lado da questão, e de natureza semântica, à dessas cadeias. É ai que o alcance e os limites das técnicas criptográficas – e as diferenças fundamentais entre redes de hierarquia fixa e aberta – começam a se manifestar. A compreensão de significados inicia-se pela identificação de referências de significantes. E as redes "fluidas" apresentam sérios

problemas relacionados com a confiança que se pode ter em processos de identificação que nelas operam.

Nenhuma área da informática é tão vasta como a segurança da informação: o ponto principal da segurança leva a um outro ponto principal, o ser humano, isso mesmo, todo o processo de segurança se inicia e tem o seu término num ser humano. Não adianta nada gastarmos fortunas em equipamentos e sistemas de segurança se não conhecermos quem utilizará os nossos sistemas, e quem pode ter acesso a eles mesmo sem autorização.

No ciberespaço, a percepção do que é ser herói ou bandido dissipa-se nos interesses pessoais, opções políticas, ideologias e vínculos ao poder, e a acção puramente sintáctica da criptografia encontra enormes obstáculos para realizar o papel principal que pode exercer no processo da segurança de redes fechadas (Oliveira, 2001).

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um tema complexo e pode abranger várias situações: erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, etc. Com a intensificação do uso da Internet, pelas empresas – particularmente, após o advento do comércio electrónico, a segurança tem sido um assunto que vem exigindo maiores cuidados do que aqueles até então existentes, embora haja quem entenda que esta preocupação não é assim tão importante. A tecnologia, em si mesma, não pode ser considerada a única peça de um projecto de segurança. Porém, ela tem um papel vital neste tipo de projecto. Para dar conta da crescente procura, fornecedores e integradores passaram a propor políticas gerais de segurança para empresas, incluindo nos seus catálogos serviços de certificação das soluções de segurança e implementação de processos de contra-engenharia social, entre outra inovações (Oliveira, 2001).

A segurança da informação define-se como o processo de protecção de informações e activos digitais armazenados em computadores e redes de processamento de dados.

A segurança não é uma questão técnica, mas uma questão estratégica e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem formar e consciencializar o nível administrativo da empresa e todos os seus funcionários.

Os elementos básicos da segurança da informação são:

- Confidencialidade: proteger informações confidenciais contra revelação não autorizada ou captação compreensível.
- Disponibilidade: garantir que informações e serviços vitais estejam disponíveis quando requeridos.
- Integridade: manter informações e sistemas computadorizados, entre outros activos, exactos e completos.

Na gestão empresarial integrada na empresa virtual, os gestores deverão ter uma política de segurança bastante eficaz, pois qualquer tomada de decisão depende da informação. A área de tecnologia deve garantir o controlo de acesso às informações.

A informação tem um valor inenarrável. Além disso, na Empresa Virtual, a informação passa a ser "conduzida" pelo mundo todo, dependendo de como está estruturada a Empresa Virtual.

As lideranças de um programa de transformação devem estar conscientes que qualquer projecto de mudança pode ser sabotado. Precisam saber como essas sabotagens tendem a ocorrer na sua organização e como devem proceder para evitá-las.

Na gestão empresarial integrada na empresa virtual, os gestores devem preocupar-se com:

- quão seguros estão as bases de dados da empresa;
- quais os planos de contingência em caso de catástrofes;
- qual o critério de acesso aos servidores de base de dados;
- qual o nível de confiança nas pessoas, sejam internas ou terceiros em *outsourcing*;
- qual o critério de auditoria para prevenir desastres;
- qual o tipo de formação para as pessoas envolvidas no ciclo completo da informação;
- quais os aspectos jurídicos a serem tratados com o uso incorrecto da informação;
- quais os procedimentos de auditoria interna de sistemas;
- quais os procedimentos de auditoria externa de sistemas.

Toda a informação tem valor e precisa ser protegida contra acidentes e contra ataques de *Hackers* e *Crackeres*.

A segurança da informação tem a finalidade de garantir disponibilidade, sigilo, integridade, autenticidade, controlo de acesso e não-repúdio das informações.

Segurança

Devemos ter como premissa básica que: não existe nenhum sistema seguro em todos os aspectos.

"o único sistema que é totalmente seguro é aquele que não possui nenhuma forma de acesso externo, está trancado numa sala totalmente lacrada e da qual uma única pessoa possui a chave. E esta pessoa morreu no ano passado."

Existem diferenças fundamentais na segurança voltada para o mercado corporativo onde nos deparamos com a utilização de tecnologias avançadas com alta capacidade de tráfego e gestão de estações quando comparadas com a segurança voltada para o mercado doméstico, do utilizador da Internet ou da dona de casa que guarda suas receitas no computador.

Os principais atentados à segurança que se pode sofrer usando o computador pessoal dividem-se em três grandes categorias que muitas vezes estão interligadas, sendo necessário um ataque a uma categoria antes de se iniciarem os ataques às outras. São elas: ataques à privacidade, destruição e obtenção de vantagens.

Ataques à privacidade – este é o ataque directo mais comum ao utilizador doméstico. Assim como muitas pessoas têm compulsão em ler correspondência alheia ou observar vizinhos com binóculos, os *hackers* têm compulsão em "dar uma olhadela" à sua vida pessoal e a melhor maneira de se descobrir coisas sobre a vida de uma pessoa é olhar para dentro do seu computador. Os principais alvos são os e-mails enviados, recebidos e apagados, histórico de visitas de sites ou "ficheiros.doc", que podem conter cartas, procurações, contractos, etc.

Destruição – Apesar de ser perfeitamente possível para um *hacker*, uma vez estando dentro de um computador, destruir dados nele existentes, as estatísticas mostram que grande maioria dos incidentes nos quais há perdas de informação a causa é a acção de vírus ou programas com funções semelhantes, que raramente são implantados de forma propositada. Geralmente a infecção ocorre com programas recebidos de terceiros que muitas vezes também não sabem que estão infectados.

Obtenção de Vantagens – para se obter vantagens causando incidentes de segurança nos computadores pessoais geralmente é necessária a utilização de técnicas onde primeiro a vítima será exposta a ataques de privacidade ou destruição. As motivações deste tipo de ataque são tão distintas quanto o seu próprio objectivo real.

Computadores e equipamentos informatizados podem comunicar uns com os outros através de *standards* estabelecidos que ditam como cada participante na conversa se deve comportar. O padrão utilizado na Internet (e na maioria dos sistemas actuais) é o chamado "Cliente/Servidor".

A comunicação num ambiente cliente/servidor é composta de dois módulos básicos: um módulo que faz requisição dos serviços – cliente e outro que recebe estes pedidos para executar as tarefas pedidas – servidor e, eventualmente , retornar o resultado desta tarefa. Este esquema é muito utilizado quando se faz uma ligação a Internet.

A maior parte dos programas utilizados no computador só precisam de fazer pedidos e esperar a resposta, ou seja, são programas clientes. Teoricamente é isso o que deve acontecer, mas nem sempre os nossos computadores são tão inofensivos. Os maiores vândalos dos últimos anos são programas que invertem este papel, fazendo com que os nossos computadores se tornem servidores. A maioria arrasadora vem na modalidade de "cavalos de Tróia", por isso se convencionou chamar a este método "invasão através de cavalos de Tróia ".
O que acontece geralmente, é que um utilizador recebe um programa de alguém, através de qualquer meio – por e-mail, ICQ, fazendo um download ou por disquete e executa-o. Este programa, após ser executado, instala um "servidor "que passa a responder aos pedidos de ligação pela Internet. Os tipos de pedidos que ele pode aceitar e executar variam de acordo com o "servidor" instalado.

Uma característica presente neste tipo de comunicação é a necessidade de se atribuir "portas de comunicação" por onde os pedidos e as respostas irão passar. Todos os programas para uso na Internet utilizam portas que geralmente são abertas com intuito de fazer pedidos a servidores remotos. Quando um computador está, digamos "infectado" por um programa servidor, este abre uma porta naquele, de forma a permitir que outros computadores façam pedidos através dela.

Pode-se perceber que não é necessário nem interessante impedir que os nossos computadores abram portas. Se isso for feito, nenhum dos nossos programas irá funcionar. O que deve-se fazer é impedir que programas maliciosos abram portas para receber ligações. Através delas é que os hackers vasculham os computadores.

Cavalo de Tróia ou trojan Horse

"Em tempos os gregos tentaram invadir Tróia, mas os troianos insistiram em resistir. Muito tempo se passou e nada; até que os estrategos gregos tiveram a brilhante ideia de criar um cavalo de madeira gigante dentro do qual iriam colocar a infantaria grega, sendo o cavalo enviado como presente para troianos como declaração de paz. Recebido o presente, os troianos fizeram uma grande festa, e depois dela, quando todos já dormiam, os gregos saíram de dentro do cavalo e atacaram Tróia para conquistá-la. Essa história ficou conhecida como Cavalo de Tróia."

Um *trojan Horse* funciona da mesma forma: é recebido um programa que diz que é um jogo, foto ou texto e que, quando se tenta usar, aparentemente não acontece nada. Depois, quando se liga à Internet, corre-se o risco de ser invadido, pois esse programa permite que um utilizador remoto controle o computador (Oliveira, 2001).

Alguns sintomas:

- o seu computador é reiniciado ou desligado sem sua ordem;
- o *drive* do CD-ROM abre e facha sem o seu comando;
- o *Windows* passa uma mensagem estranha, ameaçadora ou mal-educada;
- e outros.

Normalmente quem invade computadores dessa forma está a procura de códigos secretos, documentos, ficheiros, programas ou até mesmo de causar sustos ou estragos.

Como prevenir-se de invasões:

- ter sempre um bom antivírus actualizado no computador;
- nunca ter no computador programas de invasão pois, por puro descuido, o tiro pode sair pela culatra;
- manter sempre os códigos secretos bem protegidos.

Backdoors

Os *backdoors* são muito utilizados para estabelecer uma porta de entrada num servidor ou num computador qualquer e estão a ser mais utilizados através da popularização do *back*

office. Como têm o servidor e o cliente para Windows a sua disseminação pela Internet foi enorme.

Backdoor como o próprio nome indica é uma "porta dos fundos", por onde o produtor do sistema tem acesso aos sistemas a qualquer momento. Os *backdoors* são criados de maneira intencional ou por "engano" dos produtores do software em questão.

Com o *backdoor* o produtor do sistema cria uma "passagem secreta" que apenas ele sabe onde se encontra, mas com o aumento de peritos em segurança e principalmente em quebra de segurança, muitos desses *backdoors* foram descobertos por pessoas que por vezes, tinham más intenções, como por exemplo invadir um sistema.

Estratégias para Segurança

Desenhar uma estratégia de segurança depende muito da actividade que se esta a desenvolver. Podemos considerar os seguintes passos gerais:

- criar uma política global de segurança;
- realizar análises de riscos;
- aplicar medidas correspondentes.

Política global de segurança: deve estabelecer um *status* da informação para a empresa ou para a organização, conter um objectivo geral, a importância da tecnologia da informação para a empresa, o período de tempo de validade da política, os recursos com que se conta, os objectivos específicos da empresa.

Deve estabelecer a qualidade da informação com que se manejam os objectivos, a qualidade que deve ter a informação, deve decidir que se estabeleça quando e para quem a informação deve ser confidencial, quando deve verificar a sua integridade e quando deve verificar a autenticidade tanto da informação como dos utilizadores.

Análise de risco: consiste em enumerar todo o tipo de riscos e quais destes expõem a informação e quais são as consequências, os possíveis hackers entre pessoas das

empresas e dependências de inteligências, etc., enumerar todo tipo de possibilidade de perdas directas como dinheiro, clientes, tempo, etc., assim como indirectas: créditos, perda de imagem, perda de confiança, etc.

Em análise de risco deve-se também incluir os possíveis ataques que possam existir e os seus possíveis efeitos.

Medidas de segurança: esta parte pode ser planeada como a determinação de toda a estrutura de segurança da informação. Uma vez planeada uma política de segurança, decidir quanto vale a informação. Devemos estabelecer as medidas para o cumprimento da política de segurança, para que as perdas sejam o menor possíveis.
As possíveis medidas a estabelecer podem dividir-se segundo a tabela:

Table 1 Medidas de segurança

Tipo	Protecção Física	Medidas Técnicas	Medidas de Organização
Preventivas	PF	PT	PO
Detectivas	DF	DT	DO
Correctivas	CF	CT	CO

PF: guardas na entrada do edifício, controlo de acesso de entrada, protecção ao hardware, dados, etc.

DF: monitor de vigilância, detector de metais, detector de movimento, etc.

CF: respaldo de fonte de poder, etc.

PT: *firewalls*, criptografia, etc.

DT: controlo de acesso lógico, secção de autenticação, etc.

CT: programa antivírus, etc.

PO: cursos de actualização, organização das chaves, etc.

CO: respaldos automáticos, plano de incidentes (sanções), etc.

3 CRIPTOGRAFIA

3.1 Breve historial

A criptografia é algo bastante antigo, tão antigo quanto a escrita. Era usada no antigo Egipto e na Mesopotania. No *Kama-Sutra*, é citada como uma das 64 artes, ou yoga, que a mulher deveria conhecer e praticar. Na Grécia antiga, o que hoje conhecemos como civilização ocidental teria sido extinto se não fosse uma mensagem criptografada avisando da invasão persa. Júlio César também relatou o uso de mensagens cifradas em seu livro, sobre as Guerras Gálicas. Seu nome foi dado a qualquer tipo de alfabeto cifrado semelhante ao que usou : alf. César: D E F G H I J K L M N O P Q R S T U V X Y Z A B C D (sabugo, 1999). Esta foi utilizada pelos egípcios há mais de 4000 anos e, mais tarde, também pelos romanos.

