

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

**UM ESTUDO SOBRE A UTILIZAÇÃO DE CRIPTOGRAFIA PARA GARANTIA DE
SEGURANÇA DE DADOS EM REDES DE COMPUTADORES**

**UM ESTUDO SOBRE A UTILIZAÇÃO DE CRIPTOGRAFIA PARA GARANTIA DE
SEGURANÇA DE DADOS EM REDES DE COMPUTADORES**

Projeto de Monografia apresentado
no curso de Especialização em
Redes de Computadores, da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do
Norte, como requisito parcial para a
obtenção do título de Especialista
em Redes de Computadores.

Orientador:

Gleydson de A. Sued de Souza Lima

LIGA DE ENSINO DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

UM ESTUDO SOBRE A UTILIZAÇÃO DE CRIPTOGRAFIA PARA GARANTIA DE SEGURANÇA DE DADOS EM REDES DE COMPUTADORES

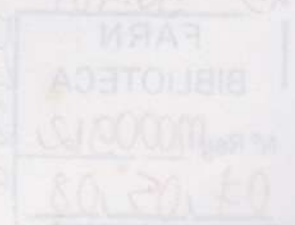
Sued de Souza Lima

Projeto de Monografia apresentado
ao curso de Especialização em
Redes de Computadores, da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do
Norte, como requisito parcial para a
obtenção do título de Especialista
em Redes de Computadores.

Orientador:

Gleydson de A. F. Lima, Mestre

NATAL/RN
2008



SUED DE SOUZA LIMA

UM ESTUDO SOBRE A UTILIZAÇÃO DE CRIPTOGRAFIA PARA GARANTIA DE
SEGURANÇA DE DADOS EM REDES DE COMPUTADORES

Projeto de Monografia apresentado
ao curso de Especialização em
Redes de Computadores, da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do
Norte, no âmbito do curso de
Especialização em Redes de Computadores.

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Lima, Sued de Souza

Um estudo sobre a utilização de criptografia para garantia de
segurança de dados em redes de computadores / Sued de Souza Lima. –
Natal: FARN, 2008.
89 f.

Orientador: Gleydson de A. F. Lima (M.Sc.)
Monografia (Especialização em Redes de Computadores) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Criptografia – Monografia. 2. Segurança de Redes – Monografia. 3.
Redes de Computadores – Monografia. I. Título.

RN/FARN/BC

CDU 004.7

RB-30.781

M

FARN
BIBLIOTECA

Nº Reg

0000912

07.05.08

004.7

271

2008

ex 01

NATALIAN
8005

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

**UM ESTUDO SOBRE A UTILIZAÇÃO DE CRIPTOGRAFIA PARA GARANTIA DE
SEGURANÇA DE DADOS EM REDES DE COMPUTADORES**

Sued de Souza Lima

**Monografia apresentada e aprovada em _____ de março de 2008, pela banca
examinadora composta pelos seguintes membros:**

Gleydson de A. F. Lima, Mestre
Orientador

Aluízio Ferreira da Rocha Neto, Mestre
Membro examinador

Natal/RN, _____ de março de 2008.

Agradecimentos

Ao meu orientador, Professor Oleydson Lima, pela confiança depositada quando prontamente aceitou ser meu orientador, pela paciência e compreensão nas muitas dificuldades, e pelo cuidado com que guio as minhas passagens na construção desta monografia. Aproveito, também, para deixar registrada a minha sincera admiração pelo seu profissionalismo e dedicação com que exerce o seu trabalho.

Ao meu noivo, Elvis Zanetti Evangelista, meu principal incentivo para conclusão deste trabalho, que de uma forma muito carinhosa me apoiou na organização de meu tempo de estudo e nas minhas prioridades.

Especialmente à minha família, que incondicionalmente acredita na minha capacidade e sempre me apoiou em todos os meus projetos e sonhos, me fornecendo todo amor que preciso.

Dedico este trabalho ao meu Deus, que é o principal responsável por tudo aquilo que tenho e conquistei. Foi nele que encontrei a força e o ânimo para vencer cada desafio, a saúde para continuar lutando, a inteligência e a capacidade necessária para chegar até aqui. Obrigada, Senhor!

Agradecimentos

Ao meu orientador, Professor Gleydson Lima, pela confiança depositada quando prontamente aceitou ser meu orientador, pela paciência e compreensão nas minhas dificuldades, e pelo cuidado com que guiou os meus passos na construção desta monografia. Aproveito, também, para deixar registrada a minha sincera admiração pelo seu profissionalismo e dedicação com que exerce o seu trabalho.

Ao meu noivo, Elvis Zamith Evangelista, meu principal incentivo para conclusão deste trabalho, que de uma forma muito carinhosa me ajudou na organização de meu tempo de estudo e nas minhas prioridades.

Especialmente à minha família, que incondicionalmente acreditou na minha capacidade e sempre me apoiou em todos os meus projetos e sonhos, me fornecendo todo amor que precisei.

Resumo

Este trabalho apresenta um estudo detalhado sobre criptografia, focando especificamente a sua utilização na segurança de dados. Ao longo do estudo, é apresentado como a criptografia se desenvolveu no decorrer da história, desde a antiguidade até os dias de hoje, enfatizando as invenções criptográficas e pessoas que se destacaram em cada época. São apresentados os principais conceitos que envolvem a criptografia, descritos os tipos de cifras disponíveis, os protocolos utilizados na internet que implementam a criptografia e as várias formas de aplicação da criptografia em redes de computadores. Também, são apresentadas soluções em softwares que implementam a criptografia, nos mais diversos serviços utilizados no dia-a-dia do usuário.

Palavras Chaves:

Criptografia, Cifras, Algoritmos, ICP, Certificação Digital, Hash, Assinatura Digital, Segurança de dados, Protocolos, Internet, Rede Wireless, Ferramentas Criptográficas.

Abstract

This essay presents a minute study about cryptography, emphasizing specifically your utilization in data security. In this study, it is presented how the cryptography developed along the history, since the antiquity until the present day, emphasizing the cryptographics inventions and the detachable peoples that show up in each age. They are presented the main concepts involving cryptography, described the types of available ciphers, the protocols utilized in internet that implement cryptography and the several ways of applications of the one in computers nets. Also, they are presented software solutions that implement cryptography, in more diverse services utilized by user day-by-day.

Keywords:

Cryptography, Ciphers, Algorithms, ICP, Digital Certification, Hash, Digital Signature, Data Security, Protocols, Internet, Wireless Net, Cryptographic Tools.

Lista de Figuras

Figura 1. Esquema de funcionamento do modo ECB	29
Figura 2. Esquema de funcionamento do modo CBC	30
Figura 3. Esquema de funcionamento do modo CFB	30
Figura 4. Esquema de funcionamento do modo OFB	31
Figura 5. Exemplo de aplicação de encriptação por Cifra de Fluxo.....	32
Figura 6. Exemplo de utilização da Criptografia Assimétrica.....	37
Figura 7. Cabeçalho genérico para o modo de transporte	60
Figura 8. Exemplo de um cabeçalho do modo túnel	60
Figura 9. Exemplo de um navegador acessando um site que utiliza o protocolo SSL.....	66
Figura 10. Ataques man-in-the-middle e hijack	74
Figura 11. Rede WLAN com VPN/IPSec	74
Figura 12. Tela do software Encrypted Magic Folder.....	81
Figura 13. Tela do software Best Crypt.....	81
Figura 14. Exemplo de criptografia de arquivos com o software PGP	82
Figura 15. Tela do software DriveCrypt.....	84
Figura 16. Tela do software FineCrypt.....	85
Figura 17. Tela do software TrueCrypt	86
3.2.3.1. DES (Data Encryption Standard)	37
3.2.3.2. DES-Triplo	38
3.2.3.3. IDEA (International Data Encryption Algorithm)	39
3.2.3.4. Rijndael	39
3.2.3.5. RC (Ron's Code or Rivest Cipher)	39
3.2.3.6. Blowfish	39
3.2.3.7. Twofish	39
3.3. Criptografia Assimétrica	39
3.3.1. Funções One-Way	39
3.3.1.1. Implementação das Chaves Públicas e Privadas	39
3.3.2. ECC (Elliptic Curve Cryptography)	39
3.3.3. Algoritmos Assimétricos	39
3.3.3.1. DH	39
3.3.3.2. RSA	39
3.3.3.3. ElGamal	39
3.4. Criptografia Híbrida	39
3.5. Chaves de Sessão	39
3.5.1. Distribuição de Chaves	39
3.5.1.1. Associação de Segurança (Security Association, SA)	39
3.5.2. Acordo de Chaves	39
3.6. Funções de Hash Criptográficas	39
3.6.1. Algoritmos de Hash	39
3.6.1.1. MD4 e MD5	39
3.6.1.2. SHA-1 (Secure Hash Algorithm)	39
3.6.2. MAC (Message Authentication Codes)	39
3.7. Assinaturas Digitais	39
3.7.1. Algoritmos de Assinatura Digital	39
3.7.1.1. RSA	39
3.7.1.2. DSA (Digital Signature Algorithm)	39
3.7.1.3. ECDSA (Elliptic Curve Digital Signature Algorithm)	39
3.7.2. Assinaturas Digitais e Funções de Hash	39
3.7.3. Protocolo de Acordo de Chaves: Station-to-Station (STS)	39
3.8. ICP (Infraestrutura de Chaves Públicas)	39
3.8.1. Certificados Digitais	39
3.9. Criptografia Quântica	39
Capítulo 4 – Aplicação de Criptografia em Redes de Computadores	39

Sumário

Capítulo 1 – Introdução	10
1.1. Problema de Pesquisa.....	12
1.2. Objetivos Gerais.....	12
1.3. Justificativa	12
Capítulo 2 – História da Criptografia	14
2.1. O que é Criptografia.....	14
2.2. Criptografia na Antiguidade.....	14
2.3. Criptografia na Idade Média	17
2.4. Criptografia na Idade Moderna	18
2.5. Criptografia na atualidade	20
Capítulo 3 – Conceitos Gerais.....	25
3.1. Cifras e Códigos.....	25
3.2. Criptografia Simétrica.....	26
3.2.1. Cifras de blocos.....	27
3.2.1.1. Electronic Code Book Mode (ECB).....	28
3.2.1.2. Cypher Block Chaining Mode (CBC).....	29
3.2.1.3. Cypher Feedback Mode (CFB)	30
3.2.1.4. Output Feedback Mode (OFB).....	31
3.2.2. Cifras de fluxo.....	32
3.2.3. Algoritmos simétricos	32
3.2.3.1. DES (Data Encryption Standard)	32
3.2.3.2. DES-Triplo.....	33
3.2.3.3. IDEA (International Data Encryption Algorithm)	33
3.2.3.4. Rijndael	34
3.2.3.5. RC (Ron's Code ou Rivest Cipher)	34
3.2.3.6. Blowfish.....	35
3.2.3.7. Twofish	36
3.3. Criptografia Assimétrica	36
3.3.1. Funções One-Way	37
3.3.2. Implementação das Chaves Públicas e Privadas	38
3.3.3. ECC (Elliptic Curve Cryptography).....	38
3.3.4. Algoritmos assimétricos.....	39
3.3.4.1. DH.....	39
3.3.4.2. RSA.....	39
3.3.4.3. El Gamal	39
3.4. Criptografia Híbrida.....	40
3.5. Chaves de Sessão	41
3.5.1. Distribuição de Chaves	41
3.5.1.1. Associações de Segurança (Security Association, SA).....	42
3.5.2. Acordo de Chaves	42
3.6. Funções de Hash Criptográficas.....	43
3.6.1. Algoritmos de Hash	44
3.6.1.1. MD4 e MD5	44
3.6.1.2. SHA-1 (Secure Hash Algorithm)	44
3.6.2. MAC (Message Authentication Codes)	45
3.7. Assinaturas Digitais	46
3.7.1. Algoritmos de Assinatura Digital.....	47
3.7.1.1. RSA.....	47
3.7.1.2. DAS (Digital Signature Algorithm)	48
3.7.1.3. ECDSA (Elliptic Curve Digital Signature Algorithm).....	48
3.7.2. Assinaturas Digitais e Funções de Hash	48
3.7.3. Protocolo de Acordo de Chaves: Station-to-Station (STS)	49
3.8. ICP (Infraestrutura de Chaves Públicas).....	49
3.8.1. Certificados Digitais	50
3.9. Criptografia Quântica.....	51
Capítulo 4 – Aplicação de Criptografia em Redes de Computadores.....	53

4.1.	Segurança de Informação e Segurança em Rede.....	53
4.2.	Requisitos de Segurança	53
4.3.	Gerência de Segurança OSI	54
4.4.	Ataques a Sistemas Computacionais.....	55
4.5.	Protocolos de rede que implementam Criptografia.....	55
4.5.1.	SSL (Secure Sockets Layer).....	55
4.5.2.	TLS (Transport Layer Security).....	56
4.5.3.	HTTPS (HyperText Transfer Protocol Secure).....	58
4.5.4.	IPSec (IP Security Protocol)	58
4.5.5.	SSH (Secure SHell).....	61
4.5.6.	Kerberos.....	61
4.6.	Criptografia na Internet.....	62
4.6.1.	Utilização de Criptografia em Emails	63
4.6.2.	Uso de criptografia nos navegadores	65
4.7.	Criptografia em redes Wireless	66
4.7.1.	Protocolos de segurança em redes Wireless.....	67
4.7.1.1.	WEP (Wired Equivalent Privacy)	67
4.7.1.2.	TKIP (Temporal Key Integrity Protocol).....	68
4.7.1.3.	WPA (Wi-Fi Protected Access)	69
4.7.1.4.	WPA2.....	70
4.7.1.5.	IEEE 802.11w	71
4.7.1.6.	IEEE 802.1X (RFC 3580).....	72
4.7.2.	Segurança em rede Wireless com VPN.....	74
Capítulo 5 – Soluções criptográficas em softwares		76
5.1.	Programas de Email	76
5.1.1.	Microsoft Office Outlook 2003.....	76
5.1.2.	Mozilla Mail / Thunderbird.....	77
5.2.	Criptografia em listas de discussão	77
5.3.	Assinatura digital como proteção de software	78
5.4.	Criptografia de arquivos.....	78
5.4.1.	Criptografia de arquivos em ambiente Linux.....	79
5.4.2.	Criptografia de arquivos em ambiente Windows	80
5.4.2.1.	Encrypted Magic Folder.....	80
5.4.2.2.	Best Crypt	81
5.4.2.3.	PGP	82
5.4.2.4.	Cypher Millenium	83
5.4.2.5.	DriveCrypt	83
5.4.2.6.	FineCrypt	84
5.4.2.7.	TrueCrypt.....	85
5.5.	Criptografia em ambientes corporativos	86
Capítulo 6 – Conclusão		76
Referências Bibliográficas		lxxxix

planos de batalha. A criptografia digital já era usada secretamente desde 1949 por militares e governos. A criptografia foi largamente utilizada na Segunda Guerra Mundial, para comunicar planos de ação, posicionamento de tropas e trocar mensagens entre altas patentes. Mas foi só com a invenção do computador que a criptografia mostrou todo seu poder, utilizando-se de complexos algoritmos matemáticos para geração de seus códigos. Em meados da década de 1970 a IBM inventou o padrão DES (Data Encryption Standard) de criptografia, que passou a ser largamente utilizado até os dias de hoje.

O rápido avanço tecnológico exigiu sistemas de segurança cada vez mais complexos onde a criptografia deve ser implementada de forma integrada. Devido a isso, atualmente não

Capítulo 1 – Introdução

Com o advento das redes de computadores e posteriormente com a explosão da Internet, surgiram inúmeras possibilidades para fornecimento de serviços, nas mais diversas áreas, facilidades para o compartilhamento de informações e para a comunicação de um modo geral. Porém, como na Internet as informações fluem publicamente, em inúmeras situações surge a necessidade de se garantir segurança a esses dados, sendo muitas as motivações para se introduzir segurança na comunicação em redes de computadores. Isto por que, atualmente, através da Internet é possível realizar transações financeiras, bancárias ou mesmo compra de produtos e serviços; comunicação através de emails; e o armazenamento de dados, pessoais ou comerciais. Acrescenta-se a contra-espionagem industrial e militar, além de ações antiterroristas, que aumentam a demanda por sistemas de segurança de alta confiabilidade.

A técnica utilizada para atender a esta demanda por segurança e privacidade é a criptografia. As técnicas de criptografia figuram hoje como um dos principais recursos utilizados no contexto de serviços de segurança da informação. O objetivo é transmitir as informações de uma maneira que somente o destinatário possa compreender, obtendo-se segurança das transmissões de dados. Assim, a mensagem distribuída em um canal de comunicação público passa a ser não inteligível aos usuários para os quais a mesma não foi endereçada ou autorizada. É desta forma que se tornou possível utilizar a Internet para tráfego de informações confidenciais.

A preocupação com a segurança dos dados é antiga. A origem da criptografia, provavelmente, remonta ao princípio da existência humana, logo que as pessoas tenham tentado aprender a comunicar, tendo de encontrar meios para garantir a confidencialidade de parte das suas comunicações. Os romanos já utilizavam códigos secretos para comunicar planos de batalha. A criptografia digital já era usada secretamente desde 1949 por militares e governos. A criptografia foi largamente utilizada na Segunda Guerra Mundial, para comunicar planos de ação, posicionamento de tropas e trocar mensagens entre altas patentes. Mas foi só com a invenção do computador que a criptografia mostrou todo seu poder, utilizando-se de complexos algoritmos matemáticos para geração de seus códigos. Em meados da década de 1970 a IBM inventou o padrão DES (Data Encryption Standard) de criptografia, que passou a ser largamente utilizado até os dias de hoje.

O rápido avanço tecnológico exige sistemas de segurança cada vez mais complexos onde a criptografia deve ser implantada de forma integrada. Devido a isso, estudiosos têm

devotado esforços à criação de novas técnicas de encriptação que sejam dignas de confiança e apresentem boa performance.

Durante o século XIX, foi apresentado os princípios da encriptação moderna. Um destes princípios afirmava que a segurança de um sistema encriptado não residia no processo de encriptação em si, mas na chave que era utilizada. Em 1948, foram adicionadas bases científicas à criptografia com duas produções de Claude Shannon: "Uma Teoria Matemática da Comunicação" e, principalmente, "A Teoria de Comunicação de Sistemas Secretos". O Shannon provou a cifração de Vernam que havia sido proposta alguns anos antes – e também a renomeou para One Time Pad – e era o único sistema, incondicionalmente, seguro que poderia existir. Porém, não era possível pôr tal sistema em prática. Por esta razão, atualmente, a evolução dos sistemas de segurança é baseada em segurança computacional. Esta defende que a chave de cifração é segura se nenhum ataque conhecido não faça mais do que procurar por todas as chaves possíveis.

Este trabalho fará um estudo dos principais conceitos sobre criptografia, possibilitando uma visão geral do que há hoje disponível e o que tem sido utilizado em segurança de informações digitais. Estruturalmente, a monografia está dividida em mais cinco capítulos:

- Capítulo 2 – História da Criptografia. Neste capítulo é feita uma retrospectiva de como surgiu a criptografia, como ela se desenvolveu nos vários períodos da história, começando na antiguidade e passando pela idade média, idade moderna até os dias de hoje. Em cada uma dessas fases, é apresentado o contexto histórico, com os principais acontecimentos que marcaram o período, abordando como a humanidade se utilizava da criptografia e os principais avanços nesta área.
- Capítulo 3 – Conceitos Gerais. Aqui são apresentados os pontos fundamentais que estão associados ao estudo da criptografia. Nele, é abordada a criptografia simétrica e assimétrica, os principais algoritmos criptográficos, o funcionamento das cifras por blocos e de fluxo, a vantagem de se utilizar chaves de sessão, o que é criptografia híbrida e quântica e como as funções de hash e as assinaturas digitais são combinadas com a criptografia para garantir segurança.
- Capítulo 4 – Aplicação de Criptografia em Redes de Computadores. Este capítulo inicia abordando a importância de se garantir segurança em redes de computadores e os conceitos que estão associados no estudo de segurança da informação. Depois é apresentado os principais protocolos de rede que se utilizam da criptografia para garantir confidencialidade nas diversas camadas da arquitetura TCP/IP, o uso de

criptografia em emails e navegadores web e, por fim, é abordado o uso de criptografia em redes wireless.

- Capítulo 5 – Soluções criptográficas em softwares. É cada vez mais comum a conscientização dos usuários de computadores da necessidade de proteger seus dados. Neste capítulo são apresentadas algumas ferramentas, para aplicações diversas, que implementam criptografia, a fim de garantir confidencialidade da informação digital.
- Capítulo 6 – Conclusão. É neste capítulo onde é apresentada, de forma resumida, a contribuição desse trabalho no estudo da criptografia.

1.1. Problema de Pesquisa

Diante da disponibilidade de informação através da Internet, ficou mais fácil adquirir conhecimento em diversas áreas. Porém, esta facilidade tem permitido que pessoas mal intencionadas tenham acesso a dados pessoais ou comerciais, que utilizados de forma irresponsável ou dolosa, poderia causar danos irreparáveis financeiras ou até mesmo morais. Tem sido feito pesquisas e desenvolvido técnicas no sentido de garantir a segurança de dados, mesmo em um canal inseguro como a Internet. Porém, muitas pessoas ainda não percebem o risco a que estão passíveis e não dão a devida atenção à segurança de seus dados.

Como as técnicas de criptografia figuram como um dos principais recursos utilizados no contexto de serviços de segurança da informação, têm-se verificado a necessidade em disseminar os conceitos que envolvem a ciência da escrita em cifras a fim de proporcionar segurança e confiabilidade no uso de redes de computadores.

1.2. Objetivos Gerais

Esse projeto tem a finalidade de servir como um bom referencial teórico para estudantes e pessoas interessadas em ter uma visão abrangente sobre criptografia de dados, abordando de forma clara e objetiva as principais questões sobre o assunto.

1.3. Justificativa

Por meio deste projeto, qualquer pessoa poderá ter acesso aos conceitos essenciais para entender o que é a criptografia de dados e como é e pode ser aplicada e qual a sua importância na segurança da informação digital. Terá uma visão geral sobre a evolução histórica do uso de criptografia, quais as diversas técnicas utilizadas, quais os principais

algoritmos, podendo confrontar suas vantagens e fraquezas. Além disso, para dar uma visão prática da utilização da criptografia, são apresentados algumas soluções em softwares que implementam criptografia, de forma que seja possível ter uma idéia da utilização de cada uma dessas ferramentas e a sua aplicação no dia-a-dia do usuário.

Criptografia (do grego *kryptōs*, "oculto", e *graphō*, "escrever") é geralmente entendida como a área do conhecimento que desenvolve métodos para codificar mensagens (escrever secretamente). É o estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida uma "chave secreta", com o objetivo de garantir que apenas o destinatário a decodifique e compreenda. Na prática, a criptografia é um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática.

O estudo das formas de esconder o significado de uma mensagem, usando técnicas de cifragem, tem sido acompanhado pelo estudo das formas de conseguir ler a mensagem quando não se é o destinatário; este campo de estudo é chamado *Criptanálise* (do grego *análysis*, "decomposição"), que trata do ato de decifrar ou quebrar o sistema criptográfico. A *Criptologia* é a ciência que engloba a Criptografia e a Criptanálise.