Do trabalho de Feistel na IBM, no inicio dos anos 70 até à adopção do DES (Data Encryption Standard) em 1977 iniciou-se uma nova era na criptografia. O mais arrebatador desenvolvimento na história da criptografia surgiu em 1976 quando Diffie e Hellman publicaram "New Directions in Cryptography", onde foi introduzido um conceito revolucionário de criptografia assimétrica. Em 1978, Rivest, Shamir e Adleman descobriram a primeira aplicação prática deste método, hoje designado RSA (Domingues, 2000).

Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de códigos. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

3.2 Terminologia

Em geral, considera-se a necessidade de transmitir uma **mensagem** (*M*), entre um **emissor** e um **receptor**. A mensagem designa-se por **texto simples**. Na realidade, esta designação não significará texto propriamente dito, corresponderá antes a qualquer sequência de *bits* que se pretenda transmitir em segurança. O processo de disfarçar a

mensagem chama-se **cifragem/encriptção** e transforma o texto simples num **criptograma** (C). O processo de recuperar o texto simples original a partir do criptograma denomina-se **decifragem/decriptção** (Schneier, 1999).

Por seu turno, a **criptanálise** é a ciência (e arte) de quebrar criptogramas, ou seja, descobrir como fazer a decifragem de um criptograma, sem saber, à partida, como ele foi cifrado. Há um ramo da matemática, a **criptologia**, que engloba a criptografia e a criptanálise (Schneier, 1999).

Os **algoritmos de criptografia**, também denominados **cifras**, são as funções matemáticas que fazem a cifragem e a decifragem, tendo, portanto, em geral, dois componentes, respectivamente, o **algoritmo ou função de cifragem** (E)

$$E(M) = C \tag{1}$$

e o algoritmo ou função de decifragem (D)

$$D(C) = M \tag{2}$$

devendo, naturalmente, verificar-se

$$D(E(M)) = M \tag{3}$$

Se a segurança de um algoritmo é baseada no seu secretismo, classifica-se como **restrito**. Actualmente são pouco utilizados porque, quanto maior é o número de utilizadores, maior é a probabilidade de algum deles revelar o segredo, quebrando a segurança de todo o sistema. A sua utilização restringe-se a aplicações de baixa segurança (codificadores de vídeo, por exemplo).

Todos os actuais algoritmos seguros são conhecidos e usam, no seu funcionamento, uma **chave/senha**. Basicamente a chave é um número k

$$k \in K$$

em que **K** é o espaço finito das chaves, que interessa ser de grande dimensão, para uma maior segurança.

Em algoritmos com chave, as três primeiras equações, podem rescrever-se na forma

$$E_k(M) = C \tag{4}$$

$$D_k(C) = M \tag{5}$$

$$D_k(E_k(M)) = M \tag{6}$$

As chaves devem definir univocamente o criptograma, ou seja

$$E_{k1}(M) \neq E_{k2}(M) \quad \text{se} \quad k_1 \neq k_2$$

Com maior generalidade, considera-se a utilização de duas chaves diferentes, uma de cifragem e outra de decifragem vindo

$$E_{k1}(M) = C \tag{7}$$

$$D_{k2}(C) = M \tag{8}$$

$$D_{k2}(E_{k1}(M)) = M \tag{9}$$

Nos **algoritmos simétricos**, a chave de cifragem pode ser obtida a partir da chave de decifragem, e vice-versa, sendo as duas chaves, normalmente, idênticas. Em qualquer caso, é necessário, que o emissor e o receptor acordem numa chave, antes de poderem usar o sistema.

Nestes algoritmos, a segurança reside no secretismo da chave. Visto que o funcionamento do algoritmo é conhecido, sabendo a chave, é possível cifrar e decifrar qualquer mensagem.

De modo a obviar a este problema surgiram os **algoritmos assimétricos ou de chave pública**, em que as duas chaves são obrigatoriamente diferentes, com a condicionante de a chave de decifragem ser impossível de obter a partir da chave de cifragem (pelo menos num tempo aceitável).

Chamam-se de chave pública, porque a chave de cifragem pode ser divulgada, permitindo a qualquer emissor enviar mensagens cifradas para um destinatário que, só ele, conhece a chave de decifragem. O sistema inverso também é possível, isto é, publicar a chave de decifragem e manter secreta a chave de cifragem, e designa-se por sistema de **assinatura**. Permite garantir a autenticidade das mensagens do emissor (Sabugo, 1999).

Os algoritmos de cifragem podem também dividir-se em duas categorias conforme a maneira como subdividem as mensagens a cifrar. Os algoritmos de **cifra corrida** (*stream cipher*) fazem um tratamento bit a bit do texto original. Os **algoritmos de blocos**, tratam um determinado número de *bits* simultaneamente. Em implementações usando computador a dimensão do bloco é, normalmente, 64 bits - um valor suficientemente grande para afastar a criptanálise e suficientemente pequeno para ser tratável.

Caracterização das funções de cifragem

Seja

- V o conjunto dos caracteres usado para formar o texto simples
- W o conjunto dos caracteres usado para formar o criptograma
- V* e W* representam os conjuntos das palavras construídas a partir de V e W, respectivamente.
- ξ representa a palavra vazia.

No caso geral, se Z* for um conjunto de todas as palavras obtidas a partir de um conjunto de caracteres Z, temos

Z^n $\prod$ Z* designa o conjunto de todas as palavras de comprimento n

Z(n) é o conjunto de todas as palavras de comprimento ¾ n incluindo ξ.

Define-se então uma cifragem como uma relação

X: V* -> W* com v a w

Para que o receptor seja capaz de reconstituir a mensagem sem ambiguidades uma cifragem é injectiva, i.e. não ambígua da direita para a esquerda: (x a z) ⇒ (y a z) ⇒ $x = y$

No entanto uma mesma letra do texto simples pode dar origem a várias outras que se denominam as suas **homófonas**. Se a relação X for bijectiva, é uma função e a cifragem é determinística, relacionando de 1 para 1 todos os elementos de V* com os de W*.

Seja então um sistema de cifragem definido do seguinte modo:

$M = \{x_0, x_1, \ldots, x_{\theta-1}\}$ com $x_i : V^{(n_i)} \rightarrow W^{(m_i)}$

cada x_i é denominado um passo de cifragem e $\theta = |M|$ é a cardinalidade do sistema, n_i é a largura (máxima) de cifragem do texto simples, e mi é a largura (máxima) cifrada do passo de cifragem (relação) x_i.

Um passo de cifragem em que V=W denomina-se **endomórfico**.

Uma cifragem $X = [x_{i1}, x_{i2}, x_{i3}, \ldots]$ gerada por M é **monoalfabética** se só tem um passo de cifragem (um alfabeto). De outro modo é **polialfabética**.

Uma cifragem é **monográfica** se todos os n_i forem iguais a 1, e **poligráfica** nos outros casos.

No caso mais restrito em que $x_i : V^n \rightarrow W^m$

- se n=2, 3, 4, ... temos grupos de caracteres no texto simples, denominados, respectivamente, **digramas**, **trigramas**, **tetragramas**,...

- se m=1, 2, 3, ... temos grupos de caracteres no criptograma, denominados, respectivamente, **unipartidos**, **bipartidos**, **tripartidos**,...

Frequentemente neste caso (palavras de comprimento fixo) escolhe-se V=W e m=n, o que dá origem a um sistema de cifragem em blocos, no sentido restrito.

3.3 Encriptação e Decriptação

A encriptação ou cifragem consiste na aplicação de um algoritmo aos dados por forma a que eles se tornem ilegíveis, para recuperar os dados originais será necessário conhecer o algoritmo de desencriptação ou decifragem

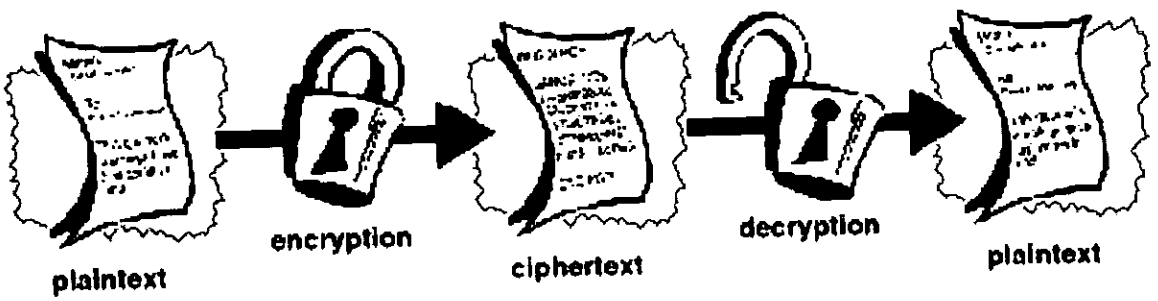

Figure 1 Encriptação e Decriptação

3.4 O que é Criptografia?

Criptografia é a ciência de usar a matemática para encriptar ou decapitar dados. Permite guardar informação sensível ou transmiti-la numa rede insegura, como Internet de tal modo que não pode ser lida por alguém a quem não se destina.

Enquanto que a Criptografia consiste na ciência (e arte) da transformação de texto simples em texto ilegível, de tal modo que apenas quem saiba qual o processo de reverter a transformação possa recuperar o texto original, a criptanálise é o que faz quem quer tentar descobrir o conteúdo de uma mensagem cifrada. Sendo uma actividade associada a alguém que pretende "atacar" uma cifra, é também o processo que permite avaliar a qualidade de uma cifra - se não for possível, ou for extremamente demorado, por criptanálise, decifrar um criptograma, então o algoritmo de cifra é garantidamente seguro. Como tal, qualquer novo algoritmo de criptografia só é considerado seguro depois de resistir, com êxito, à criptanálise de outros investigadores.

Os principais tipos de criptanálise que existem são:

1. **Ataque apenas com texto cifrado**

   O atacante possui apenas cifras (com o mesmo algoritmo) de várias mensagens. O objectivo é recuperar o texto original, ou, melhor ainda, deduzir a chave ou chaves.

   Dados: $C_1 = E_k(M_1), C_2 = E_k(M_2), \ldots, C_i = E_k(M_i)$

   Deduzir: $M_1, M_2, \ldots, M_i$; ou k; ou um algoritmo para inferir M_{i+1} a partir de $C_{i+1} = E_k(M_{i+1})$

2. **Ataque com texto simples conhecido**

   O atacante possui cifras (com o mesmo algoritmo) de várias mensagens conhecidas. O objectivo é idêntico ao anterior.

   Dados: $M_1, C_1 = E_k(M_1), M_2, C_2 = E_k(M_2), \ldots, C_i, E_k = (M_i)$, Deduzir: k ou um algoritmo para inferir M_{i+1} a partir de $C_{i+1} = E_k(M_{i+1})$

3. **Ataque com texto simples escolhido**

   Semelhante ao anterior, com a diferença de ser o criptanalista a escolher o texto das mensagens a cifrar

   Dados: $M_1, C_1 = E_k(M_1), M_2, C_2 = E_k(M_2), \ldots, C_i, E_k = (M_i)$, com $M_1, M_2, \ldots, M_i$ escolhidos

   Deduzir: k ou um algoritmo para inferir M_{i+1} a partir de $C_{i+1} = E_k(M_{i+1})$

4. **Ataque adaptativo com texto simples escolhido**

   Caso particular do anterior em que os Mi não precisam de ser escolhidos todos à partida, mas podem ir sendo escolhidos à medida que se conhecem os resultados da cifragem anterior

5. **Ataque com texto cifrado escolhido**

   Os criptanalistas podem escolher diferentes C_i e ter acesso aos M_i resultantes da respectiva decifragem

   Dados: $C_1, M_1 = D_k(C_1), C_2, M_2 = D_k(C_2), \ldots, C_i, M_i = D_k(C_i)$. Deduzir: k

Como já foi referido, os algoritmos de cifragem considerados seguros são aqueles de que se conhece o funcionamento, sendo secreta apenas a chave. Na realidade, os algoritmos restritos são quebráveis, dependendo isso apenas do tempo e dinheiro disponíveis pelo criptanalista (normalmente é necessário muito menos do que seria de esperar...):

- Em sistemas comerciais, implementados em código é uma questão de descodificar (*disassembly*) o programa e recupera-se o algoritmo.
- Em sistemas de comunicação militares é uma questão de comprar (ou roubar) um equipamento e recuperar o algoritmo a partir da maneira como o aparelho está construído.

Os ataques a um sistema de comunicações seguro, isto é, um sistema em que as mensagens são cifradas, podem ter um dos seguintes três objectivos:

1. Determinar o conteúdo da mensagem M - problema de **Privacidade**
2. Alterar M para M', de modo a ser aceite pelo receptor como tendo sido enviada pelo emissor de M - problema de **Autenticação**

3. Iniciar uma comunicação com um receptor, como se fosse um emissor autorizado - problema de **Disputa**

Nem sempre é necessário que o sistema garanta, simultanêamente, defesas contra estes três tipos de ataques, de modo que as técnicas criptográficas a aplicar dependem do objectivo da protecção pretendida.

Medidas de Segurança

Um algoritmo é considerado seguro se não puder ser quebrado com os recursos computacionais existentes, actualmente ou no futuro. É de realçar que, dada a evolução da velocidade de processamento dos computadores, é necessário prever uma margem de complexidade do algoritmo, de modo a não poder ser quebrado em tempo útil nas próximas décadas.

Ex: são considerados seguros algoritmos que, mesmo com 106 processadores cada um a realizar 106 cifragens por segundo, demorem a quebrar um tempo comparável... à idade do universo!!! (ou mesmo um pouco menos, claro...).

A segurança do algoritmo de criptografia é, portanto, a dificuldade associada à inversão dos algoritmos de cifragem do sistema. Uma das maneiras de avaliar a segurança do algoritmo é através da incerteza associada ao espaço das chaves **K**, e que, sendo as chaves todas equiprováveis de serem usadas, é $H(K) = \log\#\mathbf{K}$.

3.5 Criptografia Convencional

Também chamada de Criptografia de chave secreta ou simétrica. Usa uma única chave para encriptar e decriptar o texto. DES é o grande exemplo.

O DES (*Data Encryption Standard*) é um algoritmo simétrico, de blocos, que surgiu a partir de um outro algoritmo LUCIFER, desenvolvido pela IBM. Foi adoptado, em 1976, como um "standard" nos EUA sob o patrocínio do NBS (*National Bureau of Standards*) e tem tido, desde então, uma grande utilização, inclusivamente em empresas privadas.

Apesar da sua divulgação generalizada em todo o mundo, a lei dos EUA não permite a exportação de qualquer implementação do algoritmo.

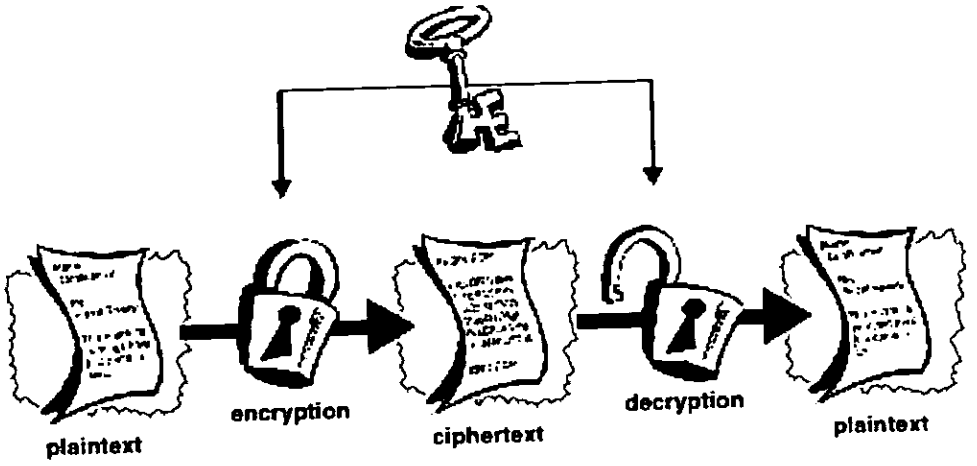

Figure 2 Criptografia Convencional

O grande problema da criptografia convencional é a segurança da chave. Vamos usar dois personagens, Alice e Bruno, para exemplificar a troca de mensagens cifradas. Na criptografia convencional, Alice e Bruno usam a mesma senha para cifrar e decifrar mensagens. Para combinar a senha a ser utilizada, Alice e Bruno precisam se encontrar pessoalmente ao menos uma vez.

Criptografia convencional é rápida, apropriada para dados que não transitam na rede. Cara se usada para informação que transita na rede, devido a gestão do processo de distribuição da chave secreta.

3.6 Criptografia de chave pública

Também chamada de Criptografia Assimétrica, utiliza duas chaves: uma pública que pode ser divulgada e outra secreta conhecida somente por pessoas autorizadas. Em um sistema de chave pública, cada pessoa tem duas chaves: uma chave pública e uma privada. As mensagens criptografadas com uma das chaves do par só podem ser decriptografadas com a outra chave correspondente; portanto qualquer mensagem criptografada com a chave privada só pode ser decriptografada com a chave pública e

vice-versa. Como o nome sugere, normalmente a chave pública é mantida universalmente disponível e a chave privada é mantida em segredo.

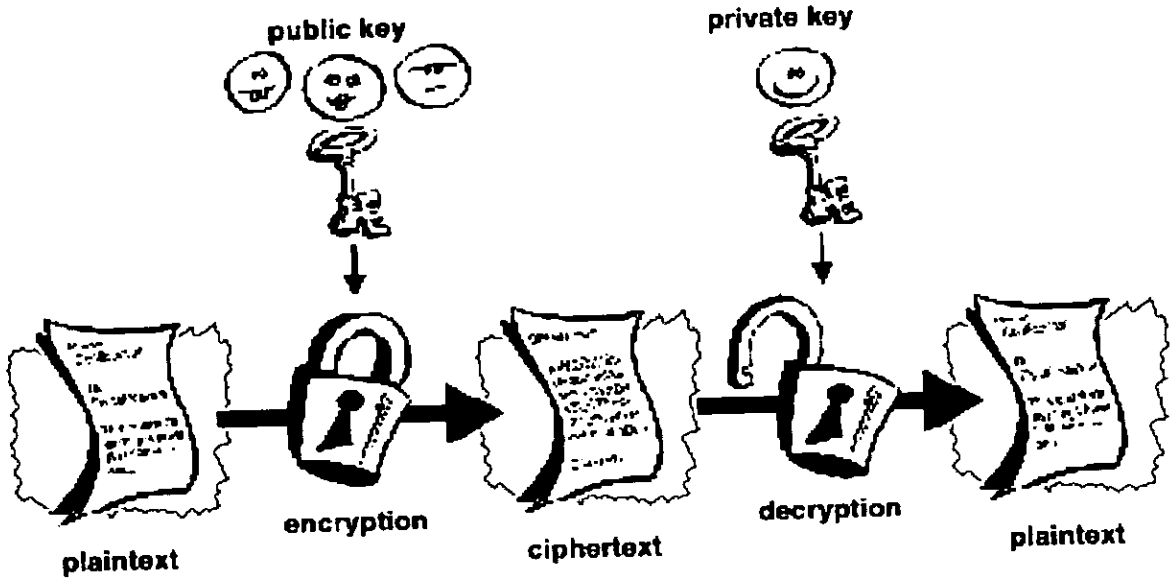

Figure 3 Criptografia de Chave Pública

Computacionalmente ou Matematicamente não é possível deduzir/derivar a chave secreta a partir da chave publica.

Alguns exemplos de sistemas de Chave Pública são:

- **RSA**

Nome de um procedimento criptográfico desenvolvido por Ronald Rivest, Shamir e Leonard Adleman do MIT. RSA pode ser usado para encriptação de informações e assinaturas digitais. As chaves podem ter vários tamanhos dependendo do tipo de implementação. Chaves maiores geralmente são mais seguras.

- **Elgamal**

Desenvolvido por Taher Elgamal, é baseado na exponenciação e aritmética modular. É usado principalmente para encriptação de assinaturas digitais de uma maneira similar ao RSA.

- **Diffie-Hellman**

Diffie-Hellman não é actualmente um método de Encriptação e Decriptação, mas um método de desenvolvimento e trocas de um compartilhador de chaves privadas em cima de um canal de comunicação público. No efectuar, as duas partes concordam em alguns valores numéricos, e cada parte cria uma chave. Transformações matemáticas das chaves são trocadas. Cada parte pode então calcular uma terceira sessão da chave que não pode facilmente ser derivada por um ataque sem conhecer ambas as trocas de valores. As chaves podem ter vários tamanhos dependendo do tipo de implementação.

- **DSA (Digital Signature Algorithm)**

Desenvolvido e adoptado como um Federal *Information processing Standard* (FIPS) pelo NIST. Usa somente chaves entre 512 e 1024 bits. DSA pode ser usado apenas para assinaturas digitais.

3.7 Pretty Good Privacy (PGP)

PGP é um programa desenvolvido por Phil R. Zimmermann que permite a comunicação de forma segura em um canal inseguro. Usando PGP pode-se facilmente e seguramente proteger a privacidade de dados encriptando-os para que apenas indivíduos desejados possam lê-la.

PGP é baseado na criptografia por chave pública: duas chaves complementares, chamadas de *par de chaves*, são usadas para manter a segurança das comunicações. Uma das chaves é criada como *chave privada* que apenas quem a cria tem acesso e a outra é a

chave pública que se pode distribuir livremente para outros usuários do PGP. As chaves (pública e privada) são armazenadas em um *arquivos-chaveiro* (keyring files).

Antes de começar a usar o PGP, você precisa gerar seu par de chaves. Depois de criar um par de chaves, você pode começar a se corresponder com outros usuários do PGP. Você precisará de uma cópia da chave pública deles e eles da sua. A chave pública é apenas um bloco de texto, por isso é tão fácil de trocar chaves com alguém. Algumas técnicas padrão permitem que você inclua sua chave pública em uma mensagem de e-mail, copiando ela para um arquivo, ou fixando ela num servidor público ou corporativo de chaves onde qualquer um pode ter uma cópia quando for necessário. Depois de você ter gerado suas chaves e trocado chaves públicas, você pode começar a criptografar e assinar e-mails e arquivos.

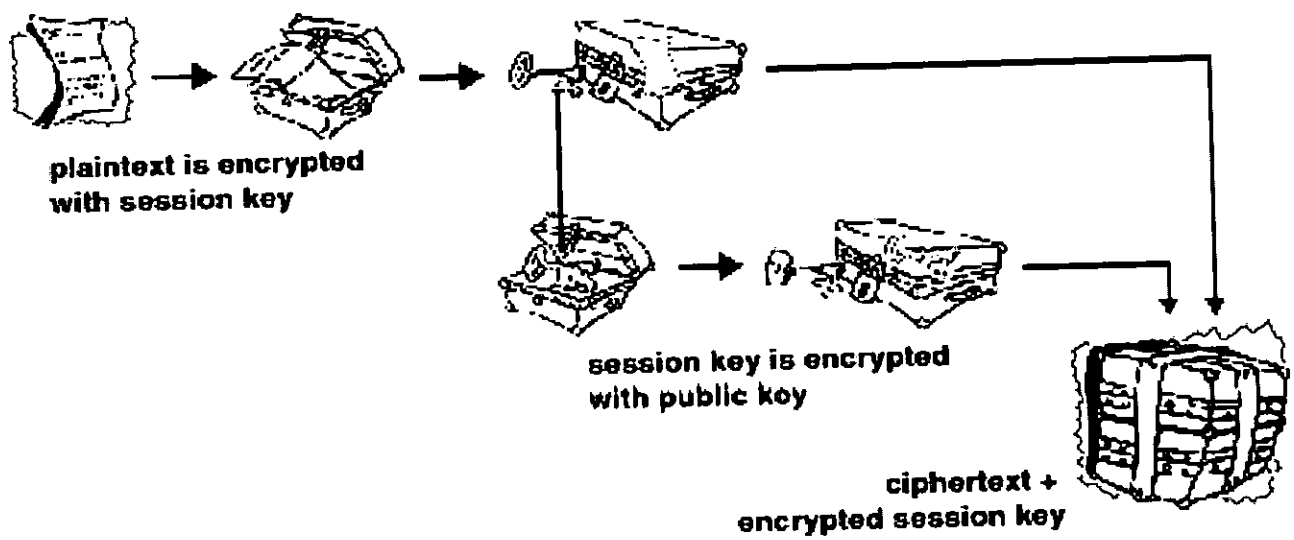

Figure 4 Encriptação em PGP

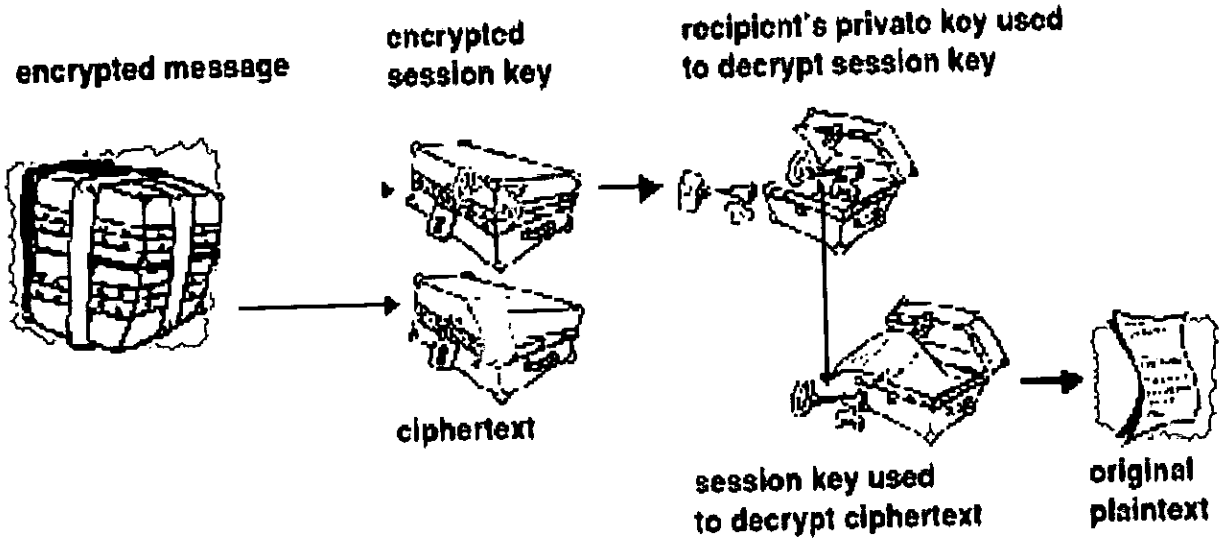

Figure 5 Decriptação em PGP

3.8 Chaves

Uma chave é um valor que funciona com o algoritmo criptográfico para produzir um texto encriptado.

Chaves são na prática números muito grandes.

O tamanho das chaves é medido em bits. Uma chave com 1024 bits é muito grande. Em criptografia de chave publica quanto maior for a chave, maior é a segurança do texto encriptado.

Contudo os tamanhos das chaves usadas na criptografia convencional e das chaves na criptografia de chave pública não tem relação nenhuma uma com a outra.

Por exemplo uma chave com tamanho de 80 bits na criptografia convencional tem a segurança equivalente a uma chave de 1024 bits na criptografia de chave pública. 128 bits seria equivalente a 3000 bits.

Isto se deve ao facto de que os algoritmos usados são bastante diferentes.

As chaves públicas e privadas estão matematicamente relacionadas.

Mas para uma chave bem grande deduzir a privada a partir da pública requer capacidade de computação não convencional.