2.2. Criptografia na Antiguidade

A necessidade de viver em bandos, para vencer as condições hostis do meio ambiente, levou o ser humano primitivo a desenvolver uma sofisticada linguagem falada. Ao mesmo tempo, gradualmente, ele foi criando símbolos para retratar situações de seu cotidiano, como as imagens pictográficas, em pinturas, nas paredes de cavernas. Esta lenta evolução nas linguagens de comunicação possibilitou o surgimento da escrita e, com ela, a necessidade de transmissão de mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor. Consequentemente, surgiu também o desejo de interceptar mensagens e de decifrá-las, por diversos motivos: segredos militares, políticos, religiosos, questões de comércio ou questões sentimentais.

Segundo Costa e Figueiredo (2006), na Antiguidade, foram desenvolvidos dois métodos de ocultar mensagens. O primeiro consistia em esconder a mensagem propriamente dita. É uma técnica de transmissão secreta de mensagens, conhecida como Estenografia, que consiste em ocultar a mensagem, sem mudanças em seu estado original. Foi desenvolvida por volta de 1500 a.C., por culturas como a do Egito, China, Índia e da Mesopotâmia. Ela não é considerada parte da Criptologia, apesar de muitas vezes ser estudada em conjunto

Capítulo 2 – História da Criptografia

2.1. O que é Criptografia

Criptografia (do grego *kryptós*, "escondido", e *gráphein*, "escrever") é geralmente entendida como a área do conhecimento que desenvolve métodos para codificar mensagens (escrever secretamente). É o estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida uma "chave secreta", com o objetivo de permitir que apenas o destinatário a decodifique e compreenda. Na prática, a criptografia é um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática.

O estudo das formas de esconder o significado de uma mensagem, usando técnicas de cifragem, tem sido acompanhado pelo estudo das formas de conseguir ler a mensagem quando não se é o destinatário; este campo de estudo é chamado *Criptoanálise* (do grego *análysis*, "decomposição"), que trata do ato de decifrar ou quebrar o sistema criptográfico. A *Criptologia* é a ciência que engloba a Criptografia e a Criptoanálise.

2.2. Criptografia na Antiguidade

A necessidade de viver em bandos, para vencer as condições hostis do meio ambiente, levou o ser humano primitivo a desenvolver uma sofisticada linguagem falada. Ao mesmo tempo, gradualmente, ele foi criando símbolos para retratar situações de seu cotidiano, como as imagens pictográficas, em pinturas, nas paredes de cavernas. Esta lenta evolução nas linguagens de comunicação possibilitou o surgimento da escrita e, com ela, a necessidade de transmissão de mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor. Conseqüentemente, surgiu também o desejo de interceptar mensagens e de decifrá-las, por diversos motivos: segredos militares, políticos, religiosos, questões de comércio ou questões sentimentais.

Segundo Costa e Figueiredo (2006), na Antiguidade, foram desenvolvidos dois métodos de ocultar mensagens. O primeiro consistia em esconder a mensagem propriamente dita. É uma técnica de transmissão secreta de mensagens, conhecida como Estenografia, que consiste em ocultar a mensagem, sem mudanças em seu estado original. Foi desenvolvida por volta de 1500 a.C., por culturas como a do Egito, China, Índia e da Mesopotâmia. Ela não é considerada parte da Criptologia, apesar de muitas vezes ser estudada em contextos

semelhantes. Diferentemente da Criptografia, que confunde a mensagem de forma a tornar seu significado ininteligível, a Estenografia apenas oculta a mensagem. A vulnerabilidade do método é muito grande, uma vez que sendo descoberta, a mensagem é imediatamente decifrada. Exemplos do uso da Estenografia:

- tatuagens com mensagens na cabeça de escravos (era preciso esperar o cabelo crescer);

- marcas na madeira de placas de cera (as marcas eram escondidas com cera nova; para decifrar, bastava derreter a cera); e

- mensagens dentro do estômago de animais de caça e também de humanos.

O segundo método usava processos em que a mensagem, mesmo tornada pública, não seria entendida pelo interceptador, uma vez que a chave era desconhecida para a leitura. Entretanto, neste período, ainda não se utilizava sistema de códigos ou cálculos matemáticos. Tratava-se de soluções criativas, que acabaram dando base e consistência à criptologia. Foi uma evolução lenta, porém constante. Traços de criptografia apareceram por volta de 2000 a.C., no Egito e na Mesopotâmia.

Segundo Braga (2007?), o primeiro exemplo documentado da escrita cifrada ocorreu cerca de 1900 a.C., numa vila egípcia, perto do rio Nilo. Khnumhotep II, um arquiteto do faraó Amenemhet II, construiu alguns monumentos para o faraó, os quais precisavam ser documentados, porém estas informações, escritas em tabletes de argila, não deveriam cair no domínio público. O escriba de Khnumhotep II teve a idéia de substituir algumas palavras ou trechos de texto destes tabletes. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro, ao invés disso, morreria de fome, perdido nas catacumbas da pirâmide.

Em 1500 a.C, a criptografia da Mesopotâmia ultrapassou a egípcia, chegando a um nível bastante moderno. O primeiro registro do uso da criptografia nesta região está numa fórmula para fazer esmaltes para cerâmica. O tablete com a fórmula, cerca de 8cm x 5cm, foi achado às margens do rio Tigre e utilizava símbolos especiais, que podiam ter vários significados diferentes.

Atbash, Albam e Atbah são três das cifras hebraicas mais conhecidas. Datam de 600-500 a.C. e eram usadas principalmente em textos religiosos, como foi utilizado a cifra Atbash no livro de Jeremias. Estas cifras baseiam-se no sistema de substituição simples (ou substituição monoalfabética). As três são denominadas reversíveis porque na primeira operação obtém-se o texto cifrado e, aplicando-se a mesma cifra ao texto cifrado, obtém-se o texto original.

A cidade-estado grega de Esparta era dominada por uma rígida cultura da guerra e por isso tinha grande preocupação com a segurança das comunicações militares. Em 475 a.C., foram entregues ordens ao príncipe e general espartano, Pasanus, através do que poderia ser o sistema de criptografia militar mais antigo: o **scytale** ou **bastão de Licurgo**. O scytale consistia num bastão de madeira ao redor do qual se enrolava firmemente uma tira de couro ou pergaminho, longa e estreita. Escrevia-se a mensagem no sentido do comprimento do bastão. Em seguida, a tira era desenrolada e, dessa forma, a mensagem estava cifrada.

Braga (2007) relata que, em 300 a.C., **Artha-sastra**, um livro atribuído a Kautilya, foi escrito na Índia, referindo-se a diversas cifras criptográficas e recomendando uma variedade de métodos de criptoanálise para obter relatórios de espionagem. Pouco tempo depois, Euclides de Alexandria, um matemático grego, que viveu aproximadamente de 330 a.C. a 270 a.C., compilou e sistematizou a geometria e a teoria dos números da sua época no famoso texto "**Elementos**", obra que teve grande influência na criptologia atual. Outro importante personagem da história foi Erastótenes de Cirene, filósofo e geômetra grego, que viveu de 276 a.C. a 194 a.C. Era conhecido como criador de um método para identificar números primos, o **crivo de Erastótenes**, e por ter calculado o diâmetro da Terra com surpreendente precisão. Políbio, um historiador grego nascido em Megalópolis, que viveu de 204 a.C. a 122 a.C., escreveu vários livros sobre o Império Romano. A ele é atribuída a uma cifra de substituição que converte os caracteres da mensagem em cifras - o **código de Políbio**. Porém o mesmo não relatou qualquer utilização do seu sistema.

Por volta de 50 a.C., Júlio César usou sua famosa cifra de substituição para cifrar mensagens governamentais. Para compor seu texto cifrado, César alterou letras desviando-as em três posições: A se tornava D, B se tornava E, e assim por diante. Às vezes, César reforçava sua cifragem substituindo letras latinas por gregas. O **código de César** é o único da antiguidade que é usado até hoje, apesar de representar um retrocesso em relação à criptografia existente na época. Atualmente em homenagem ao imperador romano, denomina-se qualquer cifra baseada na substituição cíclica do alfabeto de código de César. Com um alfabeto de 26 letras são possíveis 25 códigos distintos de César. O número de casas deslocadas é a chave do código. Os códigos de César se revelaram úteis em um período em que poucas pessoas sabiam ler. Uma época em que não havia ainda começado a criptoanálise.

De modo geral, durante a Idade Antiga e na primeira metade da Idade Média (até o ano 800), dominaram as cifragens monoalfabéticas. De acordo com Costa e Figueiredo (2006), as cifras mais populares, em virtude da fácil utilização e memorização, foram aquelas baseadas em Códigos de César.

2.3. Criptografia na Idade Média

A idade Média iniciou efetivamente por volta de 476, com a queda do Império Romano, e terminou em 1453, com a queda de Constantinopla. Foi uma época caracterizada por relativa recessão no domínio das idéias. A criptografia não escapou desta "recessão". Segundo Costa e Figueiredo (2006), grande parte do conhecimento sobre o assunto foi perdido, pois era considerada magia negra ou bruxaria. Este período, principalmente o da primeira metade da Idade Média, foi marcado por perseguições religiosas. Nessa época, era muito perigosa a correspondência através de mensagens misteriosas e indecifráveis. A escrita secreta era interpretada como um hábito estranho, que teria ligação com forças do mal e era usada nos tribunais civis e religiosos como peças de incriminação em processo de toda natureza. Os escassos sinais históricos do uso da criptografia, no início da idade Média, referem-se a hábitos de monges utilizando-a em escritas, como forma de passatempo e diversão ou, ainda, em sociedades religiosas.

Os primeiros sinais de ressurgimento da criptografia ocorreram com a Idade de Ouro da civilização árabe, que teve início por volta do ano 750. Pouco interessados em promover guerras de conquistas, as Califas Árabes favoreceram o desenvolvimento das ciências, do comércio e da indústria, e desenvolveram uma administração eficaz, utilizando a criptografia na segurança de suas comunicações.

O nascimento da criptoanálise ocorreu nesta época com a descoberta do "**método da análise de frequências**". A análise de frequências explora uma fraqueza fundamental nas mensagens codificadas por meio de cifras monoalfabéticas: as diferentes frequências com que aparecem os vários símbolos. Não se sabe ao certo quem, pela primeira vez propôs o método. Para Costa e Figueiredo (2006), o primeiro registro aparece no livro "Escritos sobre a decifração de mensagens criptográficas", do sábio árabe al-Kindy. Este feito árabe marca o início efetivo da criptoanálise e coloca os decodificadores na frente dos codificadores.

Segundo Costa e Figueiredo (2006), a Itália foi um dos primeiros países a ver com profissionalismo e como questão de estado o uso da criptografia. Este momento da história italiana, por volta de 1300, coincidiu com as primeiras manifestações do Renascimento. O governo italiano cria um órgão ligado diretamente ao centro do poder, dedicado exclusivamente ao estudo da criptografia, com o objetivo de decifrar as mensagens dos inimigos e aperfeiçoar os métodos de cifragem. Era uma época em que a Europa estava perto de uma revolução no campo das idéias, que influenciou definitivamente o desenvolvimento posterior das ciências, das artes, da política e a visão estabelecida do mundo. Durante toda a

Idade Média, a Europa usou velhas técnicas criptográficas, embora os árabes tenham demonstrado a fragilidade destes métodos diante da análise de frequências. A reação da criptografia, com a criação de novos métodos para escapar à análise de frequências, só ocorreria na aurora da Idade Moderna, coincidindo com o início do Renascimento. Este tempo é também marcado pelo nascimento da Imprensa e a conseqüente mecanização da escrita, que influenciaria fortemente o desenvolvimento posterior da criptografia.

2.4. Criptografia na Idade Moderna

A Idade Moderna é marcada pelo início do movimento renascentista na Itália, em 1450, e vai até o fim do século XIX. O renascimento abre uma era de grande desenvolvimento das ciências e das artes, causando impacto na economia e na política.

No ano de 1450, a Itália figura como palco ideal para o desenvolvimento da criptografia. Colocada no epicentro do movimento que criou a Renascença, a Itália era constituída de cidades-estados independentes, cada uma buscando sua hegemonia, de forma que grande parte da correspondência política, econômica e militar era altamente sensível e necessitava de proteção.

Segundo Costa e Figueiredo (2006), conscientes da fragilidade dos códigos monoalfabéticos, frente à análise de frequências, a primeira reação européia foi de Crema, em 1452, com os **"códigos de substituição homofônica"**. Trata-se de uma cifra construída fazendo corresponder cada letra do alfabeto a um conjunto de símbolos diferentes (podendo ser, inclusive, as próprias letras permutadas), de forma que a quantidade de símbolos associados a cada letra corresponde ao nível de frequência estatística com que esta letra aparece em textos longos.

O primeiro grande nome da criptoanálise da Europa foi Giovanni Soro, que assumiu seu posto em Veneza no ano de 1506. Sua capacidade em decifrar mensagens marcou o período. Em Viena, a partir do ano de 1750, prosperou a mais organizada e eficiente "câmara negra" da Europa (uma secretaria dentro do governo com o objetivo de lidar com a escrita secreta, solucionando e criando cifras), liderada por Barão Ignaz von Koch. Toda correspondência nacional ou internacional que chegava ou saía de Viena passava antes pela câmara. As cartas eram violadas e entregues a um batalhão de copistas. Em seguida, o selo era reconstituído e a carta, enviada ao destinatário. A mensagem copiada era entregue a outra equipe de criptoanalistas. Viena se tornou tão eficiente neste setor que vendeu serviço às nações aliadas da Europa.

Na França, o primeiro nome ilustre foi Babou, nomeado decifrador de François I. Depois surge o matemático Viète, como o criptologista de Henri IV. No entanto, finalizando um ciclo, o mais renomado entre os franceses foi Antoine Rossignol (1600-1682), que se tornou célebre por seus trabalhos para Richelieu. Rossignol e seu filho Bonaventure elaboraram a **Grande Cifra** de Luís XIV, a qual mais tarde foi usada por Napoleão em suas campanhas militares. A Grande Cifra, muito robusta, era homófona e trabalhava com mais de 500 números. Cada grupo de números era associado a uma sílaba de língua francesa. Após a morte de Antoine e seu filho, a cifra caiu em desuso e suas regras foram perdidas. Ela foi quebrada em 1870 pelo militar francês Bazeris, que procurava desvendar dados históricos dos tempos de Rossignol. Bazeris trabalhou durante três anos para conseguir decifrá-la.

Uma alternativa à fragilidade das cifras homofônicas começou a ser desenvolvida por Leon Battista Alberti, em 1470, com a criação da primeira cifra polialfabética. Além disso, Alberti introduziu um princípio de mecanização no processo, criando um disco de cifragem. Os **discos de Alberti** tratavam-se de dois discos concêntricos. O disco externo é fixo e suas letras representam as letras da mensagem original. O disco interno pode girar sobre o eixo e suas letras servem para encriptar a mensagem. Ao girar o disco interno, é possível definir 26 posições distintas de coincidências de letras entre o disco externo e o interno. Portanto, o disco interno é girado quantas vezes necessário, segundo a indicação da chave, esta indicando as correspondências do disco externo com o interno na sequência de utilização das posições.

Apesar de representar o primeiro avanço significativo em um período de quase 800 anos, Alberti não foi capaz de aprofundar sua idéia e organizar uma cifra que pudesse resistir à análise de frequências. Em 1523, Blaise de Vigenère publica o livro "Tratado das cifras", no qual aprofunda as idéias de Alberti, criando uma nova cifra que permaneceria indecifrável durante quase toda a Idade. A **cifra de Vigenère** consiste em usar vários discos de Alberti simultaneamente, de acordo com uma palavra-chave. O número de discos para cifrar a mensagem é igual ao comprimento da palavra-chave, enquanto que as posições iniciais de cada disco são definidas por cada uma das letras da palavra. No entanto, apesar de Ter sido uma cifra poderosa, A Europa não a utilizou intensivamente devido a sua complexidade e à fraca mecanização da escrita e da comunicação. Ela seria usada com regularidade apenas 200 anos mais tarde, por volta de 1760. Porém em 1854, a cifra de Vigenère, considerada indecifrável, foi quebrada por Babbage, o que representou uma realização extraordinária da criptoanálise, sendo o primeiro resultado relevante depois da criação da análise de frequência pelos árabes, mil anos antes. De modo independente e nove anos depois, Friedrich Wilhelm Kasiski, um oficial da infantaria prussiana, repetiu o mesmo feito de Babbage. Com a quebra

da Cifra de Vigenère, a idade Moderna termina como começou: os criptógrafos em desvantagem e em busca de uma nova cifra que pudesse restabelecer a comunicação secreta.

Em 1844, Samuel Morse desenvolve o código que recebeu seu nome e inventa o telégrafo. A invenção alterou profundamente a criptografia e as comunicações, fazendo da cifragem uma necessidade quase absoluta, mesmo para o público em geral, que se utilizavam da criptografia para proteger segredos sentimentais e comerciais de relativa importância do próprio operador do telégrafo, que precisava ler a mensagem antes de transmiti-la em código morse. Em 1894, o físico italiano Guglielmo Marconi começou a realizar experiências com circuitos elétricos e descobriu que, sob certas condições, um circuito elétrico percorrido por uma corrente elétrica pode induzir uma corrente em outro circuito isolado a alguma distância do primeiro. O projeto dos dois circuitos é aperfeiçoado com uso de antenas. Marconi foi capaz de transmitir e receber pulsos elétricos a grande distância e deu os primeiros passos na criação de uma nova e mais poderosa ferramenta de comunicação, o rádio, um sistema de comunicação rápido, eficiente e sem fios, com o sinal viajando pelo ar, à longa distância, mas fracamente aberto, impondo imensos desafios à proteção da informação e provocando ainda maior necessidade de uma comunicação segura.

2.5. Criptografia na atualidade

Para Costa e Figueiredo (2006), a criptografia moderna é basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores, dividindo-se em dois grandes grupos: criptografia de chave simétrica e criptografia de chave assimétrica. Com o passar do tempo, com o aumento da capacidade computacional, foi possível utilizar complexos esquemas criptográficos, antes impraticáveis, permitindo maior velocidade nos processos de encriptação e decriptação de mensagens.

A era da criptografia moderna começou realmente com Claude Shannon, possivelmente o pai da criptografia matemática, quando, em 1949, publicou um artigo com Warren Weaver, "Communication Theory of Secrecy Systems". Este artigo, junto com outros de seus trabalhos, que criaram a área de Teoria da Informação, estabeleceu uma base teórica sólida para a criptografia e para a criptoanálise. Depois disso, quase todo o trabalho realizado em criptografia se tornou secreto, realizado em organizações governamentais especializadas (como o NSA nos Estados Unidos). Apenas, em meados de 1970, as coisas começaram a mudar.

Em 1976 aconteceu dois grandes marcos da criptografia para o público. O primeiro foi a publicação, pelo governo americano, do DES (Data Encryption Standard), um algoritmo aberto de criptografia simétrica, selecionado pela NIST em um concurso onde foi escolhido uma variante do algoritmo Lucifer, proposto pela IBM. O DES foi o primeiro algoritmo de criptografia disponibilizado abertamente ao mercado. O segundo foi a publicação do artigo "New Directions in Cryptography", por Whitfield Diffie e Martin Hellman, que iniciou a pesquisa em sistemas de criptografia de chave pública. Este algoritmo ficou conhecido como "Algoritmo Diffie-Hellman para troca de chaves" e levou ao imediato surgimento de pesquisas neste campo, que culminou com a criação do algoritmo RSA, por Ronald Rivest, Adi Shamir e Leonard Adleman.

A Primeira Guerra Mundial teve início em julho de 1914, quando o império austro-húngaro declarou guerra à Sérvia. Neste conflito, a mais famosa cifra em uso, utilizada pelas tropas alemães, foi a **ADFGVX** obtida com uma combinação de técnicas de substituição e transposição. Ela foi quebrada pelo criptoanalista Georges Pavin, em junho de 1918, garantindo à França e seus aliados vantagem contra os ataques alemães.

A primeira **máquina de cifras** alemã, denominada Enigma, foi desenvolvida em 1918, pelo engenheiro alemão Arthur Scherbius, com o objetivo de facilitar a troca de documentos secretos entre comerciantes e homens de negócios. Apesar de não ter conseguido empolgar o setor, mais tarde, a invenção se torna interessante para uso militar, se tornando um marco na Segunda Guerra Mundial. O governo alemão adquire o direito de utilização da Enigma e o exército redesenha a máquina, começando a usá-la em junho de 1930, com o nome de Enigma I. Ela lembra uma máquina de escrever e era construída de um teclado com 26 letras, um painel luminoso, uma câmara com três misturadores, um refletor e um painel frontal com cabos elétricos. A chave para utilização da Enigma dependia de uma configuração de montagem, que compreendia a ordem e a posição dos misturadores, conexão dos cabos emparelhando duas letras no painel frontal e a posição do refletor. Para cifrar uma mensagem, o operador teclava uma letra e o comando estimulava o circuito elétrico, de forma que as letras cifradas apareciam, uma a uma, no painel luminoso, sendo então anotadas para compor a mensagem secreta. A máquina Enigma foi a ferramenta criptográfica mais importante da Alemanha nazista e os alemães apostavam em sua eficiência para vencer a guerra. Ela trabalhava com um processo de cifragem complexo e de chave simétrica e, por questões de segurança, a cada mensagem a chave era trocada.

Durante a Segunda Guerra Mundial, os britânicos superaram os alemães, pois decifram todos os códigos nazistas. A cifra começou a ser quebrada pelo matemático

polônês Marian Rejewski, cujo esforço inicial foi baseado em textos cifrados interceptados e em uma lista de três meses de chaves diárias obtidas por meio de um espião. A partir de 4 de Setembro de 1939, Alan Turing integra-se à equipe de Bletchley Park, na Inglaterra, e, em conjunto com Gordon Welchman, constrói um computador eletromecânico denominado **The Bombe** (Máquina de Turing), utilizando os princípios que tinha enunciado, em 1936, para a sua Máquina Universal. Para apoiar essa atividade foi lançado um projeto com o nome de código Robinson, supervisionado pelo Professor Max Newman, cujo objetivo era a construção de um computador eletrônico. O computador foi construído no Post Office Research Laboratories, em Dollis Hill, no Norte de Londres, por uma equipe liderada pelo Dr. Tommy Flowers. O computador foi denominado **Colossus** e entrou em funcionamento em Dezembro de 1943. Ele era constituído por uma unidade de leitura de fita de 5 canais que funcionava com uma velocidade de 5.000 caracteres por segundo, uma unidade de saída construída com um teletipo, 2.500 válvulas e era um computador paralelo assíncrono. A velocidade do Clock (5kc/s) era regulada pela leitura da fita perfurada. Introduzida no leitor, a fita perfurada que continha a mensagem alemã cifrada, o Colossus demorava cerca de duas horas a determinar qual a combinação que tinha sido utilizada para cifrá-la. Determinada a combinação, a mensagem era introduzida numa "Tunny machine" que, de imediato, revelava o texto decifrado. Até o final da guerra funcionaram em Bletchley Park 10 computadores Colossus. A Colossus era uma máquina mais elaborada pois possuía a característica de ser programável, o que a referenciou como a primeira e mais primitiva de uma linha de máquinas que evoluíram para os computadores.

Na criptografia mecânica era fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da máquina que produzia a cifragem. Com o desenvolvimento e aperfeiçoamento dos computadores e a necessidade de uso da criptografia pelo comércio e bancos, os algoritmos criptográficos passaram a ser de conhecimento público e o segredo a residir exclusivamente na chave.

Em 1974, a IBM apresenta à agência oficial americana NBS (National Bureau of Standards) uma cifra de criptografia simétrica, concebida para implementação em um computador, que alguns pesquisadores vinham desenvolvendo desde 1960, a fim de atender a demanda dos bancos. A NBS, após avaliar o algoritmo com a ajuda da NSA (National Security Agency), adota o código como padrão de cifragem de dados para os Estados Unidos. O código passou a ser conhecido como **DES** (Data Encryption Standard) e marca o princípio da criptografia digital.

Até esse momento, a criptografia era baseada em chaves privadas. Um processo de comunicação secreta com chave privada necessita de um canal especial de comunicação em paralelo, seguro o suficiente para a prévia troca de chaves entre o remetente e o destinatário, o que configura a principal fragilidade dos algoritmos criptográficos de chave simétrica. A resposta a esse problema foi encontrada pela dupla de pesquisadores Whitfield Diffie e Martin Hellman, em 1976, na Universidade de Stanford. O resultado obtido pelos pesquisadores, publicado no livro "New Directions in Cryptography", conhecido como o **algoritmo DH (Diffie-Hellman)**, introduzia a possibilidade do **conceito de chave pública**, solucionando o problema da troca de chaves, mas não provendo encriptação. Tratava-se de uma construção teórica, aparentemente, sem apontar possibilidades de realização prática, mas que conduziu à invenção da criptografia assimétrica.

Ron Rivest, um professor da MIT (Massachusetts Institute of Technology), juntamente com Adi Shamir e Len Adleman criaram, em 1977, um ano após a publicação de Diffie-Hellman sobre a troca de chaves, um algoritmo para encriptação de dados. O algoritmo recebe o nome de **RSA**, as iniciais de seus inventores. Em 1985, Neal Koblitz e Victor Miller, propuseram uma implementação de criptografia de chave pública usando as propriedades das curvas elípticas, conhecido como **ECDH**. O algoritmo desenvolvido por Koblitz e Miller é mais complexo do que o algoritmo RSA e fornece maior segurança por bit dentre os algoritmos conhecidos hoje. Além da garantia de confidencialidade, a criptografia assimétrica permitiu ainda outras inovações revolucionárias como a possibilidade de assinatura digital.

Os algoritmos de chave assimétrica têm a desvantagem de serem pesados e muito mais lentos que os algoritmos de chave simétrica. A combinação das duas técnicas surgiu para atenuar esta dificuldade e esta técnica ficou conhecida como **criptografia híbrida**. A solução mais famosa de uso da criptografia híbrida foi inventado por Philip R. Zimmermann e representou um marco na popularização da criptografia. Philip se empenhou em encontrar uma saída na implementação do algoritmo RSA ou uma modificação dele em computadores pessoais. Trabalhou intensamente no projeto em 1984. Em junho de 1991, Zimmermann liberou a primeira versão do programa que iria se tornar o cavalo de batalha da criptografia para as massas. Denominou seu sistema de o **PGP (Pretty Good Privacy)**. Diante do dilema de uma demorada negociação com os detentores da patente do RSA e temeroso de que o uso popular de programas de criptografia por chave pública terminasse sendo proibido por imposição da NSA, Philip liberou gratuitamente o código-fonte do PGP para uso do público em geral. O PGP espalhou-se rapidamente em todo planeta. A reação da NSA foi imediata, processando Philip por usar nas rotinas internas do PGP o algoritmo patentado RSA. A

argumentação de Philip se baseou no fato de não haver cobrado pelo PGP e que a distribuição seguiu a tradição acadêmica de divulgação dos resultados de um projeto de pesquisa científica.

O desenvolvimento da técnica reunindo o conceito de **criptografia** e a **teoria quântica** é mais antigo do que se imagina, sendo anterior à descoberta da criptografia de Chave Pública. Stephen Wiesner escreveu um artigo por volta de 1970 com o título: "Conjugate Coding" que permaneceu sem ser publicado até o ano de 1983. Em seu artigo, Wiesner explica como a teoria quântica 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, pela impossibilidade de violar uma lei da natureza (o princípio de incerteza de Heisenberg). A partir do início de 1990, é quando começa o trabalho de pesquisa para a construção de computadores quânticos e o desenvolvimento de uma criptografia quântica. Os primeiros ensaios experimentais são publicados por Charles H. Bennett, Gilles Brassard e colaboradores, relatando o uso de fótons para transmitir um fluxo de bits.

As cifras são implementadas através de algoritmos. Segundo as definições apresentadas por Putini e Júnior (2000), algoritmos criptográficos são funções matemáticas usadas para codificar os dados, garantindo sigilo e autenticação. A operação do algoritmo funciona ter como parâmetro uma chave (secreta), em sua maioria, secreta, que consiste de longas sequências de números e/ou letras. Quanto maior for o tamanho da chave maior será o grau de confidencialidade da mensagem, pois dificulta a sua descoberta por meios criminosos. Alguns exemplos de cifras são:

1. Cifras de Transposição: o conteúdo da mensagem é o mesmo, porém com os caracteres postos em ordem diferente. Se a sequência dos caracteres for a mesma do idioma, denomina-se substituição por transposição, caso contrário por substituição.
2. Cifras de Substituição: neste método troca-se cada caractere ou grupo de caracteres de acordo com uma tabela de substituição. Subdividem-se em:

- *Monocriptográfica*, denominada também de Cifra de César. Caracteriza-se pela substituição na ordem de 1 por 1, onde cada caractere é substituído por outro, de acordo com uma tabela pré-estabelecida.

- *Policriptográfica*: consiste em utilizar várias cifras de substituição simples, porém com valores diferentes. Ou seja, substitui o texto de acordo com várias tabelas.

Capítulo 3 – Conceitos Gerais

3.1. Cifras e Códigos

Historicamente, a criptografia é dividida entre códigos e cifras, usando para ambas a mesma terminologia (codificar, decodificar, etc...). Na linguagem não-técnica, um código secreto é o mesmo que uma cifra. Porém, na linguagem especializada, os dois conceitos são distintos. Um código funciona no nível do significado, normalmente pela substituição simples de palavras ou frases, não envolvendo chave criptográfica, apenas tabelas de substituição ou mecanismos semelhantes. Uma cifra, ao contrário, trabalha no nível dos símbolos (letras, grupos de letras ou bits). O conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original.

Atualmente, apenas as cifras são de interesse teórico, devido ao fato de suplantarem em eficiência o uso de códigos. A principal vantagem das cifras em relação aos códigos é a não limitação das possíveis mensagens a serem enviadas ao destinatário, além de se tornarem mais difíceis de serem decifradas.

As cifras são implementadas através de algoritmos. Segundo as definições apresentadas por Puttini e Júnior (2000), algoritmos criptográficos são funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. A operação do algoritmo costuma ter como parâmetro uma chave (senha), em sua maioria secreto, que consiste de longas sequências de números e/ou letras. Quanto maior for o tamanho da chave maior será o grau de confidencialidade da mensagem, pois dificulta a sua descoberta por teste exaustivo. Alguns exemplos de cifras são:

1. **Cifras de Transposição:** o conteúdo da mensagem é o mesmo, porém com os caracteres postos em ordem diferente. Se a frequência dos caracteres for a mesma do idioma, denomina-se substituição por transposição, caso contrário por substituição.
2. **Cifras de Substituição:** neste método troca-se cada caractere ou grupo de caracteres de acordo com uma tabela de substituição. Subdividem-se em:
 - *Monoalfabética:* denominada também de Cifra de César. Caracteriza-se pela substituição na ordem de 1 por 1, onde cada caractere é substituído por outro, de acordo com uma tabela pré-estabelecida.
 - *Polialfabética:* consiste em utilizar várias cifras de substituição simples, porém com valores diferentes. Ou seja, substitui o texto de acordo com várias tabelas.

- *Polígramos*: conhecido também por Máquinas de cifragem. Este método trabalha com grupos de caracteres de tamanho variável, onde cada palavra é substituída por outra. Quebrar um código deste equivale a quebrar uma gigantesca substituição monoalfabética onde as unidades são as palavras, e não mais os caracteres.

3.2. Criptografia Simétrica

Neste tipo de criptografia, utiliza-se uma chave secreta para criptografar os dados. A chave simétrica é uma sequência de bits e é ela que define o nível de segurança da comunicação. Chama-se simétrica porque todos os interessados em se comunicar devem ter uma cópia da mesma chave.

Um exemplo de uso de chave simétrica é o código de César. Neste método, a chave é definida por um número, e é utilizada para cifrar e decifrar a mensagem. As duas partes, o emissor e o destinatário, conhecem a chave. Este sistema de comunicação coloca toda a segurança do processo sobre a chave e nenhuma sobre o algoritmo.

Existem dois tipos de criptografia simétrica: **cifras de bloco** e **cifras de fluxo**. A criptografia de cifras de bloco opera em blocos de dados, com um número fixo de bits (geralmente 64 bits nas cifras modernas) como unidades de cifragem, e os algoritmos utilizados na sua maioria utilizam a permutação, com o objetivo de causar difusão. Quanto à criptografia de cifras de fluxo, ela opera em unidades menores, geralmente bits, o que a torna bem mais rápida. Por ser bastante simples, ela é implementada com menos código, porém tem a desvantagem de não se poder reutilizar a chave, necessitando assim de geradores randômicos de chaves para sua utilização.

Para Puttini e Júnior (2000), uma das vantagens dos algoritmos de criptografia simétrica é serem rápidos na velocidade dos processos de encriptação e deciptação, por serem computacionalmente mais simples, porém existe um grande problema que é a distribuição da chave privada para os destinatários, a qual ocasiona um nível de segurança baixo.

A comunicação utilizando cifras simétricas exige os seguintes passos:

1. Alice e Bob combinam uma cifra.
2. Alice e Bob acordam uma chave.
3. Alice cifra a mensagem e envia-a a Bob.
4. Bob decifra a mensagem.

Como a criptoanálise de uma cifra é geralmente muito difícil, os ataques centram-se muitas vezes nos dois primeiros passos. É por este motivo que a gestão de chaves é um problema muito importante em Criptografia. A chave tem de permanecer secreta antes, durante e depois da comunicação.

Para solucionar o problema do compartilhamento de chaves entre as pessoas envolvidas, foi criado um centro de distribuição de chaves (Key Distribution Center - KDC). Este centro é responsável pela comunicação entre as pessoas, tendo armazenado em sua base de dados todas as chaves privadas dos usuários que utilizam seus serviços. Embora isto gere outro problema, que é centralização de chaves privadas em um único lugar, podendo, casualmente, ser corrompidas por pessoas maliciosas que tenham acesso a base de dados.

3.2.1. Cifras de blocos

As cifras de blocos são fundamentais aos sistemas criptográficos, não apenas para garantir confidencialidade, mas também como componentes na construção de funções de hash, geradores de números pseudoaleatórios, ou Message Authentication Codes. Os algoritmos de cifragem de blocos mais conhecidos são o DES (Data Encryption Standard), DES Triplo, IDEA (International Data Encryption Algorithm), Skipjack, CAST-128, RC5, Blowfish, AES.

O principal componente destas cifras é uma função de cifragem polialfabética pura, que trabalha sobre blocos de tamanho fixo (tradicionalmente 64 bits, mas hoje em dia 128 ou mais bits). Associadas à função de cifragem, são necessárias unidades de partição e padding (enchimento garantindo que o texto limpo tenha tamanho múltiplo do tamanho do bloco), para produzir blocos de tamanho apropriado a partir do texto limpo. Na decifragem, a função inversa da função de cifragem é aplicada aos blocos do criptograma e os processos de padding e partição são posteriormente revertidos para recuperar o texto limpo.

As cifras por blocos devem ter as seguintes características:

- Cada bit do criptograma deve depender de todos os bits da chave e de todos os bits do texto limpo.
- Não deve haver nenhuma relação estatística evidente entre os bits do texto limpo e os bits do criptograma.
- A alteração de um bit do texto limpo ou da chave deve alterar cada bit do criptograma com uma probabilidade de $1/2$.

- A alteração de um bit do criptograma deve originar uma alteração imprevisível no texto decifrado.

Existem diversas formas de utilização da cifra por blocos. Se o texto original possuir blocos de textos que se repetem com muita frequência, no momento da codificação, produzirá o mesmo pedaço de texto cifrado, sendo um meio do criptoanalista quebrar o código. Para evitar o reconhecimento de padrões repetidos no texto cifrado, usa-se o que os criptologistas chamam de "Modo de Realimentação". Os critérios que levam ao aparecimento destas variantes são: segurança, eficiência, propagação de erros/tolerância aos erros, adequação do "throughput" do modo de funcionamento (dependente do tamanho dos blocos) às necessidades da aplicação.

Os modos de utilização mais comuns são:

- Electronic Code Book Mode (ECB)
- Cypher Block Chaining Mode (CBC)
- Cypher Feedback Mode (CFB)
- Output Feedback Mode (OFB)

Cada modo de funcionamento se adequa a uma situação específica. O ECB é muito utilizado para cifrar pequenas parcelas de informação aleatórias, como chaves. Para este tipo de informação as falhas de segurança deste modo não são relevantes. O CBC é o modo de funcionamento recomendado para aplicações genéricas. É muito utilizado para cifrar ficheiros, onde os erros são pouco frequentes. É a melhor escolha para aplicações baseadas em software. O CFB e o OFB servem para aplicações onde é necessária uma cifra seqüencial. E o OFB é preferido quando o meio de transmissão introduz muitos erros.

Os modos mais antigos descritos na literatura, como os descritos acima, provêm somente confidencialidade e não assegura integridade da mensagem. Outros modos foram desenvolvidos desde então para assegurar tanto a confidencialidade quanto integridade da mensagem, tais como os modos IAPM, CCM, EAX, GCM e OCB. O modo configurável de bloco estreito (LRW) e os modos de encriptação de bloco largo (CMC e EME), foram projetados para encriptar setores de disco com segurança.

3.2.1.1. Electronic Code Book Mode (ECB)

É o modo mais simples de encriptação. A mensagem é dividida em blocos e cada bloco é encriptado separadamente. A figura 1 apresenta um esquema do seu funcionamento.

Neste modo, os padrões existentes no texto limpo não são disfarçados. Um bloco cifrado duas vezes com a mesma chave resulta em criptogramas iguais. Ele é susceptível a ataques por code book (compilação de pares texto limpo/criptograma) e a ataques por remoção, troca e repetição de blocos. Além disso, permite o acesso aleatório a dados cifrados, de forma que qualquer bloco pode ser decifrado independentemente. Pela mesma razão, permite o processamento paralelo da informação, porém não há possibilidade de efetuar pré-processamento.

Quanto à tolerância a erros, este modo não apresenta problemas de propagação de erros entre blocos. Um erro afeta apenas um bloco de texto limpo. Porém, erros de sincronização (perda de bits) são irreversíveis.

No geral, o modo ECB não oferece uma perfeita confidencialidade de mensagem, e não é recomendado para uso em protocolos criptográficos em geral.

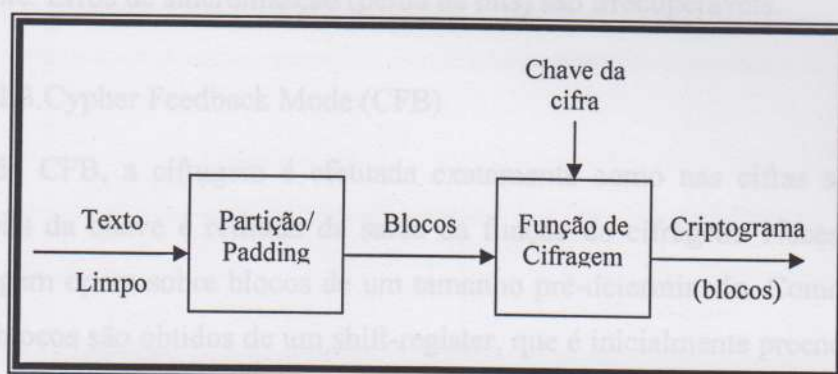


Figura 1. Esquema de funcionamento do modo ECB

3.2.1.2. Cypher Block Chaining Mode (CBC)

No modo de criptografia CBC, como apresentado na figura 2, o primeiro bloco é combinado com um Vetor de Inicialização (VI), tipicamente aleatório, através de um XOR. Os blocos que se seguem recebem como VI o resultado da criptografia do bloco anterior. O VI não tem de ser secreto e tem de estar disponível na decifragem. Como os padrões do texto limpo são mascarados pela operação XOR, blocos de texto limpo iguais passam a resultar criptogramas distintos, impedindo ataques por code book e ataques por repetição, também garantindo que ataques por manipulação de blocos sejam, em grande parte, detectáveis.

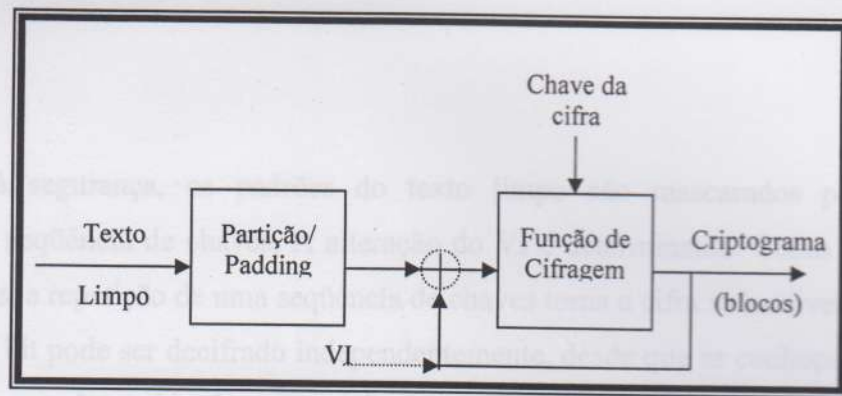


Figura 2. Esquema de funcionamento do modo CBC

Qualquer bloco pode ser decifrado independentemente, desde que se conheça o bloco anterior. Pela mesma razão, permite o processamento paralelo da informação cifrada (não aplicável na cifragem). No entanto, uma alteração ao texto limpo, como em um ficheiro, implica uma nova cifragem completa. Ele permite o acesso aleatório a dados cifrados e não há possibilidade de efetuar pré-processamento.

Um erro num bit do criptograma afeta o bloco de texto limpo correspondente, e um bit no bloco seguinte. Erros de sincronização (perda de bits) são irre recuperáveis.

3.2.1.3. Cypher Feedback Mode (CFB)

No modo CFB, a cifragem é efetuada exatamente como nas cifras sequenciais. A sequência de bits da chave é retirada da saída da função de cifragem. Necessariamente, a função de cifragem opera sobre blocos de um tamanho pré-determinado. Como mostrado na figura 3, esses blocos são obtidos de um shift-register, que é inicialmente preenchido com um VI. Os bits do criptograma vão substituindo os bits do VI, que deve ser aleatório para originar seqüências de chaves e criptogramas diferentes em cifragens sucessivas, não precisando ser secreto. A função de cifragem é usada da mesma forma na cifragem e decifragem. Na realidade, a função inversa não é necessária neste modo de funcionamento.

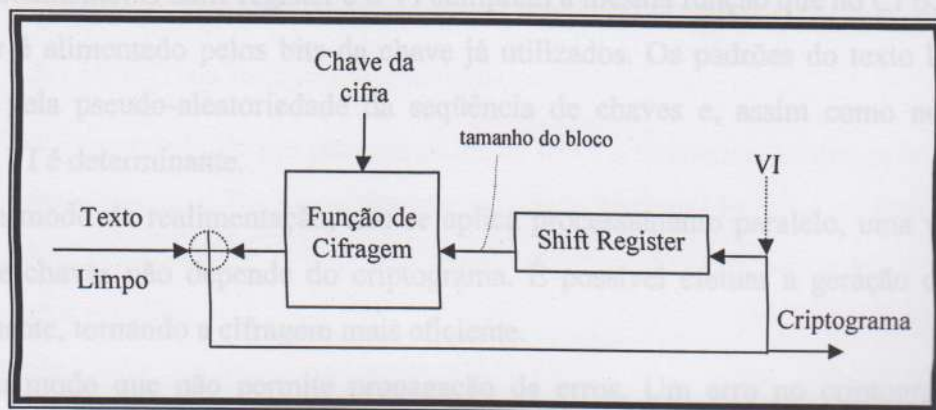


Figura 3. Esquema de funcionamento do modo CFB

Quanto à segurança, os padrões do texto limpo são mascarados pela pseudo-aleatoriedade da sequência de chaves. A alteração do VI é determinante. Como em todas as cifras sequenciais, a repetição de uma sequência de chaves torna a cifra vulnerável a ataques.

Qualquer bit pode ser decifrado independentemente, desde que se conheça um número suficiente de bits anteriores do criptograma. Permite o acesso aleatório a dados cifrados. Pela mesma razão, permite o processamento paralelo da informação cifrada (não aplicável na cifragem). Há possibilidade de efetuar algum pré-processamento dos bits da chave. É uma cifra auto-sincronizável. Os erros de sincronização (perda de bits) são recuperáveis em determinadas condições. Um erro no criptograma tem como efeito imediato uma decifragem errada do bit de texto limpo correspondente. Enquanto o bit errado estiver no shift-register, o sistema vai debitar lixo.

3.2.1.4. Output Feedback Mode (OFB)

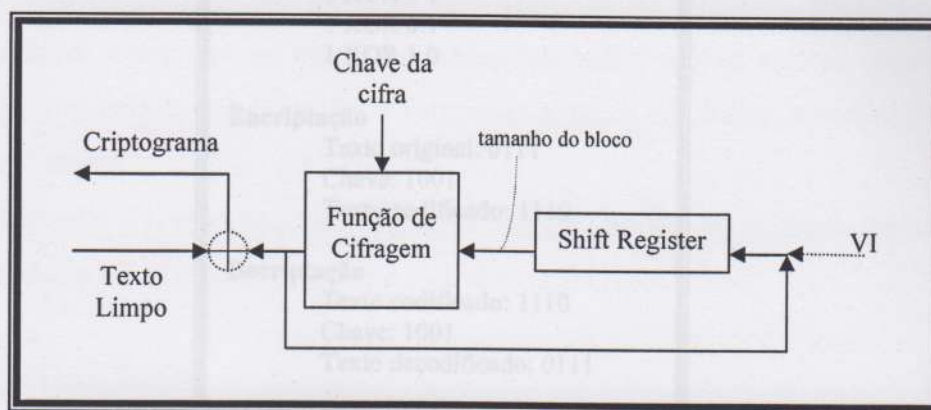


Figura 4. Esquema de funcionamento do modo OFB

O OFB corresponde a uma cifra sequencial síncrona. A figura 4 apresenta o esquema de seu funcionamento. O shift-register e o VI cumprem a mesma função que no CFB, porém o shift-register é alimentado pelos bits da chave já utilizados. Os padrões do texto limpo são mascarados pela pseudo-aleatoriedade da sequência de chaves e, assim como no CFB, a alteração do VI é determinante.

Neste modo de realimentação, não se aplica processamento paralelo, uma vez que a sequência de chaves não depende do criptograma. É possível efetuar a geração de chaves antecipadamente, tornando a cifragem mais eficiente.

É um modo que não permite propagação de erros. Um erro no criptograma afeta apenas um bit no texto limpo. Porém, erros de sincronização não são recuperáveis.

3.2.2. Cifras de fluxo

A grande maioria dos algoritmos criptográficos atuais são cifras de bloco. As cifras de fluxo, ou cifras seqüenciais, ainda são objeto de pesquisa e têm uma aplicação prática muito discreta. O motivo é que as cifras de fluxo dependem de geradores randômicos de chaves que, apesar da aparente simplicidade, são difíceis de implementar através de software ou de hardware. As cifras de fluxo funcionam basicamente convertendo o texto claro em texto cifrado bit a bit.