3.9 Assinaturas Digitais

A assinatura é algo pessoal, é uma notação única que indica a aprovação ou autoria de um documento As assinaturas digitais têm vindo a assumir uma importância cada vez maior no comércio electrónico. Isto deve-se ao facto de estas criarem a presunção de que quem apôs a assinatura digital é o seu titular, como sucede com as assinaturas em documento escrito, assim como de oferecerem a vantagem de garantir que o documento electrónico não sofreu qualquer alteração desde o momento em que foi assinado digitalmente (garantem a sua integridade).

As assinaturas digitais, na realidade, não só igualam, como superam as assinaturas manuais. Ao contrário destas últimas, uma assinatura digital é praticamente impossível de falsificar. Uma assinatura digital é dinâmica por natureza, única para cada mensagem assinada. A informação na mensagem enviada, mais a chave privada que o emissor necessita para encriptar a mensagem, é parte integrante da assinatura digital e única devido aos complexos algoritmos matemáticos utilizados. Qualquer tentativa de intercepção e alteração da mensagem original, por um hacker, irá levar invariavelmente a uma falha no momento da verificação da assinatura inicial (Klander, 1997).

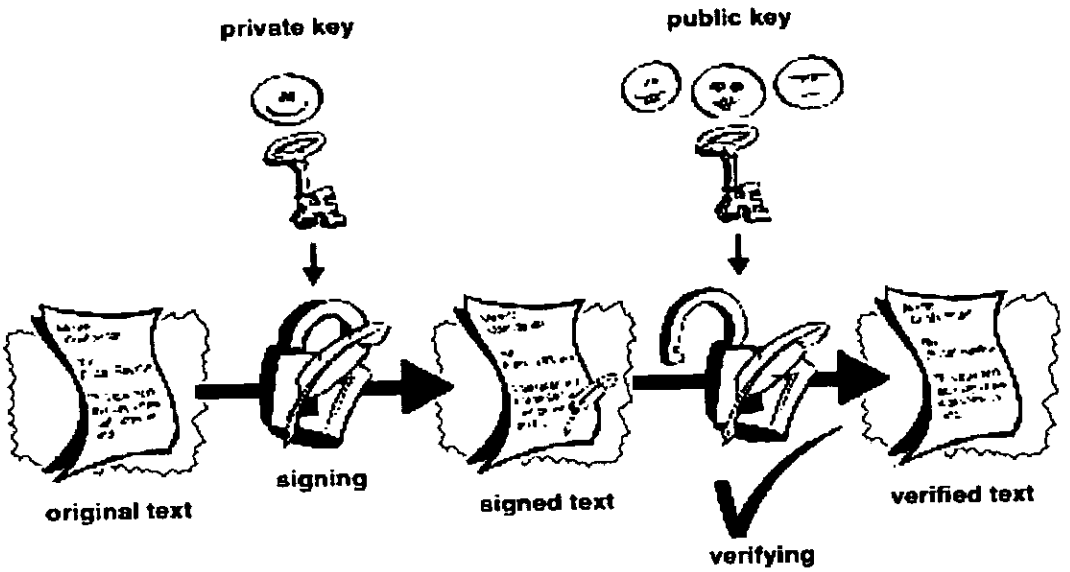

Figure 6 Assinatura digital

3.10 Funções Hash

Suponha que a Alice queira enviar uma mensagem assinada para o Bruno. Ela cria um *message digest* (resumo da mensagem) utilizando uma função *hash* (função matemática de criptografia) na mensagem. O *message digest* serve como uma "impressão digital" da mensagem; se qualquer parte da mensagem for modificada, a função *hash* retorna um valor diferente. A Alice então criptografa o *message digest* com sua chave privativa. Essa mensagem criptografada é a assinatura digital para a mensagem.

Alice envia a mensagem e a assinatura digital para o Bruno. Quando o Bruno os recebe, ele os decriptografa utilizando a chave pública de Alice, revelando o *message digest*. Para verificar a mensagem, ele então *hash* a mensagem com a mesma função *hash* Alice usou e compara o resultado com o *message digest* recebido de Alice. Se eles foram exactamente iguais, Bruno pode confiar que a mensagem tenha de fato vindo da Alice e que não mudou desde que ela a assinou. Se os *message digests* não foram iguais, ou a mensagem originou-se em outro lugar ou foi alterada depois de assinada.

Note que usar assinaturas digitais não criptografa as mensagens. Se a Alice quiser garantir a privacidade da mensagem, ela terá de criptografá-la usando a chave pública do Bruno. Então somente o Bruno poderá ler a mensagem decriptografando-a com sua chave privada.

Não é praticável que qualquer um encontre uma mensagem que *hash* a um dado valor ou encontrar duas mensagens que *hash* no mesmo valor. Se fosse praticável, um intruso poderia anexar uma mensagem falsa à assinatura da Alice. Funções *hash* específicas foram criadas para terem a propriedade de ser impossível encontrar valores coincidentes, logo são consideradas apropriadas para usar em criptografia.

Um ou mais Certificados digitais podem acompanhar uma assinatura digital. Se um Certificado digital está presente, o destinatário (ou uma terceira pessoa) pode verificar a autenticidade da chave pública.

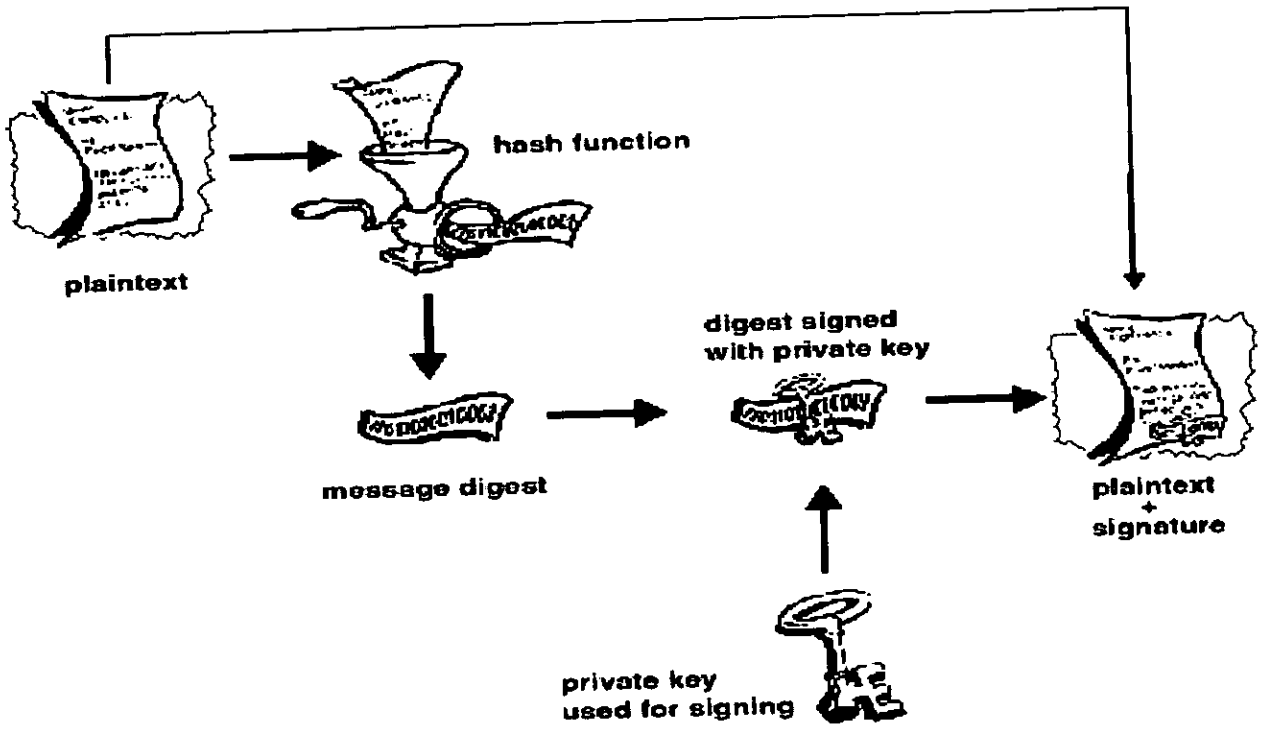

Figure 7 Secure Digital Signatures

3.11 Certificado Digital

Certificados digitais são ficheiros electrónicos que actuam como um passaporte electrónico. Eles são emitidos por uma autoridade certificadora na qual se pode confiar, e esta verifica a identidade do detentor do certificado. Eles não podem ser subvertidos ou forjados.

Um certificado digital é uma informação que é incluída com a chave pública que permite os outros certificarem que uma chave é genuína e válida.

São usados para impedir que alguém tente personificar uma outra pessoa.

Basicamente é uma chave pública com uma ou duas identidades Anexas, mais um selo de aprovação de alguém a quem se pode confiar.

Os Certificados Digitais autenticam que os seus detentores – pessoas, *websites*, e mesmo recursos de redes tais como routeadores – são verdadeiramente aquilo que eles alegam ser e protegem os dados trocados electronicamente contra roubo e subversão.

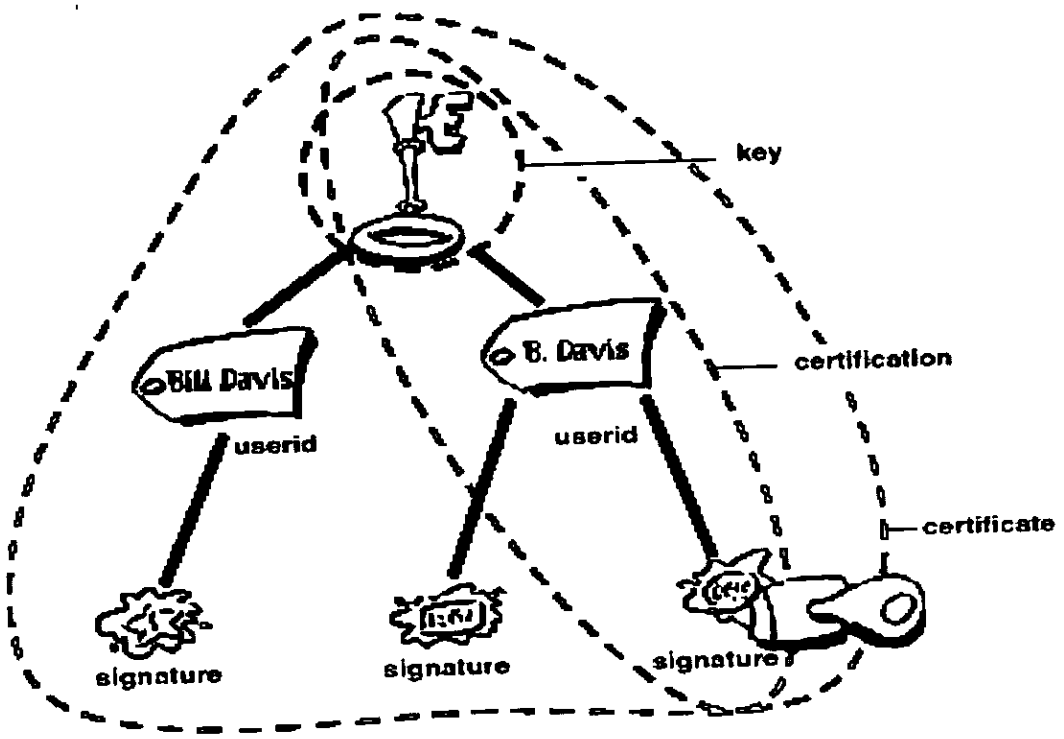

Figure 8 Anatomy of a PGP Certificate

3.12 Tipos de Certificados

3.12.1 Certificados de servidores

Permitem que visitantes do seu *website* possam trocar informação pessoal, como cartões de credito, livres do risco dessa informação ser subvertida ou interceptada.

Permite também que os visitantes possam autenticar a sua identidade

3.12.2 *Certificados pessoais*

Permitem autenticar a identidade do visitante e restringir o acesso a um especifico conteúdo para um visitante particular.

Podem ser usadas para mandar correio electrónico seguro para informação privada.

Estes certificados são perfeitos para comunicações b2b, tais como dar a possibilidade de seus parceiros poderem actualizar partes especificas da sua Internet mas negar tal possibilidade para todos os outros.

3.13 Distribuição de Certificados

- **Servidores de certificados**:

Permitem guardar informação sobre certificados

- **Public-key infrastructure (PKI)**

PKI faz a integração de certificados digitais, criptografia que usa chaves publicas, e entidades de certificação, criando uma arquitectura de segurança total para uma empresa Um PKI típico para um empresa envolve a emissão de certificados digitais para servidores e utilizadores, software para utilizadores, integração com directórios de certificados da empresa, ferramentas de gestão, renovação e revogação de certificados, e outros serviços de suporte.

4 PROBLEMAS NA TRANSMISSÃO DA INFORMAÇÃO ATRAVÉS DO RADIO CANAL E METODOLOGIA DE INVESTIGAÇÃO

As questões da segurança da informação quando transmitida num Radio Canal sempre surgem quando se pretende garantir a protecção contra ameaças de acesso ilegal. É neste contexto que um Radio Canal deve incluir várias tecnologias de protecção que deve ter em conta o seguinte:

- usar a criptografia como um dos processos seguros para transformar a informação a ser transmitida;
- tornar difícil o processo da criptanálise;
- as ondas electromagnéticas que podem provocar alteração da informação quando surge interferência com outras ondas.