Um algoritmo que implementa a cifragem de fluxo é o RC4, que é o utilizado no protocolo SSL (Secure Socket Layer). O exemplo mais simples de cifras em fluxo é a encriptação usando XOR (Ou Exclusivo - operador bitwise - bit a bit), conforme apresentado na Figura 5.

0 XOR 0 0
0 XOR 1 1
1 XOR 0 1
1 XOR 1 0
Encriptação
Texto original: 0111
Chave: 1001
Texto codificado: 1110
Deciptação
Texto codificado: 1110
Chave: 1001
Texto decodificado: 0111

Figura 5. Exemplo de aplicação de encriptação por Cifra de Fluxo

3.2.3. Algoritmos simétricos

3.2.3.1.DES (Data Encryption Standard)

O DES foi desenvolvido por pesquisadores da IBM, e adotado para uso governamental em 1977 pelo então National Bureau of Standards, hoje o National Institute of Standards and Technology (NIST). Sua adoção pelo governo norte-americano naturalmente levou a seu uso também pelo setor privado.

É um algoritmo simétrico que opera sobre blocos de 64 bits. Seu funcionamento básico consiste na criptografia de blocos de 64 bits de entrada com uma chave de 56 bits,

gerando blocos de 64 bits como saída. Para obter o texto original novamente, reverte-se o processo usando a mesma chave.

O DES realiza a criptografia em 18 estágios, basicamente através dos seguintes passos:

1. Uma substituição fixa, chamada de permutação inicial, de 64 bits em 64 bits, que não influi diretamente na segurança do DES, mas é executada com o propósito de facilitar o uso do algoritmo em chips quando é implementado em hardware;

2. Execução de uma função F , por 16 vezes. Na entrada desta função são recebidas duas metades do bloco de 64 bits (metade esquerda e metade direita) e uma subchave de 48 bits (transformação da chave de 56 bits). As duas metades do texto fonte são criadas antes da primeira volta, no passo anterior, e ao final da última volta, essas metades são reunidas novamente no passo seguinte;

3. Inversão da permutação inicial.

A decifragem consiste de um processo semelhante ao da cifragem. Para se obter o dado decriptografado, basta que se façam as interações utilizando as chaves com ordem invertida, ou seja, partindo da 16ª chave na 1ª interação, e assim em diante, até chegar na 1ª interação com a 1ª chave.

Atualmente, não é considerado um algoritmo seguro, devido ao pequeno tamanho de sua chave, que poderia ser quebrado com certa facilidade pela força bruta.

3.2.3.2.DES-Triplo

Por causa da relativa fragilidade do DES a ataques, nos últimos tempos foi adotado um variante de DES, chamado DES-triplo, que aplica o algoritmo DES três vezes, com três chaves diferentes, que equivale a uma única chave de 168 bits.

3.2.3.3.IDEA (International Data Encryption Algorithm)

Criado por volta de 1990, em Zurique na Suíça, por James Massey e Xuejia Lai, o IDEA é um algoritmo simétrico de bloco, que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES. É utilizado no software PGP (Pretty Good Privacy) de correio eletrônico seguro.

Originalmente, o IDEA foi chamado de PES (Proposed Encryption Standard). Um ano após o seu lançamento, em 1991, Biham e Shamir demonstraram que o algoritmo era susceptível à criptoanálise diferencial e os autores fizeram modificações substanciais.

Chamaram o novo algoritmo de IPES (Improved Proposed Encryption Standard). Em 1992, o IPES foi rebatizado transformando-se no IDEA. Atualmente, visando sua disseminação, foi autorizado o uso não comercial do algoritmo.

O método utilizado por este algoritmo visa misturar operações de grupos algébricos diferentes, possuindo três grupos algébricos cujas operações são misturadas. Estas operações, que podem ser facilmente implementadas via hardware e/ou software, são:

1. XOR
2. Adição módulo 2^{16} (adição ignorando qualquer overflow)
3. Multiplicação módulo $2^{16}+1$ (multiplicação ignorando qualquer overflow)

Todas estas operações são feitas com blocos de 16 bits, o que faz com que este algoritmo também seja eficiente em processadores de 16 bits.

3.2.3.4. Rijndael

Em 1997, o NIST lançou um concurso para selecionar um novo algoritmo, para ser adotado como o AES (Advanced Encryption Standard), em substituição ao DES e DES-triplo, cujo ganhador foi o algoritmo Rijndael.

Rijndael é a criação de dois recém doutores belgas, Joan Daemen e Vincent Rijmen, cuja nomeação tem origem no nome de seus criadores. Ele foi projetado para usar somente simples operações de bytes completos, podendo utilizar chaves de 128, 192 e 256 bits.

Não contando um estágio extra-executado ao término da cifragem, como um passo omitido, o Rijndael utiliza número de estágios variados, de acordo com a chave utilizada, como apresentado abaixo:

- 9 estágios, para blocos e chave de 128 bits;
- 11 estágios, se o bloco ou a chave forem de 192 bits, e nenhum deles for maior que isso; e
- 13 estágios de o bloco ou a chave forem de 256 bits.

3.2.3.5. RC (Ron's Code ou Rivest Cipher)

Criado por Ron Rivest, na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6. Essencialmente, cada versão difere da outra por trabalhar com chaves maiores.

O RC2 está na categoria dos cifradores de blocos. Ele permite uso de chaves de 1 até 2048, porém para softwares vendidos para fora dos EUA o tamanho da chave é normalmente limitado a 40 bits. É um algoritmo razoavelmente seguro, porém algumas chaves apresentam fraquezas.

O RC4 está na categoria dos cifradores de fluxo e trabalha com uma chave de extensão variável de até 256 bits, possuindo uma caixa de substituição de 256 entradas. Como o RC2, o tamanho da chave é normalmente limitado para softwares comercializados para fora dos EUA.

O RC5 foi publicado em 1994. Este algoritmo permite que os seus usuários definam o tamanho da chave, tamanho do bloco de dados e número de vezes que será aplicada a cifração sobre o arquivo a ser criptografado.

O RC6, proveniente do RC5, foi apresentado ao AES (Advanced Encryption Standard) e selecionado entre os cinco finalistas. Segundo Hinz (2000), pode ser o mais simples dos algoritmos apresentados no concurso. Destaca-se, além de sua simplicidade, por não utilizar S-Boxes.

3.2.3.6. Blowfish

Desenvolvido por Bruce Schneier, Blowfish, em 1993, é um algoritmo criptográfico simétrico de blocos, não patenteado e de código aberto. Ele consiste de um cifrador em blocos de 64 bits, com chaves de tamanho variável, de 32 até 448 bits.

A criptografia é feita através de uma função com 16 interações. Apesar do complexo algoritmo de inicialização, o Blowfish tem grande eficiência com os microprocessadores atuais. A cifração do texto é feita em blocos de 64 ou 128 bits, nos quais os bits não são tratados separadamente, mas em grupos de 32 bits. A fim de aumentar sua eficiência, foi escolhido usar na confecção deste algoritmo funções simples para os microprocessadores, tais como XOR, adição e multiplicação modular.

O algoritmo consiste de duas partes, sendo elas a expansão da chave e a criptografia dos dados. A primeira consiste na transformação da chave em subchaves, totalizando 4168 bits. A segunda consiste de 16 fases, sendo que, em cada uma dessas, é feita uma permutação dependente da chave e uma substituição dependente da chave e dos dados.

O Blowfish ainda não foi muito estudado, mas até hoje ainda não foi notificada nenhuma quebra do algoritmo. De fato, o que já se encontrou foi um grupo de chaves que podem ser detectadas, embora não possam ser quebradas. Por essas razões, esse algoritmo

vem se popularizando. Dentre as diversas aplicações que é utilizado, está o Nautilus e o PGPfone.

3.2.3.7. Twofish

O Twofish é um algoritmo de livre distribuição, criado por Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, e Niels Ferguson com a finalidade de ser um dos candidatos para o Advanced Encryption Standard (AES). Esse algoritmo vem como uma evolução para o Blowfish, também criado por Schneier.

Seu esquema de cifragem consiste em tratar a mensagem em blocos de 128 bits, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 bits. Ele realiza 16 interações durante a criptografia. De fato, é possível utilizar o algoritmo com menos estágios, visto que só foi possível quebrá-lo na quinta interação. No entanto, para se obter um bom nível de segurança, e sendo ele um algoritmo veloz, é recomendável utilizar as 16 fases. Outro ponto favorável à segurança é que não existem chaves fracas para esse algoritmo. A geração de sua chave em microprocessadores, assim como a capacidade de operar com smartcards, e o processamento em hardware foram projetados para gerar uma ótima eficiência.

3.3. Criptografia Assimétrica

A **criptografia de chave pública** ou **criptografia assimétrica** é um método de criptografia, baseada em fórmulas matemáticas (uma combinação de função exponencial com aritmética modular), que permitem que cada usuário tenha um par de chaves de criptografia matematicamente relacionadas, uma privada e outra pública, sendo a última, como o próprio nome diz, publicamente disponível para qualquer pessoa. Essas fórmulas têm a característica de o que for criptografado com uma chave, só pode ser descriptografado com seu par. Ou seja, uma mensagem criptografada com a chave pública de uma, só pode ser descriptografada com a chave privada da mesma, então a primeira pode ser livremente disponibilizada.

Por exemplo, como mostra a Figura 6, Eduardo quer mandar uma mensagem para Karina. Para isso, os dois trocam suas chaves públicas e as chaves privadas ficam em posse de seu respectivo dono. Ele escreve a mensagem e a codifica com a chave pública de Karina. Neste momento, a única pessoa capaz de decodificar esta mensagem será quem possuir a chave privada de Karina, ou seja, somente Karina poderá ler a mensagem.

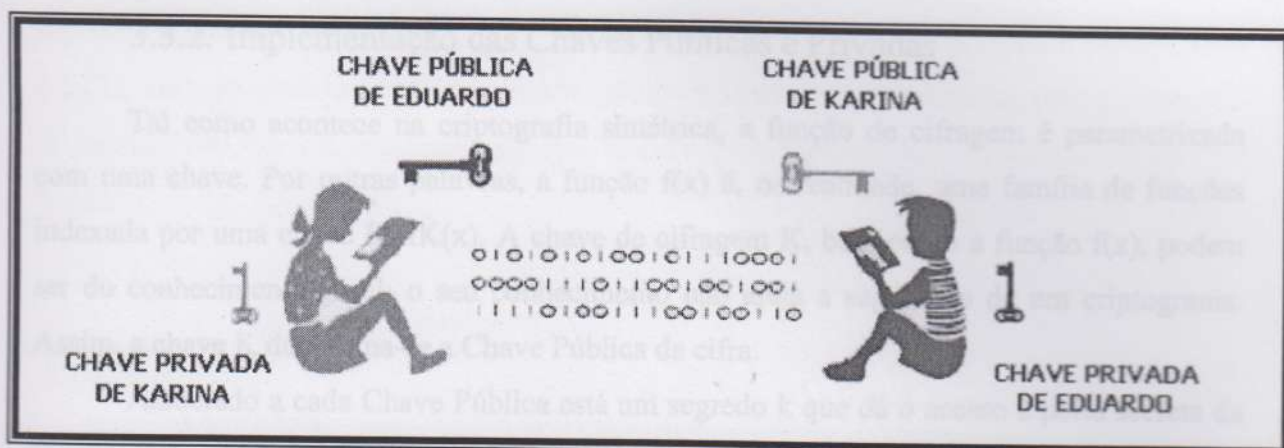


Figura 6. Exemplo de utilização da Criptografia Assimétrica
 Fonte: BASTOS. Introdução à Criptografia. p. 4

3.3.1. Funções One-Way

A idéia central da Criptografia de Chave Pública é a de uma função One-Way, ou função de mão única. Uma função deste tipo, é fácil de calcular, mas muito difícil (de preferência impraticável) de inverter. Ou seja, dado x , $f(x)$ é fácil de calcular mas, dado $f(x)$, é muito difícil obter o x . Um exemplo muito simples de uma função one-way é a exponenciação: é fácil de calcular yx , mas obter $\log(yx)$ é muito mais complicado. A dificuldade é que não há muitas funções deste tipo e, além disso, caso se disponha de uma função verdadeiramente one-way, impossível de inverter, ao utilizá-la para cifrar informação, isso significa que nunca será possível recuperá-la.

As funções utilizadas em criptografia pertencem a um subconjunto das funções one-way chamadas de funções one-way com trapdoor. Estas funções têm a particularidade de oferecerem uma porta de entrada secreta que permite a sua inversão de forma facilitada. O princípio de funcionamento destas funções é o seguinte:

- Como qualquer função one-way, $f(x)$ é fácil de calcular.
- Como qualquer função one-way, $f^{-1}(f(x))$ é difícil de calcular.
- Se for conhecido o segredo k , $f^{-1}(f(x), k)$ é fácil de calcular.

A aplicação deste tipo de função à criptografia é imediata: qualquer agente que conheça a função f pode cifrar informação. No entanto, apenas um agente que conheça o segredo k pode efetuar a decifragem.

3.3.2. Implementação das Chaves Públicas e Privadas

Tal como acontece na criptografia simétrica, a função de cifragem é parametrizada com uma chave. Por outras palavras, a função $f(x)$ é, na realidade, uma família de funções indexada por uma chave K : $f_K(x)$. A chave de cifragem K , bem como a função $f(x)$, podem ser do conhecimento geral: o seu conhecimento não afeta a segurança de um criptograma. Assim, a chave K denomina-se a Chave Pública da cifra.

Associado a cada Chave Pública está um segredo k que dá o acesso à porta secreta da função $f(x)$: a Chave Privada da cifra. Esta chave não pode ser calculável a partir dos parâmetros públicos da cifra.

Uma cifra assimétrica consiste, portanto, na função $f(x)$, e num par de chaves (K, k) , em que K é a Chave Pública e k é a Chave Privada.

3.3.3. ECC (Elliptic Curve Cryptography)

A Criptografia de Curvas Elípticas, baseada na matemática das curvas elípticas, é uma variante da criptografia assimétrica. A utilização de curvas elípticas em criptografia foi proposta de modo independente por Neal Koblitz e Victor Miller em 1985, que argumentam a ECC poder ser mais rápida e usar chaves mais curtas do que os métodos antigos, como o RSA, e proporcionar ao mesmo tempo um nível de segurança equivalente.

Existem várias versões de criptografia de curvas elípticas. Todas elas, com pequenas variações, se baseiam na crença amplamente aceita da dificuldade de se resolver o problema de um logaritmo discreto para o grupo de uma curva elíptica sobre alguns grupos finitos. Os grupos finitos mais usados para isso são os inteiros módulo um número primo ou um grupo de Galois cujo tamanho seja potência de 2. Também foram propostos grupos de Galois cujo tamanho seja potência de algum número primo, mas eles geraram dúvidas entre os criptoanalistas.

Os métodos utilizados na prática, para se codificar mensagens a partir desse valor secreto, são adaptações de antigos sistemas criptográficos de logaritmos discretos, originalmente projetados para ser usados em outros grupos. Entre eles podem ser incluídos Diffie-Hellman, ElGamal e DSA.

As operações necessárias para se executar este sistema são mais lentas do que aquelas de um sistema de fatorização ou de logaritmo discreto módulo um inteiro do mesmo tamanho. De qualquer modo, os autores de sistemas de ECC acreditam que o PLDCE é

significativamente mais complicado que os problemas de fatorização ou de PLD. Assim, com o ECC, pode-se obter a mesma segurança usando-se chaves muito menores, pelo que poderia se mostrar útil em conexões de rede que tenham requisitos muito limitados de largura de banda.

3.3.4. Algoritmos assimétricos

3.3.4.1.DH

Em 1976, Whitfield Diffie e Martin Hellman introduziram o conceito de criptografia assimétrica, com o artigo New Directions in Cryptography, e também um sistema de troca de chaves baseado no problema do logaritmo discreto, cuja dificuldade de computação é igual ou superior à fatoração do produto de números primos. Foi conhecido posteriormente que tal algoritmo havia sido criado alguns anos antes pela inteligência britânica, contudo este era um sistema anônimo, usado de base para outros métodos de autenticação, que acabou caindo no esquecimento. O algoritmo DH é vulnerável a ataques do tipo "timing".

3.3.4.2.RSA

É um dos métodos de criptografia de chave pública mais conhecido e o mais utilizado em aplicações comerciais. Foi inventado em 1978, por R. L. Rivest, A. Shamir e L. Adleman, de forma que as letras RSA correspondem às iniciais dos inventores do código. A implementação do RSA utiliza dois números primos p e q . A codificação de uma mensagem se dá utilizando o produto destes dois números (n) como a chave pública de codificação, que deve ser mantida em segredo, pois a segurança do RSA depende disto. Ou seja, sua segurança depende da dificuldade em se fatorar o produto dessa multiplicação, conseqüentemente do tamanho de chave escolhida. O algoritmo RSA é vulnerável a ataques "chosen plaintext" e "timing".

3.3.4.3.El Gamal

Taher Elgamal, em 1984, introduziu o algoritmo que recebeu seu nome. É um algoritmo assimétrico, cuja assimetria se baseia na dificuldade de se extrair logaritmos discretos em corpos finitos. Este algoritmo não é patenteado, mas sua versão para cifragem é uma variante do algoritmo de Diffie-Hellmann.

Cada assinatura ou encriptação requer um valor randômico (nonce, ou chave de sessão) k . O sistema em si é composto por 3 componentes, um gerador de chaves, um algoritmo de encriptação e um algoritmo de desencriptação. É vulnerável a ataques de "chosen ciphertext". O conhecimento de pelo menos duas mensagens ou assinaturas com o mesmo k permite a dedução da chave privada x .

3.4. Criptografia Híbrida

Apesar de todas as vantagens oferecidas, as cifras assimétricas não substituíram as cifras simétricas pelos motivos expostos a seguir. Os algoritmos assimétricos são muito mais lentos que os algoritmos simétricos, estes fornecendo a mesma segurança. Isto ocorre devido à existência de atalhos nos ataques a estas cifras, que forçam as chaves terem no mínimo 1024 bits, tornando os cálculos muito pesados. Conseqüentemente, algoritmos de chave assimétrica não são indicados para cifrar mensagens muito longas. Outra desvantagem das cifras assimétricas é o fato de sempre ser possível efetuar um ataque por texto limpo conhecido, pois ao se conhecer um criptograma e a chave pública pode-se, teoricamente, testar todas as possibilidades para o texto limpo até se obter uma correspondência. Desta forma, quando os textos limpos possíveis são poucos, se torna um problema.

A criptografia híbrida, ou "envelope digital", surgiu como um meio de aproveitar as vantagens oferecidas por esses dois tipos de algoritmos: o de chave simétrica e o de chave assimétrica. Desta forma, as aplicações mais comuns das cifras assimétricas complementam a funcionalidade das cifras simétricas, como nos sistemas híbridos de distribuição de chaves de sessão.

Como mostrado por Costa e Figueiredo (2006), o funcionamento da comunicação protegida por meio de um algoritmo híbrido, como o PGP, se dá da seguinte forma:

1. Alice prepara o envio de uma mensagem para Bob e cifra o texto destinado a Bob com um algoritmo simétrico rápido;
2. Alice cifra a chave simétrica com a chave pública de Bob e envia a mensagem ;
3. Bob recebe a mensagem e a chave cifrada;
4. Bob utiliza a sua chave privada para decifrar a chave simétrica e em seguida decifra a mensagem.

3.5. Chaves de Sessão

Há diversas vantagens de se utilizar de um servidor central responsável por armazenar todas as chaves secretas, como: a redução do espaço necessário para o armazenamento, a centralização da gestão das chaves, a redução da exposição das chaves, etc. Porém, uma vez que as chaves permanecem válidas, durante a atividade do sistema, elas estão expostas a ataques durante um tempo prolongado ou, caso uma chave seja corrompida, e isso não seja detectado, a comunicação entre o par de agentes correspondente deixa de ser segura. O conceito de chave de sessão resolve estes problemas, gerando uma chave secreta para cada troca de informação. Esta chave é estabelecida entre emissor e receptor, utilizada para a troca de informação e depois é destruída.

Há duas formas para o estabelecimento de chaves de sessão: a distribuição de chaves e o acordo de chaves.

3.5.1. Distribuição de Chaves

Num esquema de distribuição de chaves, um dos agentes é responsável por gerar a chave de sessão. O problema é transmitir a chave de sessão para o interlocutor através de um canal seguro. Em geral, a solução adotada consiste na introdução no sistema de um Agente de Confiança ou Trusted Agent (TA), e na adoção de uma classificação das chaves secretas em dois tipos: chaves para cifragem de chaves e chaves para cifragem de dados. As chaves para cifragem de chaves são geradas e pré-distribuídas por um canal seguro exterior ao sistema, permitindo ao TA comunicar com todos os agentes de forma segura. As chaves para cifragem de dados correspondem às chaves de sessão. Estas são geradas por um dos interlocutores ou pelo TA e transmitidas, através do TA, utilizando as chaves anteriores. Como grande desvantagem, este esquema tem a necessidade de pré-distribuir, armazenar e proteger as N chaves secretas utilizadas para comunicação segura entre o TA e os agentes. Na comunicação agente/TA podem também ser usadas cifras assimétricas, dependendo da implementação.

Uma das soluções implementadas para distribuição de chaves é o sistema de confiança tripla, chamado de Centro de Distribuição de Chaves (CDC), que é composto por duas partes separadas: um Servidor de Autenticação (SA) e Servidor de Concessão de Ticket (SCT). O CDC mantém um banco de dados de chaves secretas. Toda entidade de rede, tanto clientes como servidores, compartilham uma chave secreta que é apenas conhecido por eles mesmos e pelo CDC. Para garantir a privacidade das informações, nas comunicações entre as entidades

é gerado uma chave de sessão temporária. O Kerberos é um exemplo de um protocolo comercial baseado nesta filosofia.

3.5.1.1. Associações de Segurança (Security Association, SA)

Quando dois nós desejam se comunicar com segurança, eles devem determinar quais algoritmos serão usados (se DES ou IDEA, MD5 ou SHA). Após escolher os algoritmos, as chaves de sessão devem ser trocadas e há uma certa quantidade de informações que precisam ser negociadas. A Associação de Segurança é o método para lidar com todos estes detalhes de uma determinada sessão de comunicação. Uma SA representa o relacionamento entre duas ou mais entidades que descreve como estas utilizarão os serviços de segurança para se comunicarem. As SAs são utilizadas pelo protocolo IPSec (IP Security Protocol) e também podem ser utilizadas por outras entidades para descrever os parâmetros de segurança entre dois dispositivos, como os que utilizam IKE (Internet Key Exchange), método utilizado pelo protocolo de gerenciamento de chaves IKMP (Internet Key Management Protocol).

As SAs são unidirecionais, o que significa que para cada par de sistemas que se comunicam, deve-se ter pelo menos duas conexões seguras, uma de A para B e outra de B para A. As SAs são identificadas de forma única pela associação entre um número aleatório chamado SPI (Security Parameter Index) e o endereço IP de destino. Por exemplo, quando um sistema envia um pacote que requer proteção IPSec, ele olha as SAs armazenadas em seu banco de dados, processa as informações, e adiciona o SPI da SA no cabeçalho IPSec. Quando o destino IPSec recebe o pacote, ele procura a SA em seu banco de dados de acordo com o endereço de destino e o SPI, e então processa o pacote da forma necessária. As SAs são simplesmente o relatório das políticas de segurança que serão usadas entre dois dispositivos.

3.5.2. Acordo de Chaves

Os protocolos de acordo de chaves são mecanismos que derivam da criptografia assimétrica. O seu princípio de funcionamento é o seguinte:

1. dois agentes, A e B, pretendem comunicar utilizando uma cifra simétrica e, logo, estabelecer uma chave de sessão. Existe um canal de comunicação aberto entre os dois agentes;

2. os dois agentes seguem um conjunto de passos que lhes permitem identificar-se mutuamente;
3. os dois agentes cooperam para gerar uma chave de sessão trocando informação através do canal aberto. Na composição da chave entra informação aleatória gerada por ambas as partes, de forma que ambos os agentes tenham a garantia da frescura da chave; e
4. os dois agentes executam um conjunto de passos que lhes permitem confirmar que foi estabelecida uma chave de sessão adequada.

Em nenhum dos passos anteriores pode circular no canal aberto informação que permita a um intruso adivinhar a chave secreta acordada. O segredo está na utilização de funções matemáticas com características especiais: as chamadas funções oneway. O que se consegue na prática é eliminar a necessidade de se armazenar informação secreta, bem como a necessidade da presença de um Agente de Confiança durante o funcionamento do sistema. Apesar de que, em geral, é necessário um TA para garantir as questões de identificação. O SSL é um exemplo de um protocolo comercial que recorre a este tipo de tecnologia.

3.6. Funções de Hash Criptográficas

As funções de hash criptográficas (também chamadas funções de hash one-way, message digests, impressões digitais, etc.) são fundamentais a muitos protocolos criptográficos para garantia de integridade. São funções utilizadas na computação há muito tempo, tratando-se de funções que transformam uma entrada (input) de tamanho variável numa saída (output) de tamanho fixo.

Quando se pretende garantir integridade, o que interessa é extrair uma impressão digital não invertível de uma mensagem, de forma a obter um valor que identifique o seu conteúdo. Entretanto, como as funções de hash não são injectivas, a identificação não pode ser unívoca, sendo assim, haverá sempre várias mensagens que serão mapeadas no mesmo valor de hash. Ou seja, o que se consegue na realidade é uma identificação probabilística, sendo provável que o valor de hash tenha sido originado por aquela mensagem. Isto é possível, pois são utilizadas as funções de hash ditas "livres de colisões" em que, além de não haver uma relação visível entre input e output, é muito difícil encontrar duas mensagens que originem o mesmo valor de hash (fortemente livre de colisões). As funções de hash deste tipo podem ser tornadas públicas. A sua segurança está na baixa probabilidade de encontrar duas mensagens com o mesmo valor de hash.

3.6.1. Algoritmos de Hash

3.6.1.1. MD4 e MD5

O MD4 foi desenvolvido por Ron Rivest (um dos inventores do RSA) como uma função de hash para aplicações criptográficas que garantisse:

- segurança, no sentido em que o ataque mais eficiente à função de hash é o ataque por força bruta;
- segurança direta, no sentido em que a base da segurança da função de hash não reside em pressupostos de complexidade computacional, como sejam a dificuldade em fatorizar um inteiro grande; e
- eficiência e simplicidade.

Apesar deste algoritmo ser ainda seguro, uma série de avanços na criptoanálise de alguns dos seus rounds levou o autor a melhorá-lo, desenvolvendo o MD5. Tanto o MD4 como o MD5 produzem valores de hash de 128 bits.

No funcionamento do MD5, a mensagem é vista como uma sequência de b bits, aos quais é adicionada uma sequência $\{1, 0, 0, 0, \dots\}$ por forma a obter um bit stream de comprimento $b_0 = 448 \pmod{512}$. À sequência anterior é adicionada uma representação de 64 bits do valor b , obtendo-se um bit stream de comprimento múltiplo de 512. Quatro registos de 32 bits (A, B, C e D), que no final conterão o output do algoritmo, são inicializados com valores constantes. Cada bloco de 512 bits da mensagem tratado como 16 sub-blocos de 32 bits (X_k). O processamento consiste em 4 rounds em que os X_k são combinados com os valores dos registos A, B, C e D através de operações lógicas bit a bit (não lineares) e rotações, por exemplo:

$A = B + ((A + f(B, C, D) + X_k + t_i) \lll s)$, com $f(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$, e s, t_k variáveis.

3.6.1.2. SHA-1 (Secure Hash Algorithm)

O SHA foi desenvolvido pelas agências governamentais americanas NIST e NSA para incluir no standard de assinaturas digitais DSS (Digital Signature Standard). O SHA, como o MD5, foi também desenvolvido com base no MD4, mas de forma diferente e independentemente daquele. O valor de hash produzido pelo algoritmo é de 160 bits, mas os critérios seguidos no seu desenvolvimento não foram divulgados.

De acordo com Lima (2006), as partes internas do SHA são mais fortes que o MD5. De qualquer forma, hoje em dia, o MD5 e o SHA são os algoritmos de hash tidos como mais seguros para aplicações criptográficas.

3.6.2. MAC (Message Authentication Codes)

O MAC surgiu como uma solução para ataques man-in-the-middle na troca de mensagens. A integridade era garantida pela função hash, porém a autenticidade do hash não era garantida, podendo a mensagem ter sido interceptada e alterada antes de chegar ao destinatário.

Um MAC é uma função de hash criptográfica cujo resultado depende, não só do conteúdo da mensagem que é processada, mas também de uma chave secreta. Para gerar o MAC é necessário conhecer o algoritmo e a chave secreta, o mesmo acontece para verificar se o MAC é válido, havendo duas opções de implementação:

1. Gerar um valor de hash com uma função de hash criptográfica e utilizar uma cifra simétrica para cifrar esse valor.
2. Utilizar uma cifra simétrica por blocos num modo com realimentação dos criptogramas (CBC ou CFB), cifrar a mensagem e aproveitar o último bloco do criptograma como MAC (talvez cifrando-o mais uma vez no mesmo modo).

É possível, e até mais frequente, utilizar MACs em aplicações que não requerem confidencialidade. Nem sempre a confidencialidade implica a autenticação da origem dos dados. Ao incluir um MAC na mensagem, é possível comprovar a origem da mesma e a sua integridade, antes de a decifrar.

O MAC pode ser utilizado como uma impressão digital, ao tornar impossíveis alterações do checksum para mascarar uma modificação da mensagem. Outra aplicação possível é a proteção de arquivos contra ataques de vírus, por ser impossível que estes viessem a produzir um MAC válido que escondesse as alterações introduzidas.

O HMAC é um algoritmo de autenticação de mensagens baseado em funções hash. É um algoritmo de MAC desenvolvido inicialmente para ser utilizado no IPsec e, atualmente, é o mais utilizado. Baseia-se numa função de hash criptográfica (HMAC-SHA1 ou HMAC-MD5) e utiliza a chave secreta em operações de concatenação dos streams de bytes processados. Ele funciona da seguinte forma: duas partes que desejam se comunicar compartilham uma chave secreta; quando precisam enviar uma mensagem, fazem o resumo desta com uma função hash; este resumo é criptografado com a chave previamente

compartilhada; a mensagem é enviada para o destinatário juntamente com o MAC. Desta forma, um invasor, poderia até interceptar a mensagem, mas, para alterar o resumo, teria que conhecer previamente a chave.

3.7. Assinaturas Digitais

A assinatura manuscrita é, há muito, utilizada como prova de autoria ou, pelo menos, de concordância com o conteúdo de um documento. O que se espera de uma assinatura escrita é que seja autêntica (convença o receptor do documento de que o signatário explicitamente assinou o documento, conhecendo o seu conteúdo, por ser o seu autor ou, simplesmente, por o aceitar), que não seja falsificável (prova que o signatário, e não outra pessoa, assinou o documento), que não seja reutilizável (faz parte do documento e não se pode transpor para outro documento), que garanta a integridade do documento (o documento permaneceu inalterado desde que a assinatura lá foi colocada) e que não seja repudiável (o signatário não pode, à posteriori, negar que assinou o documento). Na realidade nenhuma destas propriedades é respeitada de forma absoluta por uma assinatura manuscrita.

A assinatura digital é equivalente a uma assinatura manuscrita, mas aplicada a documentos eletrônicos. Uma assinatura digital é uma sequência de bytes cujo valor não tem significado fora do contexto de um algoritmo específico. Ela é gerada pelo signatário e acompanha o documento assinado, como anexo. Na verdade, a implementação de assinaturas digitais é mais complicada do que no caso de documentos em papel pela facilidade em se copiar arquivos de computador e da facilidade em se alterar arquivos de computador sem deixar vestígios, mas a cada dia, este mecanismo vem sendo aperfeiçoado e ganhando credibilidade e ganhando espaço no mercado.

O objetivo das assinaturas digitais não é conferir confidencialidade, elas apenas acompanham o documento a que se referem, que pode ou não ser cifrado. Porém, associando a assinatura digital com a cifragem, obtém-se um protocolo que combina confidencialidade e autenticação.

Associados a um esquema de assinaturas digitais, há sempre dois procedimentos complementares a considerar:

- Geração da assinatura: procedimento segundo o qual o signatário produz a sequência de bytes a partir do documento e de informação secreta ou privada (uma chave). Este procedimento deve assegurar as propriedades requeridas para a assinatura; e

- Verificação da assinatura: procedimento segundo o qual o destinatário do documento assinado consegue assegurar-se de que a sequência de bytes que recebe como assinatura é um valor válido, gerado pelo signatário para esse fim.

3.7.1. Algoritmos de Assinatura Digital

3.7.1.1.RSA

A assinatura RSA é uma adaptação direta da cifra assimétrica RSA. Os cálculos matemáticos envolvidos são exatamente os mesmos, tendo em conta que a cifragem passa a ser efetuada utilizando a chave privada e que a decifragem passa a ser feita com a chave pública. Na geração da assinatura, o signatário simplesmente aplica este processo modificado de cifragem ao documento que pretende assinar. Por outro lado, o destinatário ao receber o documento, acompanhado pela sua versão cifrada, que funciona como assinatura, verifica a assinatura decifrando-a utilizando a chave pública do signatário e comparando o resultado com o documento original.

A assinatura RSA garante autenticidade, porque, em princípio, apenas o signatário conhece a sua chave privada. A assinatura não é falsificável nem reutilizável porque o destinatário, ou outra pessoa, não conseguiria apresentar outra mensagem cifrada com a chave privada do signatário. A mensagem não é alterável pela mesma razão. Além disso, a assinatura não é repudiável porque o destinatário pode sempre mostrar a assinatura com a chave privada do signatário.

As assinaturas digitais baseadas na criptografia de chave pública dominam a criptografia atual, porém nem todos os algoritmos de assinatura digital são adaptações diretas de algoritmos de cifra assimétrica. Desta forma, não se deve confundir uma assinatura digital, que confere autenticação com uma cifra assimétrica, evitando-se referir às operações de assinar e verificar uma assinatura como cifrar com chave privada ou decifrar com chave pública.

Um outro método para assinatura digital seria utilizando agentes de confiança para assegurarem a autenticidade do emissor. Este, sistema, entretanto, é demasiado exigente para o agente de confiança, do qual se espera eficiência na comunicação entre muitos agentes e no armazenamento das mensagens assinadas.

3.7.1.2. DAS (Digital Signature Algorithm)

Em 1991, a agência americana NIST propôs um novo standard de assinaturas digitais de utilização livre: o Digital Signature Standard. Esta decisão causou polêmica, uma vez que muitas aplicações tinham já sido desenvolvidas com base no RSA, nessa altura licenciado, significando isto uma considerável perda para as empresas responsáveis.

Além de ser livre de *royalties*, o grande objetivo de desenvolvimento do DSA foi tornar a operação de geração da assinatura mais leve computacionalmente para facilitar a sua implementação em *smartcards*. Ele baseia-se nas técnicas de chave pública El Gamal, cuja segurança fundamenta-se no problema do logaritmo discreto (PLD). Dentre as principais críticas ao DSA, está o fato de não poder ser utilizado para cifragem ou distribuição de chaves e por mais lento que o RSA. Além disso, inicialmente seu tamanho da chave era muito pequeno, 512 bits, tendo sido depois alterado o standard para permitir também chaves de 1024 bits.

3.7.1.3. ECDSA (Elliptic Curve Digital Signature Algorithm)

O ECDSA apresenta as seguintes vantagens sobre o DSA e outros algoritmos de assinatura digital baseados no RSA:

- utiliza chaves menores;
- utiliza soma ao invés de multiplicações;
- utiliza multiplicações (soma cumulativa) ao invés de exponenciações;
- é mais eficiente em termos de tempo de resposta;
- consome menos espaço de armazenamento; e
- é adequado para equipamentos com poucos recursos de hardware disponíveis.

De um modo geral o ECDSA vem se mostrando muito bom no que tange à resistência a ataques, especialmente para ataques quando a mensagem é conhecida. Entretanto, ele está sujeito aos seguintes tipos de ataques: contra as curvas elípticas e contra o problema dos logaritmos discretos, que fundamentam os criptosistemas baseados nestas curva, e ataques à função hash utilizada (SHA-1), dentre outros.

3.7.2. Assinaturas Digitais e Funções de Hash

Os algoritmos assimétricos são geralmente muito pouco eficientes, o que torna pouco prática a assinatura de mensagens de tamanho realista. Por esta razão, tornou-se mais comum a geração de assinaturas digitais a partir de impressões digitais das mensagens.

O processo de geração da assinatura começa pelo cálculo de um valor de hash, que é depois assinado com a chave privada do signatário. A verificação da assinatura implica um novo cálculo do hash da mensagem. A validade da assinatura é avaliada através de um algoritmo que processa este hash, a chave pública do signatário e a assinatura.

Este método tem a vantagem adicional de tornar mais difícil o ataque à assinatura. O hash funciona como checksum da mensagem.

3.7.3. Protocolo de Acordo de Chaves: Station-to-Station (STS)

O protocolo de acordo de chaves Diffie-Hellman é vulnerável a um ataque chamado man-in-the-middle, onde o intruso intercepta as mensagens trocadas entre os agentes, substituindo-as por mensagens suas. Como não há autenticação, os agentes terminam o protocolo acreditando que acordaram uma chave entre si. Na realidade, cada um dos agentes acordou uma chave secreta com o intruso, sem o saber. Enquanto o intruso fizer o relay das mensagens entre os agentes, estes não se apercebem da sua presença. Outro problema com o protocolo DH é não incluir, explicitamente, um passo de confirmação da chave acordada.

O protocolo STS corrige estes problemas acrescentando um novo passo ao protocolo DH, com base num esquema de assinaturas digitais:

1. uma vez acordada a chave de sessão, os agentes assinam digitalmente o par ordenado (X, Y) ;
2. estas assinaturas são trocadas entre os agentes, cifradas com a chave recém-acordada;
3. só se considera que o protocolo terminou com sucesso se as assinaturas forem recuperadas e verificadas corretamente.

Entretanto, para que este sistema seja seguro, é necessário estabelecer a validade das chaves públicas dos agentes, sendo necessário um sistema de certificação de chaves públicas.

3.8. ICP (Infraestrutura de Chaves Públicas)

Com o surgimento das cifras assimétricas, ficou resolvido o problema da partilha e gestão de chaves secretas, uma vez que a Chave Privada permanece na posse de um único agente. Porém, ainda continuou persistindo o problema de garantir se uma chave pública pertence a um determinado agente. A autenticação de origem de mensagens permite fornecer a uma entidade garantia sobre a identidade do emissor de uma determinada mensagem, promovendo garantias de integridade.

O PGP (Pretty Good Privacy) foi o primeiro sistema de segurança que ofereceu criptografia de chave pública e assinatura digital de qualidade para as massas. Ficou tão popular que virou o padrão OpenPGP e posteriormente recebeu várias implementações livres. É largamente usado até hoje, principalmente em troca de e-mails. Sua popularização exigiu que houvesse uma forma para as pessoas encontrarem as chaves públicas de outras pessoas, que muitas vezes nem eram conhecidas pelas primeiras. No começo dos tempos do PGP, haviam sites onde as pessoas publicavam suas chaves públicas para as outras encontrarem, tendo sido a forma mais rudimentar de uma ICP.

Uma Infra-Estrutura de Chaves Públicas é um órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de acreditação e confiança em transações entre partes que utilizam certificados digitais. A principal função do ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública.

3.8.1. Certificados Digitais

A certificação digital é a maneira de autenticar uma chave pública. Um certificado digital é um arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente a chave privada que acredita-se ser de posse unicamente da entidade especificada no certificado.

Um certificado digital normalmente é usado para ligar uma entidade a uma chave pública. Para garantir a integridade das informações contidas neste arquivo ele é assinado digitalmente. No caso de uma Infraestrutura de Chaves Públicas (ICP), o certificado é assinado pela Autoridade Certificadora (AC) que o emitiu e no caso de um modelo de Teia de Confiança (Web of trust), como o PGP, o certificado é assinado pela própria entidade e assinado por outros que dizem confiar naquela entidade. Em ambos os casos as assinaturas contidas em um certificado são atestamentos feitos por uma entidade que diz confiar nos dados contidos naquele certificado.

Na prática um cliente que deseje ter acesso a sua conta bancária, através da Internet, para que envie sua senha com segurança, precisa primeiro receber do banco a chave pública deste, assinada digitalmente por uma outra instituição de grande credibilidade. Para facilitar, os fabricantes de navegadores (Mozilla, Microsoft, etc) instalam em seus produtos, na fábrica,

os certificados digitais dessas entidades, que são usadas para verificar a autenticidade da chave pública e identidade do site da empresa. Esta, por sua vez, tem que passar por um processo burocrático junto a essa entidade certificadora, provando ser quem diz ser, para obter o certificado.

Um certificado pode ser revogado se for descoberto que a sua chave privada relacionada foi comprometida, ou se o seu relacionamento (entre uma entidade e a sua chave pública) embutida no certificado estiver incorreta ou foi mudada; isto poderá ocorrer, por exemplo, se uma pessoa muda de nome ou CPF. Uma revogação não é comum, mas a possibilidade da ocorrência significa que quando um certificado é confiável, o usuário deverá sempre checar a sua validade. Isto pode ser feito comparando o certificado com uma Lista de certificados revogados (LCR). Seu objetivo é mostrar todos os certificados revogados ou cancelados no âmbito daquela AC. Garantir que a lista está correta e atualizada é a parte mais importante em uma ICP centralizada, o que às vezes não é feito corretamente. Para a LCR ser efetiva, precisa estar disponível o tempo todo para qualquer um que a precisar e ser atualizada frequentemente. A outra maneira de conferir a validade de um certificado é fazer uma consulta a AC usando o Online Certificate Status Protocol (OCSP) para saber o estado de um certificado específico.

Um certificado normalmente inclui:

- Informações referentes a entidade para o qual o certificado foi emitido (nome, email, CPF/CNPJ, PIS etc.);
- A chave pública referente a chave privada de posse da entidade especificada no certificado;
- O período de validade;
- A localização do "centro de revogação" (uma URL para download da CRL, ou local para uma consulta OCSP); e
- A(s) assinatura(s) da(s) AC/entidade(s) que afirma que a chave pública contida naquele certificado confere com as informações contidas no mesmo.

O padrão mais comum para certificados digitais no âmbito de uma ICP é o ITU-T X.509. O X.509 foi adaptado para a Internet pelo grupo da Internet Engineering Task Force (IETF) PKIX.

3.9. Criptografia Quântica

Utilizando-se pares de fótons, a criptografia quântica permite que duas pessoas escolham uma chave secreta sem jamais terem-se visto, trocando alguma mensagem ou mesmo algo material. A criptografia quântica oferece a possibilidade de gerar uma chave segura se o sinal é um objeto quântico, assim, o termo mais correto seria Distribuição de Chave Quântica (Quantum Key Distribution - QKD) e não Criptografia Quântica.

A Criptologia atual está amparada na Matemática, mas com a introdução desse conceito de mensagens criptografadas por chaves quânticas, a física passou a ter importância primordial no tema. O maior problema, para implementação da Criptografia quântica, ainda é a taxa de erros na transmissão dos fótons, seja por via aérea ou fibra ótica. Atualmente, os melhores resultados obtidos são em cabos de fibra ótica de altíssima pureza e de elevadíssimo custo também, alcançando algo em torno de 70 km. Por via aérea, a distância chega a algumas centenas de metros e qualquer tentativa de se aumentar essa distância, tanto em um quanto em outro método, a taxa de erros se torna muito grande e inviabiliza o processo. O desenvolvimento de tecnologias que permitam o perfeito alinhamento dos polarizadores, fibras óticas melhores e amplificadores quânticos de sinais, permitirá que o sistema de Distribuição de Chaves Quânticas venha a ser o novo padrão de segurança de dados.

A Criptografia Quântica se destaca, em relação aos outros métodos criptográficos, pois não necessita do segredo nem do contato prévio entre as partes. Ela permite a detecção de intrusos tentando interceptar o envio das chaves, e é incondicionalmente segura mesmo que o intruso tenha poder computacional ilimitado. Contudo, hoje apresenta um elevado custo de implantação. A esperança é que o desenvolvimento tecnológico possa torná-la acessível a todas as aplicações militares, comerciais e de fins civis em geral.

4.2. Requisitos de Segurança

Segunda Serprest (2007), a Segurança da Informação tem quatro objetivos principais, de forma que, qualquer proposta de sistema criptográfico apresenta pelo menos um desses requisitos:

- * *confidencialidade da mensagem*: só o destinatário autorizado deve ser capaz de ler o conteúdo da mensagem da sua forma cifrada. Além disto, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.
- * *integridade da mensagem*: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.

Capítulo 4 – Aplicação de Criptografia em Redes de Computadores

4.1. Segurança de Informação e Segurança em Rede

Atualmente, tanto indivíduos como organizações possuem uma grande dependência dos meios eletrônicos para armazenamento de informações. Existe também um alto grau de conectividade entre os sistemas informatizados, devido o surgimento das redes de computadores. Essa interconexão nos sistemas informatizados leva a um cuidado maior com os ataques, que podem ser tentativas de acesso indevido de pessoas fisicamente distantes dos sistemas onde a informação está armazenada.

Em termos de segurança da informação, uma empresa que lida com segredos industriais, militares ou dados bancários tem demandas distintas em relação a uma pequena empresa prestadora de serviços, por exemplo. Cada organização possui diferentes necessidades de segurança no armazenamento da informação em meio eletrônico. Dessa forma, as políticas de segurança devem ser coerentes com as necessidades das organizações.

O ataque a uma organização é, de maneira geral, qualquer ação que compromete a segurança de uma informação que esta organização possui. Isso pode ocorrer de várias formas, como o acesso não autorizado a uma rede de computadores ou a uma informação codificada (quando o atacante decifra o código). Há vários modos de ataques e serviços utilizados para preveni-los.

4.2. Requisitos de Segurança

Segundo Serprest (200?), a Segurança da Informação tem quatro objetivos principais, de forma que, qualquer proposta de sistema criptográfico apresenta pelo menos um desses requisitos:

- *confidencialidade* da mensagem: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.
- *integridade* da mensagem: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.

- *autenticação* do remetente: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.
- *não-repúdio* do remetente: não deverá ser possível ao remetente negar o envio da mensagem.