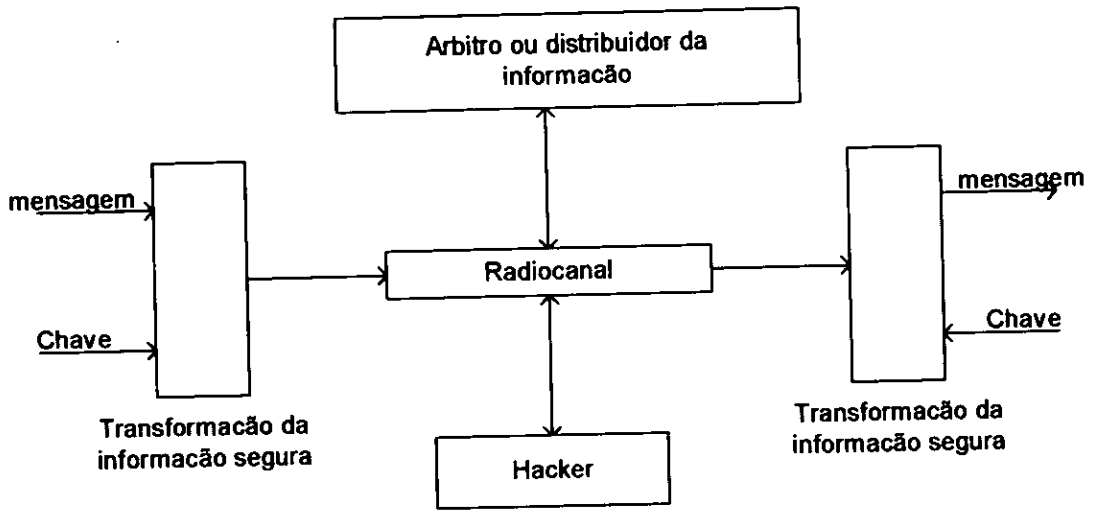

Figure 9 Problemas na transmissão da informação num Rádio Canal

A actividade que acompanhou o processo de pesquisa foi essencialmente a consulta bibliográfica (incluindo Internet); participação em palestras no DMI e na Faculdade de ciências; troca de impressões com especialistas na área de segurança de informação.

5 ENQUADRAMENTO DO TRABALHO

Todas as tentativas de acesso ilegal na transmissão da informação através de um radio canal podem-se classificar da seguinte maneira:

- Acesso ilegal passivo;
- Acesso ilegal activo.

O acesso ilegal passivo consiste na recepção da informação. Neste caso podemos encontrar duas hipóteses; a primeira consiste na leitura da informação, e a segunda no processo de análise da informação recebida.

O processo da determinação do acesso ilegal passivo é complicado, porque o receptor da informação não pode verificar uma alteração na informação depois da sua transmissão. **Por isso o presente trabalho tem como primeiro objectivo a protecção da informação contra o acesso ilegal**.

O acesso ilegal activo tem como objectivo a alteração da informação. É bem sabido que o processo de transmissão da informação através de um radio canal tem suas vantagens :

- O preço é relativamente baixo.

A desvantagens que limita o uso são as frequências que as vezes dependem das condições atmosféricas, ou seja as interferências das ondas podem provocar o surgimento de erros, que por seu turno realizam acesso ilegal activo.

Assim sendo o presente trabalho tem como segundo objectivo a criação de um critério que permitira determinar o acesso ilegal activo.

As seguintes figuras ilustram os diferentes tipos de ameaças que podem acorrer na transmissão da informação digital através de um Radio Canal:

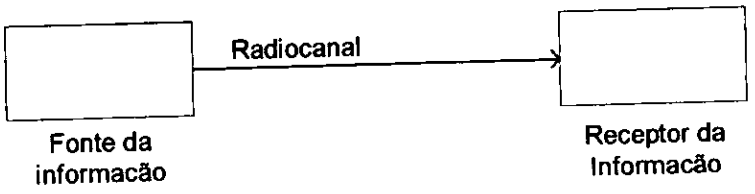

Figure 10 Situação Normal

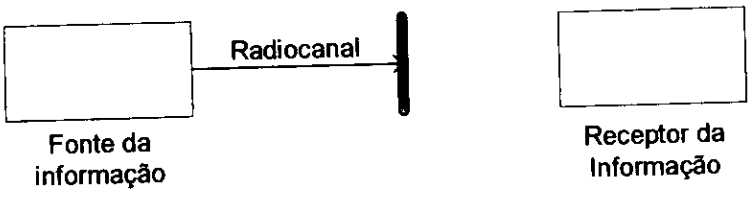

Figure 11 Interrupção da Informação

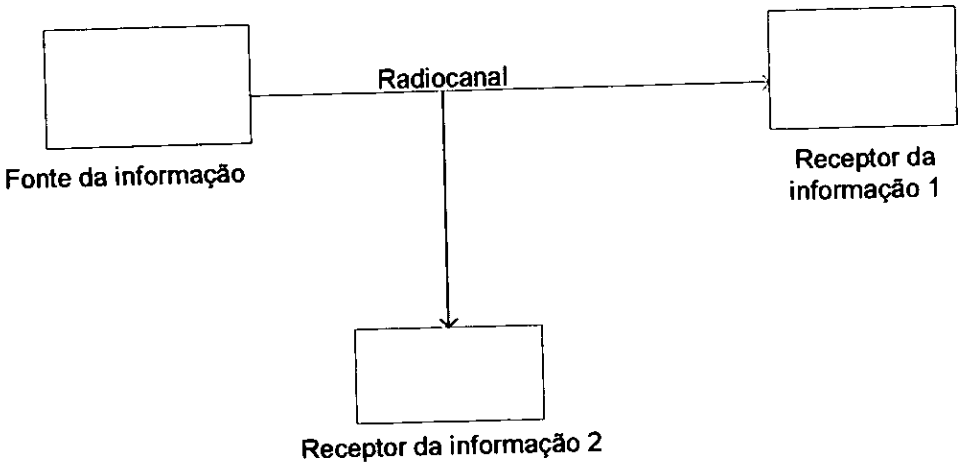

Figure 12 Acesso Ilegal Passivo

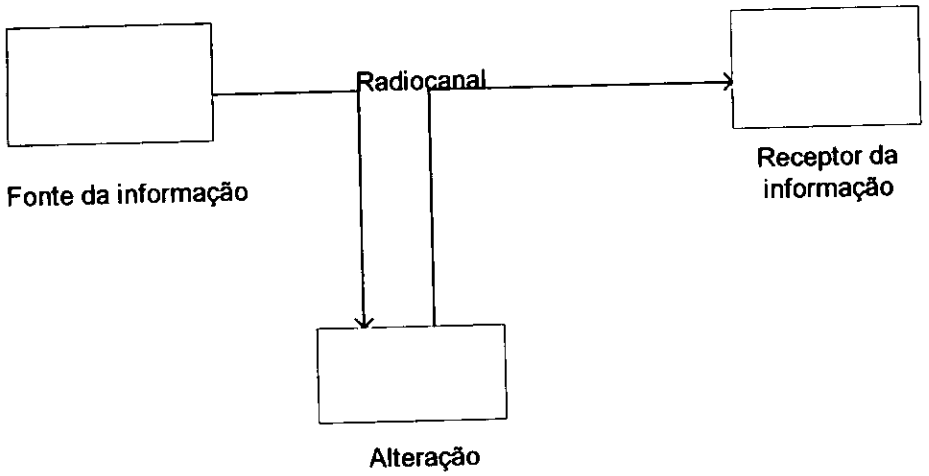

Figure 13 Acesso Ilegal Activo

6 O USO DE CÓDIGOS COM BASE IRRACIONAL

6.1 Secção Dourada, Números de Fibonacci e de Lucas

A secção dourada surge da divisão do segmento de linha AB com o ponto C no extremo e como rácio médio (Fig 14), isto é,

$$\frac{AB}{CB} = \frac{CB}{AC} \tag{10}$$

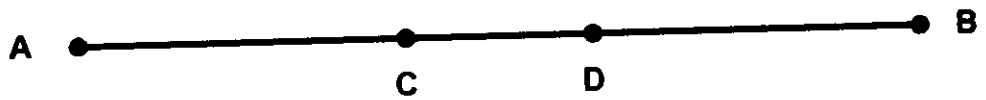

Figure 14 Secção dourada

Isto pode ser reduzido à equação

$$x^2 = x + 1 \tag{11}$$

A raiz positiva da equação $\tau = \frac{1+\sqrt{5}}{2} \approx 1{,}618$

é chamada de "rácio dourado "e a divisão do segmento de linha no rácio de (10) é chamada de "secção dourada".

Sendo a raiz da equação (11), o rácio dourado possui a seguinte propriedade maravilhosa:

$$\tau^n = \tau^{n-1} + \tau^{n-2} \tag{12}$$

onde n é número inteiro ($n = 0,\pm1,\pm2,\pm3,....$)

o rácio dourado está profundamente ligado aos números de Fibonacci e números de Lucas. O matemático italiano do século 13 Fibonacci descobriu a primeira fórmula recorrente na história da matemática.

$$G(n) = G(n-1) + G(n-2) \tag{13}$$

para diferentes condições iniciais, a fórmula (13) gera duas sequências bem conhecidas. A anterior são os *Números de Fibonacci F(n):*

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,....

dados pela fórmula recorrente

$$F(n) = F(n-1) + F(n-2)$$

para as condições iniciais $F(1)=F(2)=1$.

A posterior são os Números de Lucas L(n):

1, 3, 4, 7, 11, 18, 29, 47, 76, 142,....

para as condições iniciais $L(1)=L(2)=3$.

É necessário enfatizar que através desta descoberta Fibonacci antecipou o método de relações de recorrência, o qual foi considerado como o mais apropriado para resolver problemas combinatórias.

As sequências $F(n)$ e $L(n)$ expandidas para o lado de valores discretos de n no intervalo $-\infty$ a $+\infty$ são dados na Tabela 2

Table 2 Expansão das sequências de Lucas e de Fibonacci, para o lado dos valores discretos

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55
F_{-n}	0	1	-1	2	-3	5	-8	13	-21	34	-55
L_n	2	1	3	4	7	11	18	29	47	76	123
L_{-n}	2	-1	3	-4	7	-11	18	-29	47	-76	123

Os termos das sequências $F(n)$ e $L(n)$ possuem algumas propriedades matemáticas maravilhosas. Por exemplo, para os números ímpares $n=2k+1$, os termos das sequências $F(n)$ e $F(-n)$ coincidem, i.e., $F(2k+1)=F(-2k-1)$, e para números pares $n=2k$ elas são expressas como $F(2k)=-F(-2k)$. Em relação aos números de Lucas $L(n)$, isto é ao contrário, i.e., $L(2k)=L(-2k)$; $L(2k+1)=-L(-2k-1)$.

É fácil determinar que $L(n)$ e $F(n)$ estão ligados pelas seguintes relações:

$$L(n)=F(n-1)+F(n+1);$$

$$L(n)=F(n)+2F(n-1);$$

$$L(n)+F(n)=2F(n+1).$$

A ligação entre os números de Fibonacci e Lucas e o rácio dourado é expressa por fórmulas bem conhecidas, as chamadas *Formulas de Binet* (Hoggat,1969; Vorobev, 1978; Vaida, 1989) citado por (Petrossiuk e Stakhov, 1999). Para obtermos as fórmulas de Binet, consideremos a expressão (3) ligando as potências do rácio dourado. Se tivermos:

$$\tau^0 = 1,\ \tau^1 = \frac{1+\sqrt{5}}{2}, \text{ and } \tau^{-1} = \frac{-1+\sqrt{5}}{2}$$

E adiante definirmos as potências da secção dourada pela fórmula (12), obteremos as seguintes expressões:

$$\tau^2 = \tau^1 + \tau^0 = \frac{3+\sqrt{5}}{2};$$

$$\tau^3 = \tau^2 + \tau^1 = \frac{4+2\sqrt{5}}{2};$$

$$\tau^4 = \tau^3 + \tau^2 = \frac{7+3\sqrt{5}}{2}.$$

Como resultado, é fácil obter a fórmula geral, o que permite exprimir qualquer potência do rácio dourado na forma

$$\tau^n = \frac{L(n)+F(n)\sqrt{5}}{2} \tag{13}$$

onde $L(n)$ e $F(n)$ são números de Fibonacci e Lucas. Isto implica as fórmulas de Binet:

$$L(n) = \begin{cases} \tau^n + \tau^{-n} \\ \tau^n - \tau^{-n} \end{cases} \tag{14}$$

$$F(n) = \begin{cases} \dfrac{\tau^n + \tau^{-n}}{\sqrt{5}} \\ \dfrac{\tau^n - \tau^{-n}}{\sqrt{5}} \end{cases} \tag{15}$$

Porque é que as fórmulas de Binet são tão pouco usuais? O facto é que $L(n)$ e $F(n)$ são números inteiros conforme segue da tabela 2, enquanto que τ^n e τ^{-n} são números irracionais. Assim, as fórmulas de Binet ligam tanto números integrais como irracionais.

Neste capítulo descrevemos lemas e teoremas que permitirão facilitar e sistematizar esta investigação. Um grupo de α – códigos é semelhante ao código binário e pertence ao grupo de códigos posicionais, a única diferença é que a base destes códigos é um número irracional.

Para sistema binário;

$$ND = \sum_{i=\_\infty}^{+\infty} a_i \cdot 2^i \tag{16}$$

onde ai ∈ { 0,1}; i =[-∞ , +∞]

E para sistema de cálculo com base irracional,

$$ND = \sum_{i=\_\infty}^{+\infty} \alpha_i a^i \tag{17}$$

onde a_i é valor lógico que pertence ao conjunto de um bit; α_1 – a base irracional do sistema de cálculo.

Baseando na fórmula (17) estes códigos receberam o nome de códigos com base irracional (18). Consideremos os lemas que são a plataforma para a nossa posterior análise.

Lema 1. Sistema de cálculo de base 2 é um sistema que tem só uma única correspondência entre o número decimal e a combinação codificada e não permite excesso de codificação.

Lema 2. Qualquer número irracional que tem um valor dentro do intervalo de números [1..2] já pode ser considerado como uma base de cálculo.

Lema 3. Qualquer combinação codificada como código com base irracional possibilita codificar os números decimais contendo pelo menos mais uma combinação codificada que codifica o mesmo número decimal.

Lema 4. A quantidade destas múltiplas representações de um número decimal depende do valor da base do sistema de cálculo com base irracional.

Lema 5. Nos códigos com múltiplas representações entre todas as formas existentes funciona a correspondência rigorosa.

Teorema 1. A probabilidade de encontrar um código binário de n algarismos com dois ou mais unidades, calcula-se pela fórmula

$$P = \frac{C_n}{2^n} = \frac{C_{n-2} + C_{n-1} + 2^{n-2}}{2^n} \qquad (18)$$

Onde C_n denomina o número de códigos de n algarismos com duas ou mais unidades juntas.

Prova. A fórmula foi obtida a partir da definição da probabilidade como uma relação entre o número dos casos elementares que favorecem ao acontecimento e o número de todos os casos elementares possíveis. Por isso, basta demonstrar que

$$C_n = C_{n-2} + C_{n-1} + 2^{n-2} \qquad (19)$$

Usando o método da indução matemática e verificamos a fórmula para o caso n = 3

n = 1, códigos possíveis são 0 ou 1, então C1 = 0;

n = 2, códigos possíveis são: 00, 01, 10, 11, 1 então C2.

n = 3, códigos possíveis são: 000, 001, 010, 011, 100, 101, 110, 111, 1, então C3.

A fórmula (17) dá o mesmo valor $C_3 = C_2 + C_1 + 2^{3-2} = 1 + 0 + 2 = 3$

Suponhamos agora que a fórmula (19) é válida para n = k e mostremos que neste caso ela será válida par n = k +1, o que vai concluir a prova.

$$C_{k-1} = C_k + 2^{k-1} + C_{k-1}$$

Se rescrevermos a última fórmula como

$$C_{k+1} = C_k + C_{k-1} + 2^{(k-1)-2}$$

vemos, que a fórmula (17) é válida para qualquer que seja n.

Suponhamos que em qualquer combinação codificada no código binário não existe pelo menos dois uns vizinhos.

Neste caso, devemos usar a fórmula (19) que determina a quantidade destas combinações codificadas C_n. E agora é muito fácil a partir da fórmula (20) que o resultado neste caso dá-nos os números de FIBONACCI.

$$F_p = 2^n - C_n \tag{20}$$

Table 3 Números de Fibonacci

n	3	4	5	6	7	8	9	10	11
C_n	3	8	19	43	94	201	423	880	1815
F_p	5	8	13	21	34	55	89	144	233

6.2 Base Irracional

Para criar qualquer código no sistema de cálculo com base irracional, primeiramente será necessário obter um mecanismo que determine esta base. Por isso, neste caso usaremos o polinómio principal (21)

$$X_n = a_{i-1}X^{n-1} + a_{i-2}X^{n-2} + \ldots + a_1X + 1 \quad , \tag{21}$$

onde $a_i \in \{0,1\}$, n = { 1,2,3,... } e I = {1,2,3,...}. Variando a_i, n e I obtém-se vários grupos de polinómios parciais. Considere-se, a título de exemplo, o caso em que $a_i = 1$ e o valor n varia de 1 a n. Os polinómios parciais formados seriam:

$$\begin{aligned} x &= 1 && p = 1 \\ x^2 &= x+1 && p = 1.618 \\ x^3 &= x^2 + x + 1 && p = 1.8393 \end{aligned} \tag{22}$$

.....

$x^n = x^{n-1} + x^{n-2} + \ldots + x + 1$ p = 1.9999

A raiz positiva e maior que 1 fornece-nos a base do sistema. Os polinómios parciais em (22) permitem obter bases, exceptuando o caso p = 1, no intervalo p = [1.618....1.999], isto é abrange um código com uma base muito conhecida – a **"proporção de ouro"** e finalmente o sistema binário.

Se tomarmos em consideração, por exemplo, a base **1.6180334**.. do segundo polinómio parcial em (22), o número 13.7081 na base irracional 1.6180334... seria:

Table 4 Determinação de um número numa dada base irracional

ND	11.0901	6.854095	4.236065	2.6180334	1.6180334	0.6180334
K	1	0	0	1	0	0

Onde k = 13.7081

Além disso será possível obter outras bases de α – códigos se $a_i \in \{0,1\}$. A tabela seguinte ilustra os polinómios parciais que dão-nos as bases correspondentes.

Table 5 Polinómios parciais e bases irracionais correspondentes

N	Equações	Raízes
N=1	$x = 1$	1
N=2	$x^2 = x + 1$	1.6180334
N=3	$x^3 = x^2 + x + 1$	1.83929
	$x^3 = x + 1$	1.32472
	$x^3 = x^2 + 1$	1.46557
N=4	$x^4 = x^3 + x^2 + x + 1$	1.92756
	$x^4 = x^3 + x^2 + 1$	1.75488
	$x^4 = x^3 + x + 1$	1.61803
	$x^4 = x^2 + x + 1$	1.46557
	$x^4 = x^2 + 1$	1.27202
	$x^5 = x^4 + x^3 + x^2 + x + 1$	1.96595

N=5	$x^5 = x^4 + x^3 + x^2 + 1$	1.88852
	$x^5 = x^4 + x^3 + x + 1$	1.81240
	$x^5 = x^4 + x^2 + x + 1$	1.68514
	$x^5 = x^3 + x^2 + x + 1$	1.53416
	$x^5 = x^2 + x + 1$	1.32472
	$x^5 = x + 1$	1.16730
N=6	$x^6 = x^5 + x^4 + x^3 + x^2 + x + 1$	1.98358
	$x^6 = x^5 + x^4 + x^3 + x^2 + 1$	1.94789
	$x^6 = x^5 + x^4 + x + 1$	1.83929
	$x^6 = x^5 + x^4 + x^2 + 1$	1.78854
	$x^6 = x^5 + x^4 + x + 1$	1.74370
	$x^6 = x^5 + x^4 + 1$	1.67365
	$x^6 = x^5 + x^3 + x^2 + 1$	1.66041
	$x^6 = x^5 + x^3 + x + 1$	1.61803
	$x^6 = x^5 + x^3 + 1$	1.5385
	$x^6 = x^5 + 1$	1.2852
	$x^6 = x^4 + x^3 + x^2 + x + 1$	1.57015
	$x^6 = x^4 + x^3 + x^2 + 1$	1.51228
	$x^6 = x^4 + x^3 + x + 1$	1.48047
	$x^6 = x^4 + x^3 + 1$	1.4036
	$x^6 = x^4 + x^2 + x + 1$	1.43513
	$x^6 = x^4 + 1$	1.21061
	$x^6 = x^3 + x^2 + x + 1$	1.38028
	$x^6 = x^3 + x^2 + 1$	1.30408
	$x^6 = x^3 + x + 1$	1.27857
	$x^6 = x^3 + 1$	1.17399

6.3 Modelação de Surgimento de Erros

Nesta última parte será apresentado o resultado do processamento de um código irracional com base **1.6180334**. Analisaremos uma palavra de 12 bits que corresponde ao código binário de 8 bits. Neste programa temos dois geradores de números casuais:

- Primeiro determina número casual da combinação codificada;
- Segundo determina o número da posição do bit.

Praticamente, neste caso dois geradores determinam a localização do erro que deve ser introduzido.

Table 6 Modelação de surgimento de erros

0	0	0	0	0	0	0	0	1	0	0	0	1	5	0
0	0	0	0	0	0	0	1	1	1	0	1	2	11	9
0	0	0	0	0	0	1	0	0	1	0	1	3	15	10
0	0	0	0	0	1	0	0	0	1	0	0	4	18	10
0	0	0	0	0	1	0	0	0	0	0	1	5	19	12
0	0	0	0	0	1	0	0	1	0	1	0	6	24	11
0	0	0	0	1	0	0	1	1	0	0	0	7	34	8
1	0	0	1	0	0	0	1	0	0	0	0	8	54	1
0	1	0	1	0	0	1	0	0	1	0	0	9	61	2
0	0	0	1	0	1	0	0	0	1	0	1	10	69	12
0	0	1	0	0	0	0	0	0	1	1	1	11	80	11
0	0	1	0	0	0	1	1	0	0	0	1	12	84	7
0	0	1	0	0	0	0	1	0	1	0	1	13	86	12
0	1	1	0	0	0	0	1	0	1	0	1	14	87	2
0	0	1	0	0	0	1	0	1	0	0	1	15	92	12
0	0	1	0	0	1	0	0	0	0	1	0	16	94	11
0	1	1	0	0	1	0	0	1	0	1	0	17	100	2
0	0	1	0	1	0	0	0	1	0	0	0	18	106	9
0	0	1	0	1	0	0	0	1	1	0	0	19	110	10
0	1	0	0	0	0	0	1	0	1	0	1	20	131	10

0	1	0	0	0	1	0	0	0	0	0	1	21	142	6
0	1	0	0	0	1	0	0	0	1	0	1	22	145	6
0	1	0	0	1	0	1	0	0	1	0	0	23	166	2
0	1	0	1	0	0	0	0	0	1	0	1	24	174	4
0	1	0	1	0	0	0	0	1	0	0	0	25	175	2
1	1	0	1	0	0	1	0	1	0	1	0	26	187	1
0	1	0	1	0	1	0	1	1	0	0	0	27	193	8
0	1	0	1	0	1	0	1	0	0	0	1	28	195	12
0	1	1	1	0	1	0	1	0	0	1	0	29	197	3
1	0	0	0	1	0	0	0	0	1	0	0	30	202	5
1	0	1	0	0	0	0	1	0	0	1	0	31	208	3
1	0	0	1	0	0	1	0	0	1	0	1	32	214	4
1	0	0	0	1	0	0	0	0	1	0	1	33	232	5
1	0	0	1	1	0	1	0	1	0	1	0	34	245	4
1	0	0	1	1	0	0	0	0	0	1	0	35	248	5
1	0	0	1	0	0	0	0	0	0	1	0	36	248	1

Quantidade das combinações 36

Quantidade das combinações detectadas 12

Percentagem das combinações 33%

Como podemos ver entre 36 combinações, 12 são detectadas e neste caso a probabilidade dá-nos 33%.

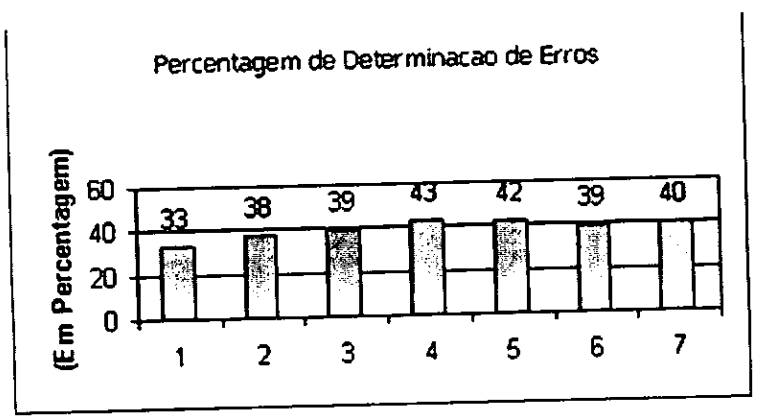

Figure 15 Percentagem de determinação de erros

7 TRANSMISSÃO DA INFORMAÇÃO ATRAVÉS DA RADIO CANAL USANDO CÓDIGOS POSICIONAIS

Com o desenvolvimento da Informática surgiu principalmente uma nova possibilidade que permitiu realizar uma rápida comunicação entre computadores e sistemas digitais. Hoje em dia é possível usar as redes dos computadores locais e gerais que realizam as transmissões das informações digitais

Como meios de comunicação podem servir linhas telefónicas, cabos ópticos e outros equipamentos radioelectrônicos e sem qualquer dúvida a transmissão das informações digitais no futuro próximo desempenhará também o papel extremamente importante, porque a tendência actual mostra que na maioria dos casos é possível encontrar mais frequentemente a transmissão da informação digital. Quer dizer, o uso da transmissão analógico em relação a transmissão digital tem grandes inconvenientes que diminuem em geral a rentabilidade de qualquer sistema informático.

Por isso, usa-se actualmente e será usado também a transmissão digital da informação (TDI).

Na fase da TDI está o principio da codificação usando códigos binários.

De facto este pormenor reflecte o uso dos códigos binários nos computadores digitais para transmitir a informação existem dois modos principais tais como; assincrónicos e sincrónicos. Como mostra a teoria e a prática é mais preferível utilizar o último modo porque neste caso aumenta-se a velocidade de transmissão.

Ë sabido que a fonte de transmissão deve formar na sua saída de transmissão o conjunto das combinações codificadas que formam realmente uma matriz das combinações codificadas, por exemplo:

$$M_i = \begin{Bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{Bmatrix}$$

Matriz inicial de combinações codificadas (I)

Essa Matriz Inicial através de uma linha de transmissão deve ser transmitida linha por linha até o seu receptor.

|...|11110011 |1110010 |11110001 |

N 3 2 1

Tempo ⟶

Mas neste caso surgem duas perguntas muito importantes:

- **Como é possível transmitir informação sem erros;**
- **Como é possível proteger a informação contra acesso ilegal sem erros.**

Para resolver positivamente estes problemas na teoria de codificação das informações usam-se sistemas de cálculos não posicionais (SPN) que utilizam por exemplo os códigos tais como; Código de Johnson, Código de Haming e outros. Como mostra essa teoria eles dão-nos maior efeito na determinação dos erros. Mas na vida real de TDI tem que assegurar simultanêamente a solução de dois problemas, isto é determinação dos erros e protecção da informação. Este aspecto torna-se mais dificil, porque devem ser elaborados outros métodos de codificação e transmissão da informação usando meios de comunicação idênticos.

Neste capítulo considera-se um novo método que permite resolver simultanêamente este dois problemas e baseia-se na utilização dos códigos com base irracional. Como podemos ver posteriormente surge uma nova vantagem que se baseia no uso de códigos posicionais.