4.3. Gerência de Segurança OSI

A Gerência de Segurança OSI é uma das cinco áreas funcionais do Gerenciamento de Redes OSI definido pela ISO. Ela tem por objetivo criar, controlar e eliminar mecanismos de segurança, bem como distribuir informações relevantes à segurança, gerando alarmes para o gerente da rede quando for detectado algum evento de segurança. O modelo de segurança definido pela ISO se baseia em dois principais conceitos:

- *arquitetura de segurança*: que objetiva descrever os serviços de segurança e os mecanismos relacionados, bem como definir em qual camada do modelo de referência OSI esses serviços e mecanismos poderão ser localizados. Os serviços de segurança são construídos por mecanismos de segurança, que, por sua vez, são implementados usando algoritmos. A arquitetura de segurança OSI é definida pela norma X.800 (Data communication networks: systems interconnection (OSI); security, structure and applications), definido pelo CCIT, um órgão permanente da ITU (International Telecommunications Union). Estes serviços e mecanismos são básicos, podendo ser utilizados em combinação com outros, a fim de se adequarem a políticas de segurança e requisitos do usuário.
- *funções de gerenciamento de segurança*: que visa fornecer relatórios de eventos e informações estatísticas, manter e analisar registros de históricos desses eventos e alterar o modo de operação do sistema através da ativação/desativação dos serviços de segurança.

A importância dos serviços de segurança varia de acordo com o tipo de aplicação. Segundo a Norma X.800 (1991), os serviços de segurança definidos pela OSI são:

- *Controle de acesso*: protegem contra acesso não autorizados;
- *Autenticação*: fornece garantias da identidade;
- *Integridade*: protege os dados de serem alterados por entidades não autorizadas; e
- *Não-repúdio*: garante que o emissor não negue a autoria.

Nos sistemas distribuídos um dos serviços mais relevantes é a autenticação dos usuários, devido ao fato da comunicação entre eles ser através de uma rede compartilhada por vários outros usuários. Nas aplicações EDI (Electronic Data Interchange), que trata-se da troca

de documentos via sistemas de teleinformática entre duas ou mais organizações de forma padronizada, o mais importante é a não-rejeição, pois além de conhecer a identidade do usuário do intercâmbio, é necessário estar apto a provar esta identidade. O serviço controle de acesso está mais relacionado com o domínio da aplicação e gerenciamento, portanto ele é um serviço mais associado à aplicação servidor.

Um mecanismo de segurança, ou a combinação entre eles, fornecem os serviços de segurança. Os três grandes blocos de mecanismos de segurança, definidos pela norma X800 (1991), são:

- *Encriptação dos dados*: usado para garantir Confidencialidade;
- *Assinaturas digitais*: usado para garantir Autenticidade, integridade e não repúdio;
- *Checksum/algoritmos de Hash*: garantem a integridade e podem garantir a autenticidade.

4.4. Ataques a Sistemas Computacionais

De modo geral, quanto maior for a chave de criptografia mais difícil é atacar um sistema criptográfico. Outros fatores influenciam na segurança, como a cultura em torno de manter bem guardadas as chaves privadas e a qualidade dos algoritmos do cifrador. Entretanto, a segurança real de qualquer esquema de criptografia não foi comprovada. Teoricamente, dependendo da capacidade de recurso computacional disponível, é possível quebrar uma mensagem criptografada, porém, necessitaria de centenas de computadores interconectados trabalhando para esse fim. Como hoje, na prática, isso é intangível, pode-se considerar seguros os produtos de criptografia que façam uso de bons algoritmos.

Os ataques podem ser passivos ou ativos. Os ataques passivos só observam a comunicação e os dados e eventualmente copiam a informação. É no caso de acesso a senhas ou outros dados confidenciais. Os ataques ativos podem alterar o conteúdo da informação, como no acesso a sistemas, emails ou sessões TCP.

4.5. Protocolos de rede que implementam Criptografia

4.5.1. SSL (Secure Sockets Layer)

O protocolo SSL simula túneis seguros entre aplicativos, provendo a privacidade e a integridade de dados entre duas aplicações que estejam se comunicando pela Internet. Isto ocorre através da autenticação das partes envolvidas e da criptografia dos dados transmitidos

entre as partes. Esse protocolo ajuda a prevenir que intermediários entre as duas pontas da comunicação tenham acesso indevido ou falsifiquem os dados sendo transmitidos. É baseado no protocolo TCP e utiliza-se do conceito introduzido por Diffie-Hellman (criptografia de chave pública) e Philip Zimmermann (criador do conceito PGP).

Desenvolvido pela Netscape, o SSL versão 3.0 foi lançado em 1996, e serviu posteriormente de base para o desenvolvimento do TLS versão 1.0, que será abordado na próxima seção. Grandes instituições financeiras aprovaram o SSL para comércio eletrônico seguro na Internet. O SSL opera de forma modular, possui design extensível, e apresenta compatibilidade entre pares com versões diferentes do mesmo.

A utilização de SSL fornece encriptação no nível de aplicação, muito usado em navegadores de Internet, como em acessos a serviços bancários on line. Na prática, o servidor do site que está sendo acessado envia uma chave pública ao navegador, usada por este para enviar uma chamada secreta, criada aleatoriamente. Desta forma, fica estabelecida a troca de dados criptografados entre dois computadores. Uma das deficiências da encriptação no nível de aplicação é que ela protege somente os dados enviados pela aplicação que a está usando, mas não de todas as outras. Cada sistema ou aplicativo deve estar adaptado a SSL, para que uma segurança geral possa ser garantida.

O SSL descomplicou a questão da credibilidade, reduzindo o número de instituições em quem pode-se confiar, distribuindo essa confiança por todos os sites que adquirirem um certificado SSL. Os certificados digitais SSL oferecem uma autenticidade de que o site que se está visitando é realmente de quem pensa-se ser e também garantem, através da criptografia dos dados, que as informações fornecidas não poderão ser interceptadas no trajeto entre o computador do usuário e o servidor da empresa.

4.5.2. TLS (Transport Layer Security)

TLS e o seu predecessor, o SSL, são protocolos criptográficos que provêem comunicação segura na Internet para serviços como email (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados. Há algumas pequenas diferenças entre o SSL 3.0 e o TLS 1.0, mas o protocolo permanece substancialmente o mesmo.

O protocolo TLS é composto de duas camadas: o protocolo de Registro (TLS Record Protocol) e os protocolos Handshaking (TLS Handshaking Protocols).

O protocolo de Registro localiza-se acima de um protocolo de transporte confiável, como o TCP, e é quem realmente efetua as operações necessárias para garantir a segurança da

conexão. Ele recebe as mensagens para serem transmitidas, fragmenta os dados em blocos, opcionalmente realiza a compressão dos dados, aplica o MAC, encripta e transmite o resultado. Logicamente, com os dados recebidos, o protocolo de Registro realiza a deciptação, verificação da integridade, realiza descompressão, reagrupa os blocos e os entrega para as camadas superiores. O TLS utiliza esta camada para encapsular todas as mensagens dos demais protocolos das camadas superiores, explicando a sua independência com os protocolos de aplicação, facilitando o desenvolvimento de aplicações que necessitam de conexões seguras. Ele apresenta duas propriedades:

- Privacidade. É utilizada criptografia simétrica para encriptação dos dados. As chaves para cifragem são geradas unicamente para cada conexão e são baseadas em um segredo negociado por um outro protocolo, neste caso o protocolo Handshake. O protocolo de Registro pode ser usado sem criptografia.
- Confiabilidade. O transporte da mensagem inclui uma verificação da integridade da mensagem, utilizando uma keyed-HMAC (Hashing Message Authentication Code). Funções hash seguras são utilizadas para computação da MAC. O protocolo de Registro pode operar sem uma MAC, porém geralmente, só é utilizado desta maneira, enquanto outro protocolo está usando o protocolo de Registro como transporte para a negociação dos parâmetros de segurança.

Os protocolos Handshaking provêm segurança da conexão, permitindo a autenticação entre cliente e servidor e a negociação de algoritmos de encriptação e de chaves criptográficas antes da transmissão ou recepção do primeiro octeto de dados por parte de um protocolo de aplicação. São três subprotocolos que permitem às partes chegarem a um acordo sobre os parâmetros de segurança que serão utilizados na camada de registro para autenticação, comunicação e para reportar condições de erro entre as partes. Estes protocolos apresentam três propriedades:

- A identificação de uma das partes pode ser autenticada através da criptografia assimétrica. Esta autenticação pode ser opcional, mas geralmente é exigida para pelo menos uma das partes.
- A negociação de um segredo compartilhado é segura. O segredo negociado fica indisponível para terceiros. Para qualquer conexão autenticada o segredo não pode ser obtido, mesmo por um atacante que pode se colocar no meio da conexão.
- A negociação é confiável. Nenhum atacante pode modificar a comunicação da negociação sem ser detectado pelas partes legítimas da comunicação.

Uma vantagem do TLS é a independência em relação aos protocolos de aplicação. Protocolos de nível acima podem comunicar com o TLS de forma transparente.

4.5.3. HTTPS (HyperText Transfer Protocol Secure)

O HTTPS é uma implementação do protocolo HTTP sobre uma camada SSL ou do TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais. Este protocolo normalmente é utilizado quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros. A porta TCP usada por norma para o protocolo HTTPS é a 443.

4.5.4. IPSec (IP Security Protocol)

IPSec é um protocolo que opera sob a camada de rede (ou camada 3) do modelo OSI. Segundo a definição dada por Rezende (2007?), trata-se de uma extensão do protocolo IP, que estabelece um conjunto de padrões utilizados para garantir uma comunicação segura entre dois computadores, de forma transparente, independente do grau de segurança do canal por onde as informações forem enviadas. Com a utilização desse protocolo é possível garantir a confidencialidade e a integridade das comunicações com base em TCP/IP, também oferecendo suporte à autenticação com base em computadores.

É um protocolo que implementa encriptação e autenticação na camada de rede, fornecendo uma solução de segurança fim-a-fim. Ele torna-se completamente transparente para os aplicativos porque os serviços de criptografia, integridade e autenticação são implementados no nível de transporte. Pode ser implementado nos roteadores ou no sistema operacional dos terminais, de forma que os aplicativos não precisam de alterações para poder utilizar comunicações seguras. Os aplicativos continuam a se comunicar uns com os outros, da maneira habitual, usando as portas TCP e UDP.

Os dados, numa rede IP, são enviados em blocos referidos como pacotes ou datagramas. O IPSec define um novo conjunto de cabeçalhos a serem adicionados aos datagramas IP. Os novos cabeçalhos são colocados após o cabeçalho IP e antes do cabeçalho da camada superior (como o dos protocolos de transporte TCP ou UDP). Estes novos cabeçalhos é que dão as informações para proteção das informações (payload) do pacote IP:

- Authentication Header (AH): este cabeçalho, ao ser adicionado a um datagrama IP, garante a integridade e autenticidade dos dados, incluindo os campos do cabeçalho

original que não são alterados entre a origem e o destino; no entanto, não fornece confidencialidade. É utilizada uma função hash com chave, ao invés de assinatura digital, pois o mecanismo de assinatura digital é bem mais lento e poderia reduzir a capacidade da rede.

- Encapsulating Security Payload (ESP): este cabeçalho protege a confidencialidade, integridade e autenticidade da informação. Se o ESP for usado para validar a integridade, ele não inclui os campos invariantes do cabeçalho IP.

AH e ESP podem ser usados separadamente ou em conjunto, mas para a maioria das aplicações apenas um deles é suficiente. Para os dois cabeçalhos, o IPSec não especifica quais algoritmos de segurança devem ser utilizados, mas dá uma relação dos possíveis algoritmos, todos padronizados e bastante difundidos. Inicialmente, quase todas as implementações trabalham com MD5 (da RSA Data Security) e o Secure Hash Algorithm (SHA, do governo dos EUA) para integridade e autenticação. O DES é o algoritmo mais comumente usado para a encriptação dos dados, apesar de muitos outros estarem disponíveis, de acordo com as RFCs, como o IDEA, Blowfish e o RC4.

Para garantir um perfeito acordo entre a origem e o destino, dos algoritmos a serem utilizados e demais informações necessárias para a comunicação com o IPSec, são utilizadas associações de segurança (Security Associations, SA). O IPSec assume que as SAs já existem para ser utilizado, mas não especifica como elas serão criadas. O IETF decidiu dividir o processo em duas partes: o IPSec fornece o processamento dos pacotes, enquanto o IKMP (Internet Key Management Protocol) negocia as associações de segurança. Após analisar as alternativas disponíveis, o IETF escolheu o IKE (Internet Key Exchange) como o método padrão para configuração das SAs para o IPSec. Dessa forma, o gerenciamento de chaves, associações de segurança e os parâmetros para a comunicação IPSec entre dois dispositivos são negociados através do IKE, que utiliza Certificados Digitais (que garantem a identidade de uma pessoa, evitando a falsificação de identidades) para autenticação de dispositivos, permitindo a criação de grandes redes seguras. Sem o suporte dos Certificados Digitais, as soluções IPSec não seriam escaláveis para a Internet.

O IPSec fornece dois modos de operação, como mostrado nas figuras 8 e 9.

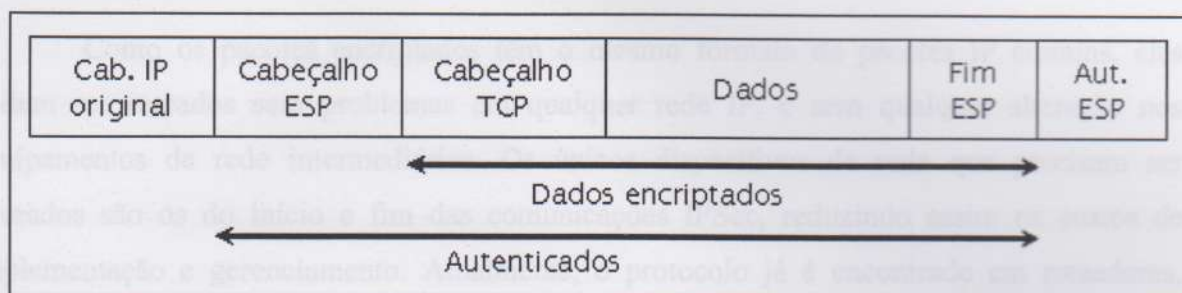


Figura 7. Cabeçalho genérico para o modo de transporte
Fonte: REZENDE. IPSec-Protocolo de Segurança IP.

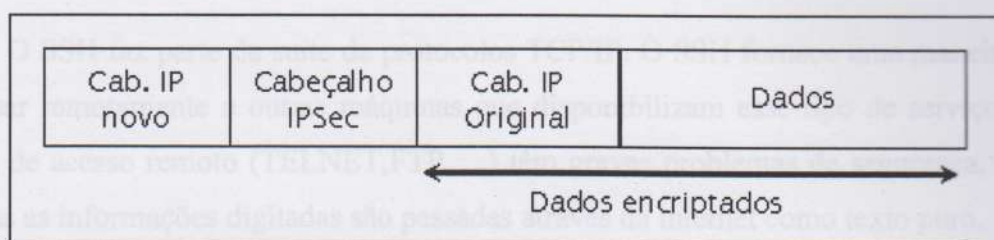


Figura 8. Exemplo de um cabeçalho do modo túnel
Fonte: REZENDE. IPSec-Protocolo de Segurança IP.

No **modo de transporte**, somente a informação (payload) é encriptada, enquanto o cabeçalho IP original não é alterado. Este modo tem a vantagem de adicionar apenas alguns octetos a cada pacote, deixando que dispositivos da rede pública vejam a origem e o destino do pacote, o que permite processamentos especiais (como de QoS) baseados no cabeçalho do pacote IP. No entanto, o cabeçalho da camada 4 (transporte) estará encriptado, limitando a análise do pacote. Passando o cabeçalho sem segurança, o modo de transporte permite que um atacante faça algumas análises de tráfego, mesmo que ele não consiga decifrar o conteúdo das mensagens.

No **modo de tunelamento**, todo o datagrama IP original é encriptado e passa a ser o payload de um novo pacote IP. Este modo permite que um dispositivo de rede, como um roteador, aja como um Proxy IPSec (o dispositivo realiza a encriptação em nome dos terminais). O roteador de origem encripta os pacotes e os envia ao longo do túnel IPSec; o roteador de destino decripta o datagrama IP original e o envia ao sistema de destino. A grande vantagem do modo de tunelamento é que os sistemas finais não precisam ser modificados para aproveitarem os benefícios da segurança IP; além disto, esse modo também protege contra a análise de tráfego, já que o atacante só poderá determinar o ponto de início e de fim dos túneis, e não a origem e o destino reais.

Como os pacotes encriptados têm o mesmo formato de pacotes IP comuns, eles podem ser roteados sem problemas em qualquer rede IP, e sem qualquer alteração nos equipamentos de rede intermediários. Os únicos dispositivos de rede que precisam ser alterados são os do início e fim das comunicações IPsec, reduzindo assim os custos de implementação e gerenciamento. Atualmente, o protocolo já é encontrado em roteadores, firewalls e em sistemas operacionais Windows e UNIX.

4.5.5. SSH (Secure SHell)

O SSH faz parte da suíte de protocolos TCP/IP. O SSH fornece uma maneira segura de acessar remotamente a outras máquinas que disponibilizam esse tipo de serviço. Outros serviços de acesso remoto (TELNET, FTP, ...) têm graves problemas de segurança, uma vez que todas as informações digitadas são passadas através da internet como texto puro.

Uma de suas mais utilizadas aplicações é o chamado Tunnelling, que oferece a capacidade de redirecionar pacotes de dados. O processo se caracteriza por duas máquinas ligadas ao mesmo servidor SSH, que faz apenas o redirecionamento das requisições do computador que está sob firewall. O processo ocorre da seguinte forma: o usuário envia para o servidor um pedido de acesso ao servidor ftp.xxxxxxxx.com pela porta 443 (HTTPS), por exemplo. Então, o servidor acessa o computador remoto e requisita a ele o acesso ao protocolo, retornando um conjunto de pacotes referentes à aquisição. O servidor codifica a informação e a retorna ao usuário via porta 443. Sendo assim, o usuário tem acesso a toda a informação que necessita. Tal prática não é ilegal caso o fluxo de conteúdo esteja de acordo com as normas da instituição.

O protocolo SSH utiliza criptografia de chave pública, que fornece autenticação e encriptação entre os hosts (cliente e servidor). Esse método usa uma chave pública para encriptação dos dados e uma chave privada para desencriptação. Assim, antes de um computador (A) estabelecer conexão com outro (B), eles passam por um processo de "reconhecimento" de troca de chaves públicas: A envia sua chave pública para B reconhecê-la, e B faz o mesmo com A. Feita a troca, a comunicação é estabelecida e mantida a segurança.

4.5.6. Kerberos

Kerberos é o nome de um protocolo de transporte de rede, que permite comunicações individuais seguras e identificadas, em uma rede insegura. Para isso o Massachusetts Institute

of Technology (MIT) disponibiliza um pacote de aplicativos que implementam esse protocolo. Ele utiliza Criptografia simétrica e necessita de um sistema de confiança tripla.

O protocolo Kerberos previne Eavesdropping e Replay attack, e ainda garante a integridade dos dados. Seus projetores inicialmente o modelaram na arquitetura cliente-servidor, sendo possível a autenticação mútua entre o cliente e o servidor, permitindo assim que ambos se autenticuem.

O Kerberos utiliza basicamente o protocolo Needham-Schroeder, algoritmo de criptografia simétrica, proposto por Roger Needham e Michael Schroeder, em 1978, que tem como objetivo estabelecer uma chave de sessão entre duas partes na rede, tipicamente para proteger comunicações à distância.

O Kerberos trabalha baseado em Tickets, utilizados para identificação dos usuários. O funcionamento do protocolo ocorre da seguinte forma: o cliente se autentica no Servidor de Autenticação, então demonstra para o Servidor de Concessão de Ticket que está autorizado a receber um Ticket para utilizar em um serviço (e o recebe), então demonstra ao Servidor de Serviço que ele está aprovado para receber um serviço. A mudança de senhas não foi padronizada, e difere entre as implementações existentes do servidor.

O principal problema do protocolo é a necessidade de uma disponibilidade contínua do servidor central. Quando o servidor do Kerberos está indisponível, ninguém pode mais se autenticar na rede. Isso pode ser resolvido utilizando diversos servidores Kerberos. Além disso, o Kerberos necessita que os relógios internos dos clientes estejam sincronizados com o dele. Os Tickets têm um tempo de vida e se o relógio do cliente não estiver sincronizado com o do servidor, a autenticação irá falhar. Na configuração padrão, é necessário que os relógios dos clientes não tenham uma diferença maior do que 10 minutos. Na prática, servidores NTP (Network Time Protocol) são utilizados para manter os relógios do servidor e dos clientes sincronizados.

4.6. Criptografia na Internet

A Internet é um espaço mundial descentralizado onde cada um pode agir, expressar e trabalhar sem ser controlado, até o presente momento, por nenhum estado ou empresa. Ela tem sido uma revolução para o comércio e para as transferências de dados em geral, as quais trouxeram novas oportunidades de negócios para todos, desde as grandes corporações, empresas em geral e mesmo indivíduos. Este desenvolvimento não está ocorrendo sem ameaças. Neste espaço revolucionário de comunicação, os riscos de fraudes, falsificações e

espionagens, autorizadas ou não pelo governo, são imensos. Além disso, o comércio eletrônico tem atraído crimes e desenvolveu uma nova legião de criminosos online, que vão desde fraudadores e hackers até terroristas cibernéticos.

Portanto, pelo caráter de abertura irrestrita, a Internet torna-se o meio ambiente adequado a todas as formas de delitos ligados à informática. As mensagens, desejadas como confidenciais, podem ser facilmente interceptadas, lidas, copiadas, adulteradas. Documentos ou informações sensíveis em circulação podem ser contestados em sua identidade. Informações sensíveis podem cair em mãos concorrentes (no caso de empresas), de agentes estrangeiros (para mensagens secretas diplomáticas ou militares secretas) ou em mãos de criminosos, que buscam oportunidades para ganhos desonestos.

Estas ameaças contribuem para minar a confiança dos usuários desta plataforma de comunicação e dificulta o desenvolvimento de uma cultura digital que favoreça o uso da web de modo amplo, compreendendo o comércio eletrônico e os serviços bancários. A crescente preocupação em como conduzir negócios online resultou no fato de que a segurança é fator fundamental para o sucesso dos negócios na internet.

Como solução para este dilema, a criptografia surgiu como guardião deste tesouro de comunicação sem fronteiras e tem a estratégica tarefa de garantir a segurança do sistema. Confiando nisto, o mercado está se educando com relação à segurança online e a maioria dos usuários agora tem a expectativa de segurança em todos os serviços que eles utilizam na internet garantindo deste modo que as informações que eles forneçam estejam seguras durante todo o processo.

4.6.1. Utilização de Criptografia em Emails

Simple Mail Transfer Protocol (SMTP) é o protocolo padrão para envio de e-mails através da Internet. É um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados) sendo, depois, a mensagem transferida. Por suportar apenas 7-bit de caracteres ASCII, este protocolo limita as mensagens de emails, incluindo somente os caracteres usados na língua inglesa. O MIME provê mecanismos para o envio de outros tipos de informação por e-mail, incluindo caracteres não utilizados no idioma inglês usando codificações diferentes do ASCII, assim como formatos binários contendo imagens, sons, filmes e programa de computadores, neste caso conhecido como SMTP/MIME (S/MIME).

Tem sido cada vez mais freqüente o uso da criptografia no envio e recebimento de emails. Uma vez que os pacotes de informação são transmitidas de servidor em servidor pela internet até chegar ao computador de destino, qualquer pessoa pode monitorar esses pacotes e obter seu conteúdo. Utilizando a criptografia, assegura-se que apenas o destinatário compreenderá o conteúdo da mensagem. Para usar criptografia ao enviar e receber emails, primeiro deve-se obter uma identificação digital de uma autoridade de certificação. Essa identificação contém uma chave privada que é armazenada no computador do remetente e um certificado (com uma chave pública). Este certificado é enviado quando se assina digitalmente as mensagens para ajudar a autenticá-lo para o destinatário. Também, utiliza-se o certificado para criptografar as mensagens. Os certificados são validados por meio de uma hierarquia de certificados. A autoridade de certificação raiz fica no topo de uma hierarquia de certificação e é a autoridade de certificação mais confiável. Essa autoridade de certificação tem um certificado auto-assinado, portanto, é importante obter certificados somente de autoridades de certificação que sejam conhecidas e confiáveis.

No caso do correio eletrônico, as coisas são ainda um pouco mais complicadas, pois não existe dificuldade nenhuma em enviar emails falsos. Qualquer pessoa pode acessar um servidor de email e redigir uma mensagem em nome de quem se deseje, sendo necessário apenas configurar o programa de email para que envie mensagens com o email dessa pessoa. Isso não se configura como uma vulnerabilidade, mas sim uma característica do serviço de email, devido à própria arquitetura do sistema de email existente na internet.

Para Rhatto (2006), na Internet existem três tipos de programas de email: os programas do tipo MTA (Mail Transport Agent), os MDA (Mail Delivery Agent) e ou MUA (Mail User Agent). Os Mail Transport Agents (ou Agentes de Transporte de Emails), conhecidos como servidores SMTP, são aqueles programas que enviam a mensagem de email para o servidor de destino, que pode ser, por exemplo, o servidor de emails do provedor de internet usado pelo destinatário da mensagem. Os MDAs (Agentes de Entrega de Email), também são conhecidos como servidores POP ou IMAP, são os programas que enviam a mensagem até o usuário de destino, e para que este usuário possa receber a mensagem ele deve utilizar um programa do tipo MUA, que são os programas de email propriamente ditos. Já os clientes de email (MUAs) podem ser tanto um site de Webmail como os programas do tipo Mail (MacOSX), Mozilla Mail, etc.

Rhatto (2006) explica que o caminho que uma mensagem de correio eletrônico ocorre da seguinte forma:

- o remetente da mensagem utiliza seu respectivo cliente de email (MUA) para enviar a mensagem até o seu programa MTA, que pode ser o servidor SMTP do seu provedor ou até mesmo ser um programa rodando no computador do remetente.
- esse MTA, por sua vez, envia essa mensagem até o MTA do usuário de destino.
- quando o destinatário verificar suas novas mensagens, basta que ele utilize seu cliente de email (MUA) para se conectar até seu servidor POP ou IMAP (MDA) e receber suas mensagens.

Em todo esse processo não existe verificação do email de origem da mensagem, isto é, uma vez que o remetente se conectou em smtp.remetente.br ele pode escolher qualquer email de origem, não precisando ser um email válido. Isso acontece porque normalmente os servidores SMTP só requerem usuário e senha para serem utilizados e eles não fazem nenhuma verificação de destinatário. Às vezes esses servidores estão desconfigurados e não precisam nem de senha para serem utilizados, sendo então muito usados para SPAM (mala direta). Já os servidores tipo MDA (pop3, imap, webmail) requerem usuário e senha para fornecerem o acesso à uma conta de email, o que impede as pessoas de receberem o email de outras pessoas. Além disso, qualquer pessoa pode rodar seu próprio programa de SMTP e com isso enviar mensagens em nome de outras pessoas. Desta forma, além de criptografar as mensagens, é muito útil assinar com chave pública as mensagens de email que se envia., para garantir autenticidade e não repúdio, o que também é possível com a utilização de um certificado digital.

4.6.2. Uso de criptografia nos navegadores

Quando um usuário usa um navegador web para se conectar a um site utilizando o protocolo de conexão segura, o navegador e o servidor do site trocam automaticamente suas respectivas chaves públicas e então é iniciada uma transmissão de informações criptografadas. O navegador não envia ao servidor a chave pública do usuário, mas sim uma chave própria criada automaticamente pelo navegador, de tal forma que não se precise de nenhum programa adicional de criptografia. Tudo isso é feito de forma praticamente transparente ao usuário.

Um usuário, ao conectar-se a um servidor que está utilizando o protocolo SSL, pode notar, na barra de endereços do navegador, que o protocolo passa a ser o HTTPS. Aliado a isto, a maioria dos navegadores mostram um tradicional cadeado, como ilustrado na Figura 7, garantindo que as informações fornecidas àquele website não poderão ser interceptadas no seu trajeto.

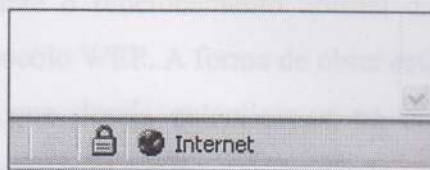


Figura 9. Exemplo de um navegador acessando um site que utiliza o protocolo SSL

4.7. Criptografia em redes Wireless

Para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados, que possuam características de segurança que garantam a compatibilidade entre conexões com e sem fios, e possibilitem a execução de aplicativos sem riscos. Basicamente, a segurança que deve ser adicionada encontra-se no nível de enlace de dados, pelo fato dos aplicativos e protocolos de níveis superiores terem sido desenvolvidos contando com a segurança física disponível nas redes com fios.

Nas redes locais sem fio (WLAN), especificadas no padrão da IEEE (*Institute of Electrical and Electronics Engineers*) como IEEE 802.11, toda autenticação deve ser realizada entre pares de estações, nunca havendo comunicação *multicast*. Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do *Access Point*. Segundo Peres e Weber (200?), o padrão IEEE 802.11 define duas formas de autenticação:

- Autenticação *Open System* - é o sistema de autenticação padrão sendo que, neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo. Foi desenvolvida focando redes que não necessitam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção. Normalmente, estas redes permanecem separadas da rede interna por um *firewall* (a semelhança de uma zona desmilitarizada – DMZ).
- Autenticação *Shared key* - nesta autenticação, é utilizado mecanismos de criptografia para realizar a autenticação dos dispositivos. Ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta, que é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de

informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP. A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.
3. A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4. O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

Na próxima seção, serão apresentados com detalhes os principais protocolos utilizados na segurança de rede wireless, abordando como cada um deles utiliza-se da criptografia para garantir a confidencialidade dos dados.

4.7.1. Protocolos de segurança em redes Wireless

4.7.1.1. WEP (Wired Equivalent Privacy)

A segurança no nível de enlace, que deveria garantir a compatibilidade entre conexões com e sem fios, foi prevista no padrão IEEE 802.11, através do protocolo WEP (Wired Equivalent Privacy). Segundo Peres e Weber (200?), este protocolo possui as seguintes características:

- é um protocolo razoavelmente robusto, devido à necessidade de grande esforço computacional para descoberta da chave secreta;
- pode ser implementado tanto em hardware como em software;
- possui capacidade de autossincronização, como forma de amenizar o impacto das grandes taxas de perda de mensagens, comuns em redes sem fio. A cada nova mensagem, existe uma sincronização entre as entidades e a escolha de uma nova chave criptográfica, de forma que o segredo permanece o mesmo, enquanto a chave é alterada. Não havendo nova sincronização, a perda de uma mensagem acarreta na impossibilidade de decifragem das subseqüentes, tendo em vista o funcionamento do algoritmo de cifragem;

- pode ser exportado dos Estados Unidos - devido à política de exportação de sistemas criptográficos norte-americana na época em que foi desenvolvido, cuidados foram tomados para que esse governo aprovasse a exportação de equipamentos que utilizassem este protocolo; e
- sua utilização é opcional.

Trata-se de um protocolo de criptografia baseado no uso de chaves criptográficas trocadas entre pares de estações. A implementação da criptografia é com base no método RC4, da RSA, que usa um VI (Vetor de Inicialização) de 24 bits e uma chave secreta compartilhada de 40 ou 104 bits. O VI é concatenado com a chave secreta compartilhada para formar uma chave de 64 ou 128 bits, que é usada para criptografar os dados. O resultado serve de entrada para um gerador de números pseudo-aleatórios, PRNG (Pseudo Random Number Generator), que é baseado no algoritmo RC4. A saída do PRNG é uma seqüência pseudo-aleatória de bits baseada na chave composta e com o mesmo tamanho do texto a ser criptografado. Para cada quadro, o protocolo WEP deve selecionar um VI diferente, permitindo que a chave secreta permaneça a mesma, enquanto a semente é alterada, mantendo o sincronismo. Como o destinatário da mensagem deve criar a chave de decifragem a partir da mesma semente, o remetente envia o VI escolhido sem criptografia com o quadro. Desta forma, o destinatário pode unir o segredo compartilhado com o VI escolhido e utilizar estas informações como semente no PRNG. Para verificar que os dados não foram alterados durante a comunicação, é utilizado um algoritmo redundante do tipo CRC-32 (Cyclic Redundancy Check) denominado ICV - Integrity Check Value.

Apesar de muito utilizado, o protocolo WEP provou-se ineficiente em uma série de estudos e a sua principal falha de segurança está na própria arquitetura. O motivo deste fato vem da possibilidade de um atacante obter uma chave (não a semente, mas a chave utilizada nas operações XOR) e com ela obter os dados cifrados com a mesma chave em outro momento. Nesse sentido, uma chave WEP nunca deve ser reutilizada. Para isso, no momento em que o número de possíveis VIs for esgotado, o segredo deverá ser modificado.

4.7.1.2. TKIP (Temporal Key Integrity Protocol)

O TKIP é um protocolo baseado em chaves que se alteram a cada novo envio de pacote. A sua principal característica é a freqüente mudança de chaves, o que garante maior segurança. Segundo Azambuja (2007), o funcionamento dele ocorre da seguinte forma: o dispositivo começa com uma chave-base secreta de 128 bit, chamada de TK (Temporal Key), então ela é combinada com o TA (Transmitter Address), o endereço MAC do transmissor,

criando a chave chamada TTAK (Temporal and Transmitter Address Key) - ou a Chave da Fase 1. A TTAK é então combinada com o vetor de inicialização, de 48 bits e não previsível, para criar as chaves que variam a cada pacote, chamadas de RC4KEY ou PPK.

4.7.1.3. WPA (Wi-Fi Protected Access)

Este protocolo surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP. O WPA é baseado no RC4 e em um subconjunto de especificações apresentadas em uma versão preliminar do IEEE 802.11i.

Segundo Linhares e Gonçalves (2006), o WPA introduz diversos mecanismos para resolver os problemas de segurança associados ao WEP. Como os 24 bits de VI, utilizado pelo WEP, permitiam pouco mais de 16 milhões de VI diferentes, facilitando repetições em um curto espaço de tempo, o WPA introduz um VI estendido de 48 bits. Assim, mais de 280 trilhões (248) de IVs diferentes são possíveis. Adicionalmente, o WPA introduz regras para a escolha e verificação de IVs para tornar ataques de reinjeção de pacotes ineficazes. O WPA usa um novo campo de 64 bits, o MIC (Message Integrity Code), para verificar se o conteúdo de um quadro de dados possui alterações por erros de transmissão ou manipulação de dados. O MIC é obtido através de um algoritmo conhecido como Michael. Além disso, o WPA automaticamente distribui e deriva chaves que serão utilizadas para a criptografia e integridade dos dados. Isto resolve o problema do uso da chave compartilhada estática do WEP. Ele não tem suporte a redes do tipo ad hoc de forma diferente ao WEP e foi projetado para ser implementado através de uma atualização de software (firmware) nos equipamentos existentes com o hardware utilizado pelo WEP.

Há dois tipos de autenticação no protocolo WPA, um direcionado para redes corporativas que utiliza um servidor de autenticação 802.1x/EAP, portanto uma infraestrutura complementar, e um outro, mais simples, projetado para pequenas redes em escritórios e para redes domésticas (redes SOHO – Small Office/Home Office). Estes dois tipos de autenticação são denominados WPA Corporativo e WPA Pessoal, respectivamente.

A integridade no WPA é composta por dois valores. Além do ICV, já utilizado pelo WEP, é adicionado ao quadro uma mensagem de verificação de integridade denominada MIC (Message Integrity Check). O algoritmo que implementa o MIC denomina-se Michael. O Michael é uma função hash não linear, diferentemente do CRC-32. O endereço de destino, de

origem, a prioridade (definida atualmente como zero, mas reservada para objetivos futuros, e.g. 802.11e), os dados e uma chave de integridade são inseridos no Michael para produzir o MIC. A saída corresponde a 8 bytes que juntamente com o ICV formam a integridade do protocolo WPA. Portanto a integridade é representada por um total de 12 bytes, 8 gerados pelo Michael e 4 pelo CRC-32.

O WPA utiliza o conceito de chaves temporais, no qual há uma hierarquia de chaves. Há uma chave principal, chamada de Pairwise Master Key (PMK), de onde se derivam outras chaves como a chave de criptografia de dados e a chave de integridade de dados. O TKIP é o responsável por essa implementação, possibilitando a criação de chaves por pacotes. Ele soluciona boa parte das vulnerabilidades apresentadas pelo protocolo WEP. No WPA o vetor de inicialização possui 48 bits o que torna praticamente impossível haver reutilização de vetores. Na estrutura do cabeçalho 802.11 o campo reservado para o VI só contém 24 bits, devido a isto criou-se outro campo chamado VI Extended, que não faz parte da estrutura do cabeçalho 802.11, para alocar o resto do VI. O VI também é utilizado como um contador de quadros (TSC – TKIP Sequence Counter). Quando uma nova chave de criptografia é estabelecida, o TSC é zerado. A cada quadro transmitido, ele é incrementado. Desta forma, quadros com TSC fora de ordem são descartados, evitando-se reinjeções de pacotes.

O processo de codificação do WPA é semelhante ao do WEP. A principal diferença está na chave que irá alimentar o RC4. Esta chave é o resultado de um algoritmo de combinação de chave cuja entrada é o vetor de inicialização, o endereço MAC do transmissor e a chave de criptografia de dados. Ao final, a chave gerada pelo algoritmo de combinação de chave e o VI são passados para o RC4 e o processo ocorre conforme visto no WEP. A Figura 10 ilustra o funcionamento do WPA.

Para Linhares e Gonçalves (2006), o WPA solucionou praticamente todas as vulnerabilidades apresentadas pelo protocolo WEP, porém, falhas em sua implementação o tornaram vulnerável.

4.7.1.4.WPA2

O padrão IEEE 802.11i, também conhecido como WAP2, foi homologado em junho de 2004 e desenvolvido com o objetivo de prover mais segurança na comunicação, visto que o protocolo de segurança então utilizado (WEP) apresentava diversas vulnerabilidades. Segundo Linhares e Gonçalves (2006), o novo método de criptografia utilizado exige um maior poder computacional do NIC (Network Interface Card) durante o processo de codificação/decodificação, impossibilitando assim, apenas uma atualização de firmware.

Parte dos mecanismos apresentados no WPA também é utilizada no WPA2, já que o WPA é baseado em um rascunho do WPA2. Os principais avanços do WPA2 em relação ao WPA são, basicamente, novos algoritmos de criptografia e de integridade.

O mecanismo de autenticação no WPA2 é, basicamente, o mesmo do WPA. O maior avanço na autenticação é uma preocupação com o roaming. Quando um usuário se autentica, há uma série de mensagens trocadas entre o AP e o cliente. Essa troca de mensagens introduz um atraso no processo de conexão. Quando um cliente desloca-se de um AP para outro, o atraso para estabelecer a associação pode causar uma interrupção notória da conexão, principalmente em tráfego de voz e vídeo. Para minimizar este atraso de associação, o equipamento pode dar suporte a PMK Caching e Preauthentication. O PMK Caching consiste no AP guardar os resultados das autenticações dos clientes. Se o cliente voltar a se associar com o AP, estas informações guardadas são utilizadas para diminuir o número de mensagens trocadas na re-autenticação. Já no Preauthentication, enquanto o cliente está conectado a um AP principal, ele faz associações com outros APs cujo o sinal chega até ele. Desta forma, quando há uma mudança de AP não há perda de tempo com a autenticação. O protocolo CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) é o responsável pela integridade e a confidência do WPA2. O CCMP é baseado no AES (Advanced Encryption Standard) que é um Block Cipher13. O modo de operação do AES implementado pelo WPA2 é o CCM cujas chaves e blocos são de 128 bits. O CBC-MAC (Cipher Block Chaining Message Authentication Code) é responsável pela integridade dos quadros.

O CCMP também é baseado no conceito de chaves temporais, como o TKIP no WPA. Portanto, no WPA2 há uma hierarquia de chaves, onde derivações da PMK geram as chaves temporais de criptografia e integridade. O algoritmo responsável pela criptografia do frame é o AES Counter Mode (CTR). A chave de criptografia de dados é simétrica e de tamanho 128 bits. O vetor de inicialização continua com 48 bits. Poucas vulnerabilidades são conhecidas sobre o WPA2 atualmente.

4.7.1.5. IEEE 802.11w

Segundo Linhares e Gonçalves (2006), o IEEE 802.11i possui melhorias significativas de segurança. Contudo, assim como no WEP e no WPA, toda a segurança é aplicada somente aos quadros de dados (data frames) e nenhuma proteção é dada aos quadros de gerenciamento (management frames) e de controle (control frames) do meio de comunicação sem fio. O Grupo de Trabalho do IEEE 802.11w foi aprovado em março de 2005 com o objetivo inicial

de melhorar a segurança das redes IEEE 802.11 através da proteção dos quadros de gerenciamento. Isso se deve a duas razões principais:

1. Os ataques do tipo DoS em redes IEEE 802.11 exploram a falta de proteção nos quadros de gerenciamento. Esses ataques injetam na rede quadros de gerenciamento do tipo deauthentication forjando facilmente pedidos de desassociação da rede de clientes legítimos. Assim, a proteção dos quadros de gerenciamento impediria a realização deste tipo de ataque;
2. Os novos padrões IEEE 802.11v, 802.11k e 802.11r estendem as funcionalidades dos quadros de gerenciamento 802.11, que poderão incluir informações sensíveis como dados sobre recursos de rádio, identificadores baseados em localização e dados para execução de handoffs¹⁴ rápidos. Desta forma, torna-se evidente a necessidade de proteção dos quadros de gerenciamento.

Linhares e Gonçalves (2006) ressalta que o padrão IEEE 802.11w está previsto para ser concluído em 2008. Assim sendo, tanto o objetivo inicial do grupo quanto os mecanismos de segurança propostos podem mudar drasticamente até a publicação da especificação final.

4.7.1.6.IEEE 802.1X (RFC 3580)

O padrão IEEE 802.1x especifica um mecanismo para autenticação de dispositivos e/ou usuários através da utilização de variações do protocolo EAP - Extensible Authentication Protocol [13]. O protocolo EAP, na sua definição, permite a utilização de uma grande variedade de mecanismos de autenticação. Segundo Linhares e Gonçalves (2006), a forma de funcionamento deste protocolo é baseada na troca de mensagens do tipo texto-desafio. A união do padrão EAP com a utilização do protocolo TLS - Transport Layer Security gerou a proposta de protocolo PEAP para utilização com o padrão IEEE 802.1x, da seguinte maneira:

1. a estação notifica o AP que deseja autenticar-se, e envia uma lista de algoritmos criptográficos suportados por ela;
2. o AP repassa esta mensagem para uma estação autenticadora localizada na rede da instituição. Esta estação é chamada back-end server. O AP não dá acesso para a rede ao dispositivo enquanto este não for autenticado;
3. o back-end server responde (através do AP) com um identificador de seção, uma lista de algoritmos criptográficos selecionados e uma chave pública;
4. a estação gera o segredo compartilhado, e cifra esta informação utilizando a chave pública do back-end server;

5. o back-end server envia para a estação uma mensagem cifrada com o segredo, finalizando a autenticação.

Como o EAP permite diferentes tipos de autenticação, alguns fabricantes adotam modelos diferentes do citado. A CISCO, por exemplo, propõe a utilização de autenticação mútua entre rede e dispositivo. O back-end-server poderá ser, por exemplo, um servidor RADIUS - Remote Access Dial-In User Service.

Após a troca inicial de chave pública e segredo, as estações podem trocar qualquer informação que desejarem como, por exemplo, dados para autenticação do usuário ou renovar o segredo compartilhado pelo WEP.

O padrão também especifica que todos os APs devem estar conectados ao mesmo back-end-server. Com isto, ao migrar entre dois APs, uma estação mantém a mesma chave de seção, simplesmente informando ao novo AP o identificador da seção que está utilizando.

Neste protocolo, não existe forma de verificar se a chave pública realmente pertence ao back-end server, devido a falta de uma entidade de certificação que assine esta chave. O padrão autentica a estação na rede, mas não garante a autenticação da rede para a estação. É possível que um atacante apresente-se como o AP para um dispositivo. Este dispositivo tentará se autenticar com o back-end server enviando seus dados diretamente para o atacante. Quando isto acontecer, o atacante se porta como um equipamento requisitando autenticação para o AP real, como demonstra a figura 10 (a). Desta forma, todo o tráfego da seção passará pelo atacante. No momento de estabelecer a seção TLS, o atacante fornece uma chave de seção para o back-end server e cria outra seção com o dispositivo alvo, efetuando um ataque do tipo "man-in-the-middle". Este mesmo ataque pode ser efetuado em protocolos de autenticação mútua sem autoridade certificadora.

Outro problema presente neste protocolo é a possibilidade de seqüestro de seção como mostra a figura 10 (b). Um atacante pode (1) enviar para uma estação já autenticada uma mensagem de desautenticação, fazendo-se passar pelo back-end-server. Desta forma, o alvo é desassociado (2), enquanto o back-end server mantém internamente o estado do dispositivo como conectado. Basta ao atacante assumir a identidade (endereço MAC) do alvo para se associar à rede (3). Este ataque só é possível graças a falta de autenticação presente nos quadros da rede sem fio. Este tipo de mensagem também pode causar um ataque de negação de serviço, desassociando as estações e impedindo a troca de mensagens. Estão em estudos algumas alternativas para aprimorar o protocolo IEEE 802.1x.

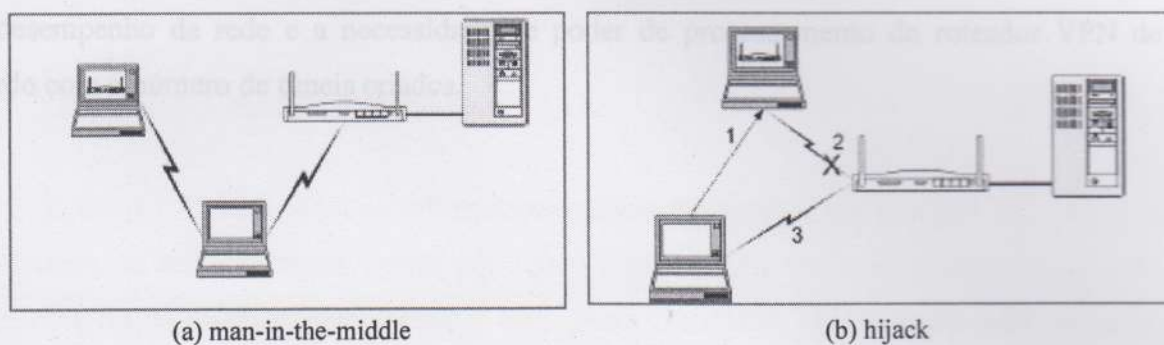


Figura 10. Ataques man-in-the-middle e hijack

Fonte: PERES e WEBER. Considerações sobre Segurança em Redes Sem Fio. p.6

4.7.2. Segurança em rede Wireless com VPN

Para Peres e Weber (2007), uma possível solução para a comunicação em redes sem fio é a implementação de segurança com redes VPN (Virtual Private Networks), utilizando um protocolo de criptografia como o IPSec. Com VPN, não há necessidade de se preocupar com a segurança dos protocolos nas camadas superiores. Um exemplo da utilização de redes VPN em um ambiente sem fio é apresentado na figura 11.