7.1 Estrutura Típica na Transmissão da Informação

É bem sabido que a transmissão é uma acção de transmitir analógica, na qual os sinais variam de uma forma continua entre dois estados duma grandeza fisica. Transmissão digital, na qual os dados são transmitidos sucessivamente, não podendo cada um deles tomar um número finito de valores descontínuos. Frequentemente, são utilizados sinais binários, cada dado é então, codificado previamente em binário. Os métodos e dispositivos fundamentais da radioelectrónica se for necessário explicar da forma mais simples estão representados na fig. 16 e na fig. 17 onde F1....Fn são frequências diferentes.

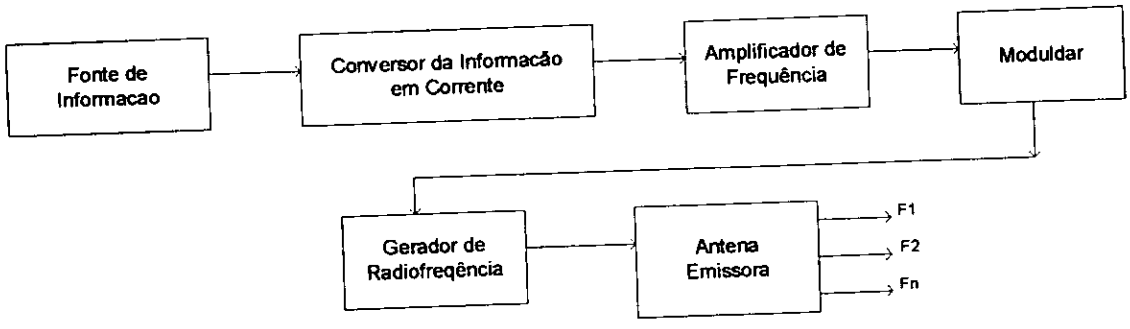

Figure 16 Esquema de blocos de um dispositivo de Radiotransmissão

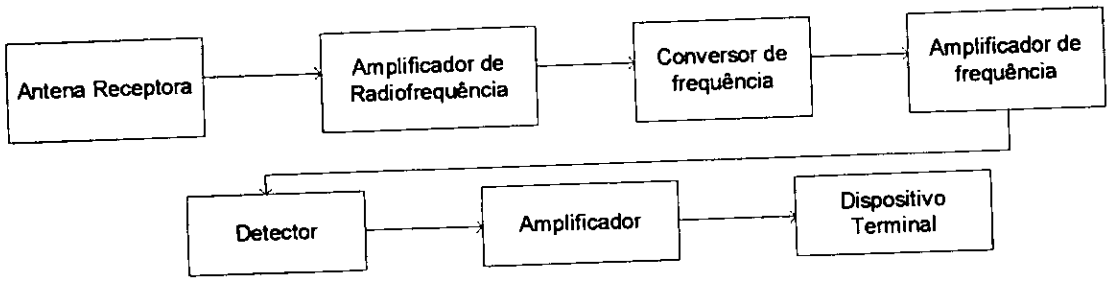

Figure 17 Esquema de blocos de um dispositivo de Radiorecepção

É evidente que a qualidade de transmissão primeiramente depende da potência de transmissão. Mas, com o aumento da distância e nas condições extremas de recepção diminui-se consideravelmente a veracidade de transmissão da informação. Por outro lado a informação que se transmite deve ser bem protegida contra ilegal acesso.

Neste caso é necessário usar os códigos especiais que permitem simultanêamente determinar os erros na sua transmissão e proteger o conteúdo desta informação.
Usam-se actualmente sistemas de cálculo não posicionais. O seu uso dá sob vários pontos de vista dificuldades como por exemplo; codificação e descodificação da informação porque os dispositivos correspondentes são complicados e os sistemas em geral são caros.

7.2 Uso dos Códigos Posicionais com Base Irracional

Qualquer tipo de mensagem que deve ser transmitida pode ser representada no sistema binário como uma matriz (I) que contém N-linhas. Cada linha neste caso representa um vector binário que codifica um caracter desta mensagem. Mas podemos usar também os códigos irracionais que dão-nos a mesma possibilidade na transmissão da informação digital. Por isso, pode-se representar a matriz (I) como:

$$F_i = \|M_p\| \tag{23}$$

Onde p = parâmetro de código irracional e F_i = mensagem codificada no código com base irracional.

Como no sistema binário podemos também transmitir a mensagem codificada no código com base irracional pode ser efectuada analogamente para proteger a nossa informação.

$$F_i = \|\overline{M_p}\| \tag{24}$$

onde M_p é vector binário invertido no código com base irracional.

Além disto, como no sistema binário é possível transmitir essa matriz directamente e vice-versa.

Por isso obteremos:

$$F_i = \|\underline{M_p}\| \tag{25}$$

Onde $\underline{M_p}$ é um vector transmitido e vice-versa

$$F_i = \|M_p\| \tag{26}$$

Onde $\overline{M_p}$ - é um vector invertido na transmissão e vice-versa.

Quatro matrizes dados estabelecem o nível de protecção da informação que pode ser transmitida através da radio canal. Mas para aumentar este nível de protecção num sistema de transmissão analógico, transmissores e receptores mudam sincronicamente a frequência de trabalho. Realmente usam-se no máximo três frequências F1, F2, F3. o aumento da quantidade de frequências torna a parte de Hardware extremamente complicada. Por isso, quatro matrizes e três frequências diferentes permitem garantir máxima protecção possível da informação. Mas, sob ponto de vista da parte técnica o processo de sincronização das alterações das frequências na maioria dos casos torna-se impossível porque existem vários pormenores, como por exemplo interferências que dificulta a recepção da informação. O uso de uma única frequência garante a transmissão mais diminui consideravelmente o nível de protecção N, porque deve ter só as variáveis I,D (Petrosiuk; Stakhov; Sotomane, 1996).

$$N \in \{I,D,F\} \tag{27}$$

onde:

I é forma da matriz inicial (normalmente invertida);

D é direcção de transmissão (directa, indirecta);

F é o conjunto das frequências.

Mas é bem sabido que códigos com base irracional podem ter vários parâmetros p=1; p=2; p=3 que formam os códigos posicionais, por isso podemos escrever a fórmula (27) em conformidade com P.

$$N \in \{I,D,P\} \tag{28}$$

onde P é parâmetro do código com base irracional.

A figura 18 ilustra o sistema de transmissão da informação digital.

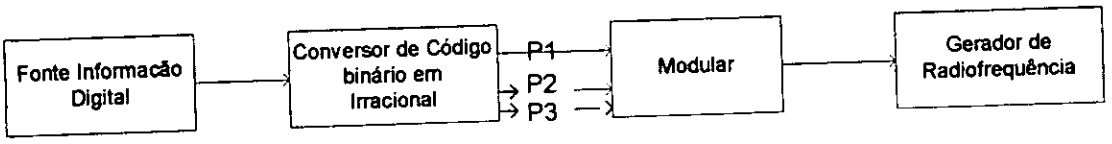

Figure 18 Esquema de Radiotransmissor

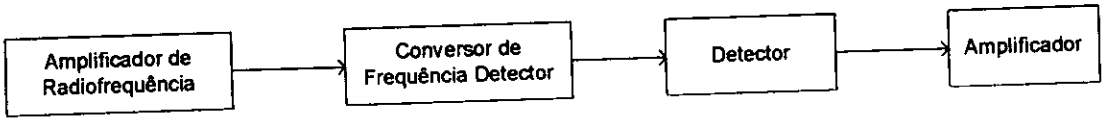

Figure 19 Esquema de um Radioreceptor

Como podemos ver na figura 19 temos um novo bloco que é dispositivo do controlo da forma mínima.

O seu uso aumenta as possibilidades funcionais deste sistema de transmissão/radiorecepção: se durante a transmissão da informação através da radio canal surgirem erros isso obrigatoriamente vai provocar alterações na forma mínima pelo menos de um vector binário.

Mas de acordo com regras da forma mínima pode-se facilmente ser determinado este erro e como resultado desta situação errada obteremos na saída lógica que nos informará sobre transmissão errada.

8 CÓDIGOS DE REFLEXÃO IRRACIONAL

Este capítulo contém um método que se baseia na utilização dos códigos não posicionais que permitem além de criptografar/decriptografar, determinar e corrigir os erros durante a transmissão da informação digital através da radio canal.

Na Teoria moderna de codificação da informação, o uso deste método permitirá garantir alta protecção contra "hacker" e mais alta veracidade da informação.

A teoria de codificação usa vários métodos para apresentar a informação numérica e alfanumérica. A evolução histórica desta teoria de codificação tem um longo caminho e podemos encontrar actualmente muitas publicações e resultados que são êxitos muito importantes na informática.

Sabe-se também que o uso de um sistema de numeração é uma plataforma na elaboração e construção da parte fisica de um computador de um computador digital ou uma base, por exemplo; na transmissão da informação entre ponto de destino e origem. Todos os resultados obtidos na teoria de codificação, e quantidade destes resultados testemunham a importância deste problema, mas por outro lado ver q não existe infelizmente um sistema de numeração que permite satisfazer todas as necessidades existentes na vida real (Petrossuik; Mannestig, 2003).

Três momentos básicos que devem ser resolvidos estão relacionados com os problemas seguintes:

- Processamento da informação sem erros;
- Transmissão da informação sem erros;
- Protecção da informação contra o acesso ilegal.

A figura a baixo permite classificar sistemas de numeração.

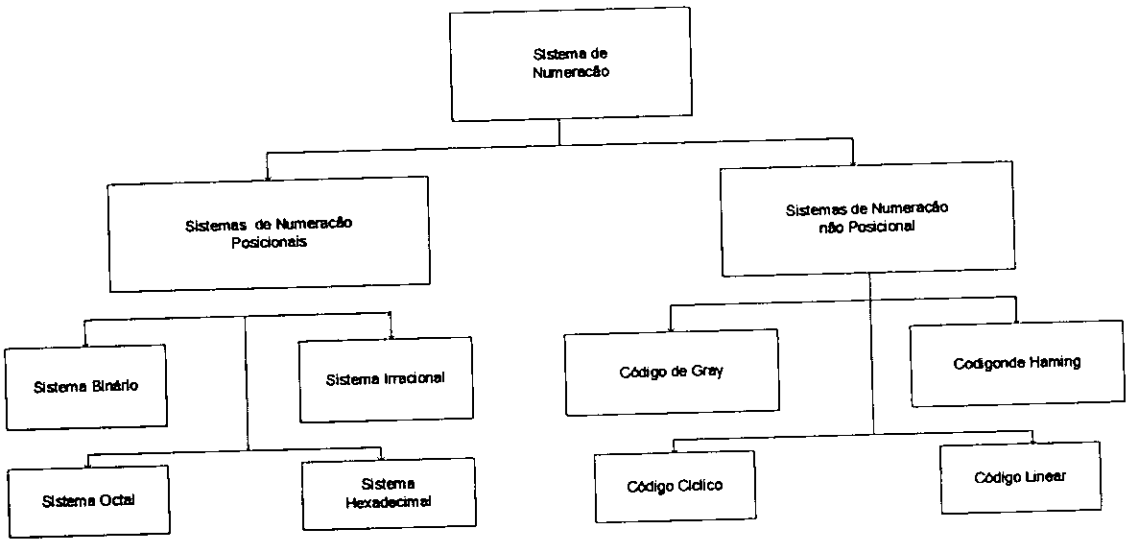

Figure 20 Classificação geral de sistemas de numeração

Uma classe grande que exige os cálculos aritméticos e lógicos usa o sistema de numeração posicional e nos casos restantes dão-nos o maior efeito vários códigos que pertencem ao sistema de numeração não posicional. Mas comparando as possibilidades e vantagens de sistemas posicionais podemos concluir que o sistema de numeração com base irracional é mais preferível porque inclui também o processo de controlo na realização das operações aritméticas e lógicas na unidade central de processamento.

Por isso focaremos a nossa atenção sobre códigos com a base irracional.

8.1 YD – CÓDIGOS

Para criar um sistema de numeração com base irracional podemos efectuar os números de Lucas e Fibonacci, usando a formula (29):

$$F_p(n) = F_p(n-p) + F_p(n-p-1) \tag{29}$$

onde $F(n)$ – número Fibonacci;

$p \in \{1,2,3...\}$ é parâmetro de código irracional, $n>p+1$.

Como exemplo consideremos três casos quando:

P=1; p=2; p=3, para 8 números usando a formula (29).

P=1: 21,13,8,5,3,2,1,1

P=2: 19,13,9,6,4,3,2,1,1,1

P=3: 10,7,5,4,3,2,1,1,1,1

Construiremos agora o código de Fibonacci para o parâmetro p = 1 que codificará os números decimais no intervalo [1..12], usando a tabela de codificação, tabela 7

Table 7 Sistema posicional de código Fibonacci

	F(7)	F(6)	F(5)	F(4)	F(3)	F(2)	F(1)
-ND	13	8	5	3	2	1	1
0	0	0	0	0	0	0	0
1	0	0	0	0	0	1	0
2	0	0	0	0	1	0	0
3	0	0	0	1	0	0	0
4	0	0	0	1	0	1	0
5	0	0	1	0	0	1	0
6	0	0	1	0	1	0	0
7	0	0	1	0	1	1	0
8	0	1	0	0	0	0	0
9	0	1	0	0	0	1	0
10	0	1	0	0	1	0	0
11	0	1	0	1	0	0	0
12	0	1	0	1	0	1	0

Onde: F(1)=F(2)=1

Na forma mínima numa combinação codificada de código Fibonacci o valor lógico está separado minimamente de ambos os lados com o valor lógico 0.

Por exemplo:

P = 1 1 0 0 1 0 1 0 1 0 0;

P = 2 1 0 0 0 1 0 0 1 0 0.

Esta última circunstância permite estabelecer um critério que desempenha um papel muito importante na detenção dos erros, por isso escolheremos entre todo conjunto das combinações codificadas no código Fibonacci só as combinações que satisfazem a uma condição rigorosa onde o valor lógico 1 deve ter obrigatoriamente dois valores lógicos 0 de cada lado, nomearemos este código YD-código.

É evidente que neste caso o conjunto de combinações codificadas de YD-códigos permitirá codificar a informação alfabética contidas no teclado do computador, e como resultado obteremos a possibilidade na codificação das mensagens alem disso, YD-códigos é um conjunto de combinações permitidas (CP) que fazem parte de 2^{n+1} combinações possíveis, e a parte restante será o conjunto das combinações não permitidas (CNP), ou seja, se durante um tratamento da informação aparecer uma combinação codificada CNP o esquema lógico deve reagir como surgimento de erro. Em resultado a probabilidade P pode ser calculada

$$P = \frac{2^{n+1} - CP}{2^{n+1}} \tag{30}$$

YD-códigos apresenta um código não posicional onde será possível formar três tipos YD-códigos, como um na ordem crescente e dois tipos de deslocamento, por exemplo para n=11 obteremos a tabela 8.

Table 8 YD-Códigos

	Crescente											Deslocamento 1											Deslocamento 2										
	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1
1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0
2	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	1	1	0	0
3	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	0	0
4	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0
5	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0
6	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0
7	0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0
8	0	0	0	0	1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0
9	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	1
A	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0
B	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0
C	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0
D	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0
E	0	0	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	0
F	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0
G	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
H	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0
I	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0
J	0	1	0	1	0	1	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0
-	----------											----------											----------										

Para o n = 11 obteremos da fórmula (2) o valor de p = 0,987. a figura seguinte ilustra uma interpretação gráfica para YD-código, onde n = 11, p = 25.

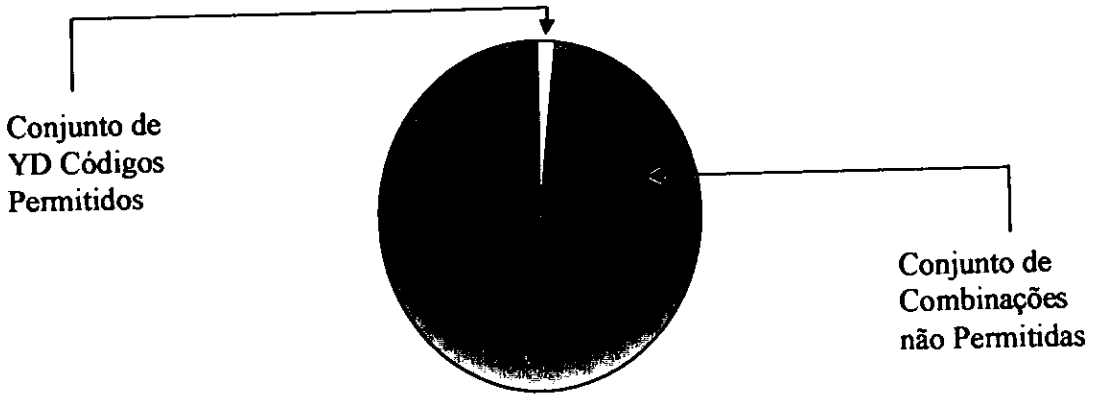

Figure 21 Interpretação gráfica de YD-código

o valor calculado da probabilidade mostra um alto nível na determinação dos erros simples, duplos, triplos, etc. Além disso o critério estabelecido no YD-codigo oferece-nos também outra possibilidade que permite corrigir esses erros.

Esta enorme possibilidade torna-se extremamente útil na transmissão dos dados num rádio canal.

8.2 Criptográfia de YD-Código

Falando sobre a transmissão da informação Digital através da Rádio canal temos que prever a possibilidade que permitirá proteger a informação contra o acesso ilegal, por isso Consideremos YD-códigos com ponto de vista de operações de tipo-R e de tipo-S.

Uma mensagem que deve ser transmitida através de uma linha de transmissão pode ser considerada como uma matriz correspondente, onde uma linha codifica um caracter que pertence ao teclado no sistema Binário. Mas o uso do sistema Binário dá-nos no processo de transmissão problemas, porque surgem erros que diminuem a veracidade da informação na sua recepção e não garantem a protecção desta informação. Por tanto, pode ser resolvido a primeira parte, usando YD-código que pode garantir alta veracidade da informação na sua recepção.

Para resolver a segunda parte do problema apresentaremos YD-código utilizando duas partes (tabela 9)

- Parte de característica;
- Parte Criptográfica.

Table 9 Código de reflexão irracional

YD código	Característica

O conjunto destas partes designamos como código de reflexão Irracional (CRI).

É evidente que este código pertencerá analogamente ao sistema de numeração não posicional.

Agora mostraremos um exemplo no processo de criptografia e de obtenção da característica no (CRI).

Da tabela 8.2-1 escolheremos P e YD-código crescente que codifica as letras A e B. Além disso, usaremos também a operação lógica do tipo-R para o parâmetro P=1

Table 10 Operação do tipo R em YD-código

	1 2 3 4 5 6 7 8 9 10 11	Característica
A	0 0 0 1 0 1 0 1 0 0 0	0 0 0
	0 0 0 1 0 1 0 0 1 1 0	0 0 0
	0 0 0 1 0 1 0 0 1 0 1	1 0 0
	0 0 0 1 0 0 1 1 1 0 1	1 0 0
	0 0 0 0 1 1 1 1 1 0 1	1 0 0
B	0 0 0 1 0 1 0 1 0 1 0	0 0 0
	0 0 0 1 0 1 0 1 0 0 1	1 0 0
	0 0 0 1 0 1 0 0 1 1 1	1 0 0
	0 0 0 1 0 0 1 1 1 1 1	1 0 0
	0 0 0 0 1 1 1 1 1 1 1	1 0 0

No resultado desta transformação as nossas letras A e B podem ter as suas formas correspondentes no CRI.

Table 11 Resultado de transformação no CRI

Letra	YD-Código	Característica
A	0 0 0 0 1 1 1 1 1 0 1	1 0 0
B	0 0 0 0 1 1 1 1 1 1 1	1 0 0

O algoritmo de transformação inversa prevê o uso da operação lógica do tipo-S e reflecte completamente o processo de decriptograr. E como resultado obteremos a matriz de mensagem no YD-Código.

As posições restantes de características podemos usar na codificação do outro parâmetro P de CRI.

O esquema de transmissão da informação da informação no CRI pode ser representado da maneira seguinte:

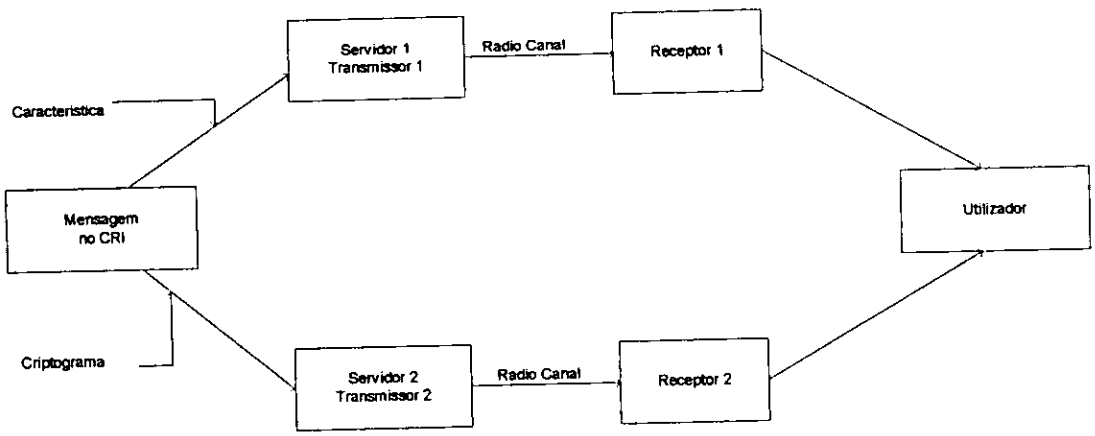

Figure 22 Esquema de Transmissão

O processo de separação de característica são criptogramas o que torna difícil para um Hacker o processo de decriptograr de CRI. Pode-se aumentar o nível de protecção do criptograma, criando YD-códigos com outros parâmetros P=2, P=3, etc.

9 CONCLUSÕES GERAIS E RECOMENDAÇÕES

A Segurança Criptográfica é um dos temas mais interessantes da actualidade, visto ocupar-se em proteger um dos bens mais valioso que é a informação. Contudo, há que ter em conta que não existe um mecanismo que seja 100% seguro uma vez que a Criptografia não pode proteger:

- Documentos não encriptados;
- Contra ataques ao sistema;
- Contra chaves roubadas;
- Erros ou utilizadores internos mal intencionados.

O objectivo deste trabalho não foi de dar soluções a todos os problemas de protecção da informação, mas sim mostrar que o uso de códigos com base irracional pode com alta rentabilidade resolver questões práticas na transmissão da informação digital através de um Rádio Canal.

Tendo em vista as limitações da criptografia em relação a segurança da informação, deve-se adoptar mecanismos de protecção fisica dos dados pois sem este os esforços gastos na criptografia serão nulos.

Em qualquer sistema informático os esforços de segurança devem estar em primeiro plano. Nunca se deve implementar um sistema criptográfico sem um pré investimento no sistema de segurança de informação.

Para futuros casos de estudos e para uma maior confiabilidade dos sistemas, é recomendável que os sistemas criptográficos sejam analisados em paralelo com o sistema de segurança da informação.

Os utilizadores internos, quando mal treinados ou por vezes quando mal intencionados no uso das ferramentas ao seu dispor, são o principal factor de ameaça para as Instituições. Por isso deve ser norma das Instituições implementar programas de formação dos seus utilizadores e promover acções tendo em vista sensibilizar os mesmos da importância de se respeitarem as regras de segurança aprovados.

10 BIBLIOGRAFIA

1. Domingues, Luís F. **Universidade Atlântica.** http://cryptanalyst.com/crypt/ . 2000.
2. Klander, Lars (1997). Hacker Proof: **The Ultimate Guide to Network Security.** Houston: Jamsa Press.
3. Pistelli, Daniela .**Criptografia.** http://nucc.pucsp.br/novo/cripto.html. Brasil, 2001.
4. Sabugo. **História da criptografia** . www.geocities.com/sabugo/ . 1999.
5. Vashnor, Demitriv**. Criptografia** .http://www.windefense.hpg.ig. 2002.
6. Schneier, B. (1993). **Applied Cryptography.** John Wiley.
7. Seberry, J. and J. Pieprzyk (1989). **Cryptography - An Introduction to Computer Security**. Prentice Hall
8. Petrossiuk, Y. Mannestig, D.(2003) **Transmissão da Informação entre Sistemas Digitais**, Matemática, Estatística Informática, DMI.
9. Stakhov, A. P. Petrossiuk Y, A. (1999). **Coding Theory Basead in Fibonacci Numbers and Golden Section**. Boletim de Informática – 3. UEM, pg 38 – 47.
10. Stakhov, A. P.; Petroussuik, Y.; Sotomane, C. (1996). **Uso de Códigos com Base Irracional nos Conversores Digitais Analógicos**. Matemática Estatística, Informática UEM – DMI.
11. Oliveira, Wilson (2001). **Segurança da Informação Técnicas e Soluções**. 1ª Edição, Lisboa, Portugal, Centro Atlântico.

11 GLOSSÁRIO

- **Algoritmo**: Conjunto de operações elementares que devem ser efectuadas para se obter um resultado desejado. Por exemplo, uma receita de bolo é um algoritmo (Schneier, 1999).
- **Ataque**: Tentativa de criptoanálise (Schneier, 1999).
- **Assimétrico**: Um algoritmo de encriptação que utiliza uma chave pública para encriptar e uma chave privada (diferente) para decifrar as mensagens(Schneier, 1999).
- **Autenticar**: Se assegurar da identidade do remetente de uma mensagem e da integridade da mensagem recebida (Schneier, 1999).
- **Chave:** Num sistema de encriptação, corresponde a um nome, uma palavra, uma frase, etc., que permite, mediante o algoritmo de encriptação, cifrar ou decifrar uma mensagem (Schneier, 1999).
- **Cifra**: Conjunto de procedimentos e conjunto de símbolos (letras, nomes, sinais, etc.) usados para substituir as letras de uma mensagem para encriptá-la. É geralmente classificada como cifra de transposição e cifra de substituição (Schneier, 1999).
- **Cifrar**: Procedimento pelo qual se torna impossível a compreensão de um documento a qualquer pessoa que não possua a chave da cifra (Schneier, 1999).
- **Codificar**: Modificar a estrutura de um conjunto de documentos aplicando um algoritmo (cifra, método de compressão, etc.). (Schneier, 1999).
- **Confidencialidade**: Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação (Schneier, 1999).
- **Cracker**: hacker mal intencionado
- **Criptografia** (kriptós = escondido, oculto; grápho = grafia) : é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e a compreenda. (Vashnor, 2002).
- **Criptoanálise** (kriptós = escondido, oculto; análysis = decomposição) : é a arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque. (Vashnor, 2002).
- **Criptograma**: Mensagem cifrada ou codificada (Schneier, 1999).

- **Criptologia** (kriptós = escondido, oculto; logo = estudo, ciência) : é a ciência que reúne a criptografia e a criptoanálise. (Vashnor, 2002).
- **Hacker:** profundo conhecedor de computadores e áreas de computadores.
- **TPC** (tranmission control protocol): é uma linguagem básica de comunicação utilizada na Internet e pode ser também em redes privadas (Oliveira, 2001).
- **UDP** (user datagram protocol): método de comunicação que pode ser utilizado como alternativa ao TCP. Quando utilizado junto ao IP é conhecido como UDP/IP, mas algumas limitações técnicas tornam o seu uso restrito a redes nas quais transitam pacotes de pequeno tamanho (Oliveira, 2001).