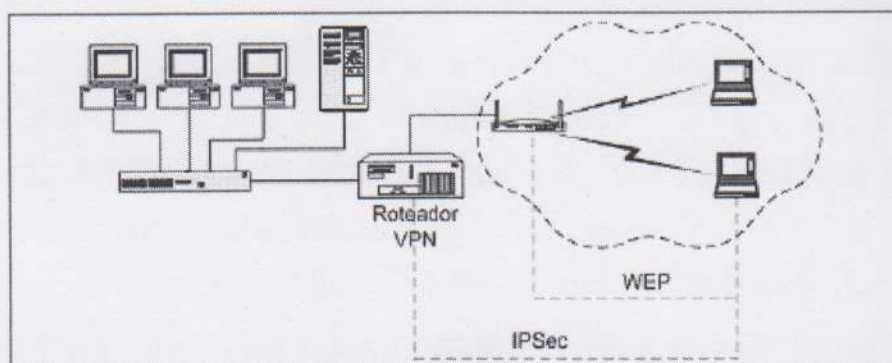


Figura 11. Rede WLAN com VPN/IPSec

Fonte: PERES. Considerações sobre Segurança em Redes Sem Fio. p.7

Para que a rede sem fio utilize VPN é necessário que todos os dispositivos sem fio (com exceção do AP) suportem VPN, e que exista um equipamento na fronteira da rede interna que faça a decifragem dos dados para a rede interna.

As informações dos níveis abaixo do nível de rede não são cifradas pelo IPSec. Isto significa que um atacante pode obter informações do nível de enlace para obter acesso à rede sem fios. Esta solução impede apenas que o atacante recupere os dados de uma comunicação

(acima do nível de rede) de forma legível. Deve ser observado o impacto deste tipo de solução no desempenho da rede e a necessidade de poder de processamento do roteador VPN de acordo com o número de túneis criados.

Como na Internet todas as informações passam de servidor em servidor até chegar ao seu destino, se essa mensagem passar por algum servidor controlado por pessoas maliciosas, as mensagens de email podem ser lidas com muita facilidade. Nessa seção, será abordado alguns programas de email que suportam criptografia, apresentando algumas características de cada um e a utilização desse recurso pelo usuário.

3.1.1. Microsoft Office Outlook 2003

Para ajudar a impedir a interceptação e a violação de emails no Microsoft Office Outlook 2003, são utilizados recursos como assinaturas digitais S/MIME e criptografia.

O Outlook 2003 usa certificados em emails criptografados para ajudar a fornecer comunicações mais seguras. Quando uma mensagem é assinada digitalmente, o certificado e a chave pública do remetente são adicionados à mensagem. Os certificados também são usados para criptografar uma mensagem.

O programa permite obter as características de um certificado (do próprio usuário ou anexado a um email recebido), para exibir a hierarquia de confiabilidade do certificado e ver quem emitiu o certificado no topo dessa hierarquia, determinar o algoritmo de assinatura usado pelo certificado (por exemplo, RSA/SHA1) ou determinar o algoritmo de criptografia usado pelo certificado (por exemplo, DES).

Para exibir as informações sobre o certificado usado para criptografar ou assinar digitalmente um email enviado, basta abrir a mensagem e clicar no botão de criptografia na extremidade direita do envelope. No caso de mensagens assinadas ou criptografadas e anexadas, na caixa de diálogo seguinte (por exemplo, a caixa de diálogo Assinatura Digital Válida), clique em Detalhes. Na caixa de diálogo Propriedades de Segurança de Mensagem, é possível ver as propriedades da mensagem, incluindo as camadas de segurança. Ao clicar em uma camada de segurança é possível ver a descrição dessa camada.

É possível, também, exibir informações adicionais sobre o certificado em uma aba de detalhes em uma camada de segurança, como descobrir porque o Outlook de um usuário que o certificado de um email é inválido ou não confiável. Em algumas situações, também pode-se executar procedimentos para corrigir o status do certificado, optando por aceitar as

Capítulo 5 – Soluções criptográficas em softwares

5.1. Programas de Email

Como na internet todas as informações passam de servidor em servidor até chegar no seu destino, se essa mensagem passar por algum servidor controlado por pessoas maliciosas, as mensagens de email podem ser lidas com muita facilidade. Nessa seção, será abordado alguns programas de email que suportam criptografia, apresentando algumas características de como é a utilização desse recurso pelo usuário.

5.1.1. Microsoft Office Outlook 2003

Para ajudar a impedir a representação e a violação de emails no Microsoft Office Outlook 2003, são utilizados recursos como assinaturas digitais S/MIME e criptografia.

O Outlook 2003 usa certificados em emails criptografados para ajudar a fornecer comunicações mais seguras. Quando uma mensagem é assinada digitalmente, o certificado e a chave pública do remetente são aplicados à mensagem. Os certificados também são usados para criptografar uma mensagem.

O programa permite obter as características de um certificado (do próprio usuário ou anexado a um email recebido), para exibir a hierarquia de confiabilidade do certificado e ver quem emitiu o certificado no topo dessa hierarquia, determinar o algoritmo de assinatura usado pelo certificado (por exemplo, RSA/SHA1) ou determinar o algoritmo de criptografia usado pelo certificado (por exemplo, 3DES).

Para exibir as informações sobre o certificado usado para criptografar ou assinar digitalmente um email enviado, basta abra a mensagem e clicar no botão de criptografia na extremidade direita do cabeçalho. No caso de mensagens assinadas, ou criptografadas e assinadas, na caixa de diálogo seguinte (por exemplo, a caixa de diálogo Assinatura Digital: Válida), clica-se em Detalhes. Na caixa de diálogo Propriedades de Segurança de Mensagem, é possível ver as propriedades da mensagem, incluindo as camadas de segurança. Ao clicar em uma camada de segurança é possível ver a descrição dessa camada.

É possível, também, exibir informações adicionais sobre o certificado ou fazer alterações em uma camada de segurança, como descobrir porque o Outlook determinou que o certificado de um email é inválido ou não confiável. Em algumas situações, também pode-se executar procedimentos para corrigir o status do certificado, optando por confiar na

autoridade de certificação que emitiu o certificado, se um certificado de assinatura digital não for confiável por esse motivo.

5.1.2. Mozilla Mail / Thunderbird

O Mozilla, na verdade, é um navegador (browser) para Internet de código aberto, mas possui um bom programa de email, que tem amplo suporte a criptografia. É possível utilizar o Mozilla Mail e o Thunderbird nos sistemas operacionais Windows, Linux ou MacOS. Para fazer uso de criptografia nestes dois programas, deve-se instalar o software Enigmail e fazer as configurações necessárias.

O Thunderbird é uma versão do Mozilla Mail mais econômica, em termos de custo computacional, por ter melhor desempenho que o Mozilla Mail em computadores mais lentos. Em conjunto com o Thunderbird, é recomendável que seja utilizado o Firefox como navegador Web, que é uma versão leve do Mozilla.

Conforme apresentado por Rhatto (2006), para instalação do Mozilla Mail e para habilitá-lo para o uso de criptografia, é necessário instalar o GPG e depois fazer as configurações gerais do Mozilla Mail, para conta de email. Em seguida, deve-se instalar o software Enigmail. Em seguida, deverá ser escolhido o par de chaves que o Enigmail utilizará. Existem três opções: gerar um par de chaves pelo próprio Enigmail, gerar utilizando outro programa de criptografia e utilizá-lo no Enigmail ou então usar um par de chaves existente. Enigmail. Caso as chaves tenham sido geradas num outro programa, basta informar ao Mozilla Mail, o **ID da chave pública** já existente. Para realizar o envio de mensagens cifradas é só compor uma mensagem normalmente e enviá-la apertando o botão **EnigSend**. O Enigmail normalmente está configurado para automaticamente decodificar mensagens que forem recebidas pelo Mozilla Mail.

A instalação do Enigmail no Thunderbird é similar à do Mozilla Mail, porém a menor integração entre o navegador e o leitor de emails faz com que algumas configurações tenham que ser feitas manualmente:

5.2. Criptografia em listas de discussão

Existem alguns softwares que já permitem o uso de criptografia em pequenas listas de discussão por email, funcionando da seguinte forma: a lista possui uma chave pública e a chave pública de todos os assinantes. Quando alguém quiser mandar uma mensagem

criptografada para a lista, basta criptografá-la apenas para a chave pública da lista que a lista irá descriptografá-la, criptografar e enviar individualmente para cada assinante usando sua respectiva chave pública.

Os seguintes softwares de lista de discussão suportam criptografia padrão OpenPGP:

- Firma: é um programa pequeno e eficiente gerenciador de listas criptografadas; ele foi desenvolvido para ignorar mensagens enviadas à lista que não estejam criptografadas e assinadas
- Mailman: o mailman é um software de listas que possui suporte parcial à criptografia através dos patches (remendos) NAH6 e GPG-Mailman

5.3. Assinatura digital como proteção de software

As assinaturas digitais permitem que qualquer tipo de arquivo seja assinado, garantindo a autenticidade de quem produziu aquele arquivo. Para os desenvolvedores de software, é muito conveniente assinar os arquivos dos programas que escrevem, pois assim é garantem aos usuários, que os programas que escreveram estão livres de vírus ou rotinas que podem comprometer a privacidade e o sistema dos usuários.

Tudo que o usuário precisa fazer é, além de baixar o código ou o programa já pronto, baixar a chave pública do programador e também um arquivo contendo a assinatura do programa, feita pelo programador, e verificá-la como se estivesse verificando a assinatura de um arquivo comum.

5.4. Criptografia de arquivos

Com a popularização da informática, e também devido ao compartilhamento do micro, em casa ou no escritório, muitas vezes há necessidade de que não haja acesso indevido às informações que estão contidas no disco. Desta forma, foi desenvolvido uma grande variedade de programas com essa finalidade, alguns distribuídos gratuitamente, tanto em plataforma Linux como Windows, cujo funcionamento é simples, permitindo ao usuário garantir confidencialidade de seus arquivos de forma rápida e eficiente. A maioria dessas ferramentas possui um modo de funcionamento similar, basicamente utilizando duas metodologias:

- Metodologia 1. É criado um arquivo no disco rígido, que será um container ou disco virtual. Este disco virtual só terá seu conteúdo visível através da utilização

- de uma senha. Assim sendo, o programa pega o arquivo que se deseja inibir o acesso, encripta e grava dentro deste disco virtual, por meio de um sistema de arquivo virtual. Mesmo que alguém copie um arquivo do disco-virtual, não conseguirá entender os dados que estão gravados nele.
- Metodologia 2. O arquivo é encriptado e sua versão original é apagada do sistema de arquivos. Para que o arquivo criptografado seja acessado, é realizada sua descriptação, de forma que o arquivo só possa ser utilizado, por algum programa, quando for descriptado.

O que muitas vezes diferencia um programa do outro é o algoritmo utilizado para encriptação dos dados, pois é ele que define a segurança da criptografia oferecida pela ferramenta.

5.4.2. Criptografia de arquivos em ambiente Windows

5.4.1. Criptografia de arquivos em ambiente Linux

No GNU/Linux existem várias implementações de criptografia em HD. Abaixo, são citadas algumas das implementações nesse ambiente, com uma breve observação, umas um pouco mais antigas, já em desuso, ou com o desenvolvimento interrompido:

- pam_mount: monta o sistema de arquivos criptografado automaticamente quando o usuário se loga e desmonta assim que ele sai.
- dm-crypt: tecnologia de criptografia em discos do linux.
- loop-aes: uma alternativa às implementações oficiais do linux.
- LUKS (Linux Unified Key Setup): um possível novo padrão para criptografia em disco no GNU/Linux; baseado na especificação TKS1 e possui suporte ao dm-crypt.
- eCryptfs: esquema bem prático de criptografia em disco, é o padrão mais recente desta lista.
- Phonebook: implementação da chamada *deniable encryption*, que é a possibilidade do usuário revelar apenas alguns pedaços da informação criptografada. Isso é feito através de um esquema de camadas, cada uma delas contendo seu próprio conteúdo criptografado.
- cryptoloop: software ainda em uso, mas já obsoleto.

- CryptoFS: utiliza o Linux Userland FileSystem para criptografia. Um diretório fica com os arquivos criptografados e o acesso aos dados é feito através do ponto de montagem.
- PPDD: cria um dispositivo que criptografa automaticamente os dados numa partição, conceito semelhante ao dm-crypt.
- CFS: sistema de arquivos criptografado que utiliza o NFS como interface.
- EncFS: sistema de arquivos criptografado em nível de usuário, utilizando o FUSE.
- TCFS: Transparent CFS (outra implementação do CFS).
- StegFS: um sistema de arquivos esteganográfico.

5.4.2. Criptografia de arquivos em ambiente Windows

A maioria dos aplicativos disponíveis para o Windows trabalha integrada ao Windows Explorer, de forma que o processo de encriptar/desenciptar se torna transparente para o usuário, pedindo apenas a senha para encriptar cada arquivo ou o disco virtual inteiro. Alguns programas ainda permitem que se envie arquivos encriptados via e-mail e, por meio de um programa somente de visualização, cujo acesso solicita senha, um outro usuário possa visualizar o arquivo. Abaixo, algumas ferramentas desenvolvidas para o ambiente Windows:

5.4.2.1. Encrypted Magic Folder

Permite a criação de pastas que ficam automaticamente codificadas e protegidas com senha, de forma transparente para o usuário. O software funciona de forma direta: quando se clica num arquivo, ele é decodificado e aberto. Quando é salvo, passa novamente pela criptografia. O programa pode ser usado por várias pessoas na mesma máquina. Cada uma tem seu conjunto de pastas, que podem ser invisíveis para os outros usuários, pois a ferramenta, além de criptografar, permite ocultar diretórios. Compatível com Windows , 95, 98, Me, 2000, XP e Vista, é disponibilizado na língua inglesa, como mostrado na figura 12.

Figura 12. Tela do software Best Crypt

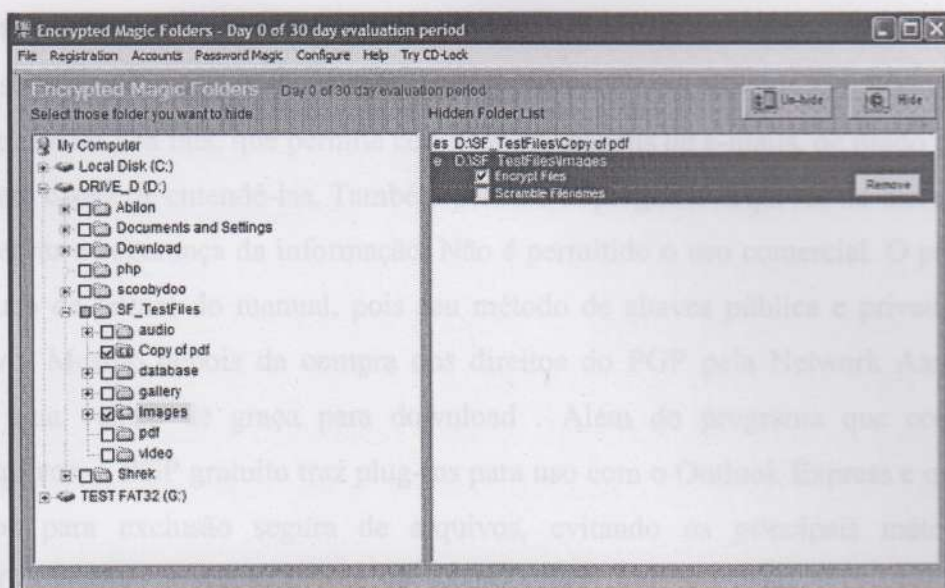


Figura 12. Tela do software Encrypted Magic Folder

5.4.2.2. Best Crypt

Permite criar um drive virtual onde os arquivos são encriptados automaticamente e com eficiência. Estes discos virtuais são, na verdade, arquivos container, como apresentado na figura 13, possibilitando facilidade de backup dos arquivos encriptados em outras mídias. O aplicativo utiliza algoritmos AES, Blowfish, Twofish, CAST e outros.. É compatível com o Windows 95, 98, NT, 2000, Millenium, XP, 2003 e Vista, mas possui também versões para Linux.

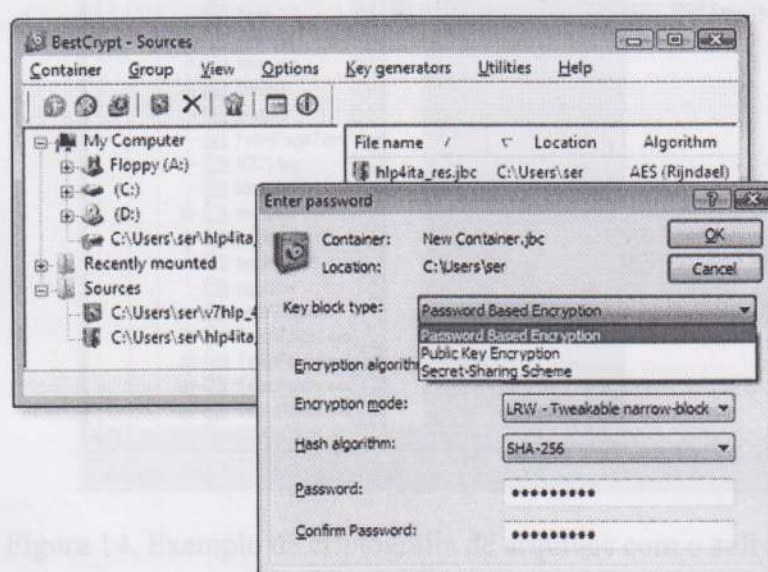


Figura 13. Tela do software Best Crypt

5.4.2.3.PGP

É um sistema robusto e praticamente imune a falhas. Fabricado por The PGPI Project, utiliza criptografia de 128 bits, que permite codificar mensagens de e-mails, de modo que só o destinatário será capaz de entendê-las. Também permite criptografar arquivos no disco rígido, a fim de preservar a segurança da informação. Não é permitido o uso comercial. O programa exige um pouco de leitura do manual, pois seu método de chaves pública e privada não é muito intuitivo. Mesmo depois da compra dos direitos do PGP pela Network Associates, ainda existe uma versão de graça para download . Além do programa que codifica e decodifica arquivos, o PGP gratuito traz plug-ins para uso com o Outlook Express e o Eudora e mecanismos para exclusão segura de arquivos, evitando os principais métodos de recuperação. Compatível com o Windows 95, 98, NT, 2000, Me, XP, 2003. É disponibilizado na língua inglesa. A figura 14 mostra como é realizada a criptografia e assinatura de arquivos com o PGP, diretamente no Windows Explorer.

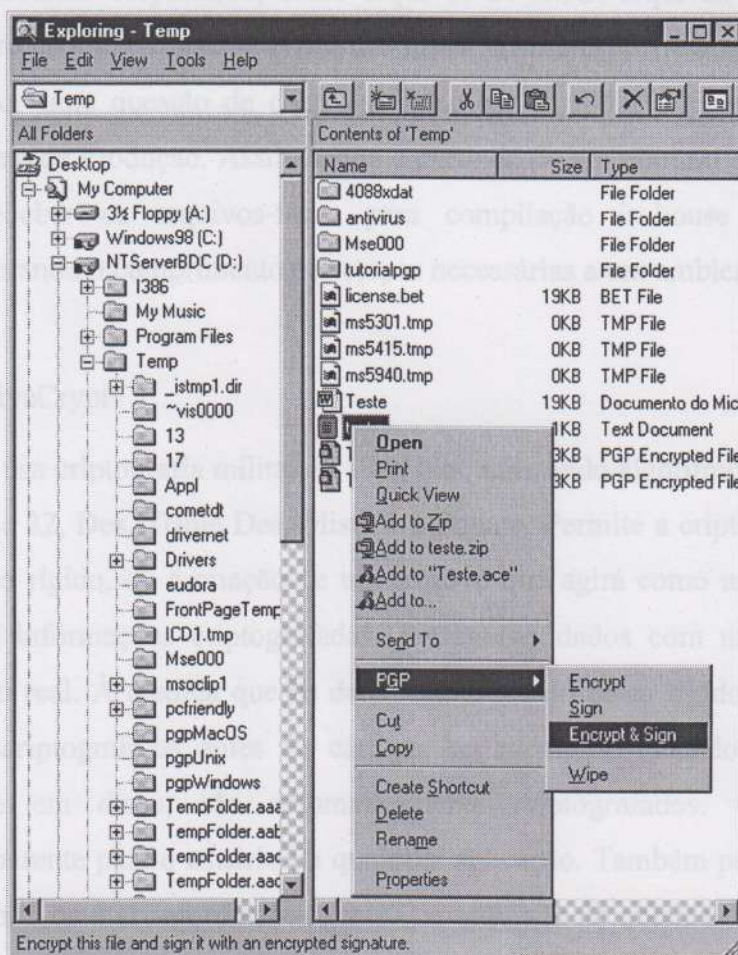


Figura 14. Exemplo de criptografia de arquivos com o software PGP

5.4.2.4.Cypher Millenium

Criptografador para arquivos e email em ambiente MS-Windows 2000, Millenium, XP e 2003. Possui mais de 60 prêmios internacionais. Chaves com até 8192 caracteres, utiliza sete algoritmos, incluindo o RIJNDAEL (AES), Twofish, Blowfish, Gost, DS2 e RC4. Dentre as diversas funcionalidades, sobrescreve o arquivo antes de deletá-lo (WIPE), possui assinatura digital, garante a entrada 100% segura de chaves secretas; permite que se criptografe emails usando apenas COPY-PASTE, possui alerta de invasão aos arquivos; modo de codificação com algoritmos randômicos, permite algoritmos diferenciados para email e arquivos e possui total integração com o Windows Explorer. Cypher Millenium é oferecido basicamente em três diferentes versões: PROFESSIONAL, CORPORATE e ENTERPRISE. A primeira versão é a mais adequada ao uso pessoal ou caseiro, embutindo todo o potencial do produto em uma versão simples de usar. A segunda, oferece além disso controles específicos para o ambiente corporativo, como arquivos de LOG, arquivos de controle de horário para uso, restrição à LAN, etc. A versão ENTERPRISE é específica nos casos onde a empresa necessita, por uma questão de controles internos, compilar o programa antes de submetê-lo ao ambiente de Produção. Assim sendo e partindo de um mínimo de 150 licenças, a empresa pode receber os arquivos-fonte para compilação in-house de CYPHER MILLENIUM, assegurando o cumprimento das etapas necessárias a um ambiente controlado.

5.4.2.5.DriveCrypt

O DriveCrypt usa criptografia militar de 1344 bits, utilizando algoritmos como o AES, Blowfish, Tea 16, Tea 32, Des, Triple Des, Misty 1 e Square. Permite a criptografia total de uma partição do disco rígido, ou a criação de um arquivo que agirá como um disco virtual para a gravação das informações criptografadas. Protege os dados com um processo de encriptação em tempo real. À medida que os dados são lidos do disco rígido, o DriveCrypt automaticamente descriptografa-os antes de carregar na memória. Quando os dados são gravados novamente em disco, são automaticamente criptografados. O processo é completamente transparente para o usuário ou qualquer aplicação. Também permite o uso de estenografia, permitindo ocultar informações dentro de arquivos de música. Esta ferramenta roda em Windows 95, 98, NT, 2000, Millenium, XP. Um exemplo do software é apresentado na figura 15, onde é mostrada a tela principal do programa.

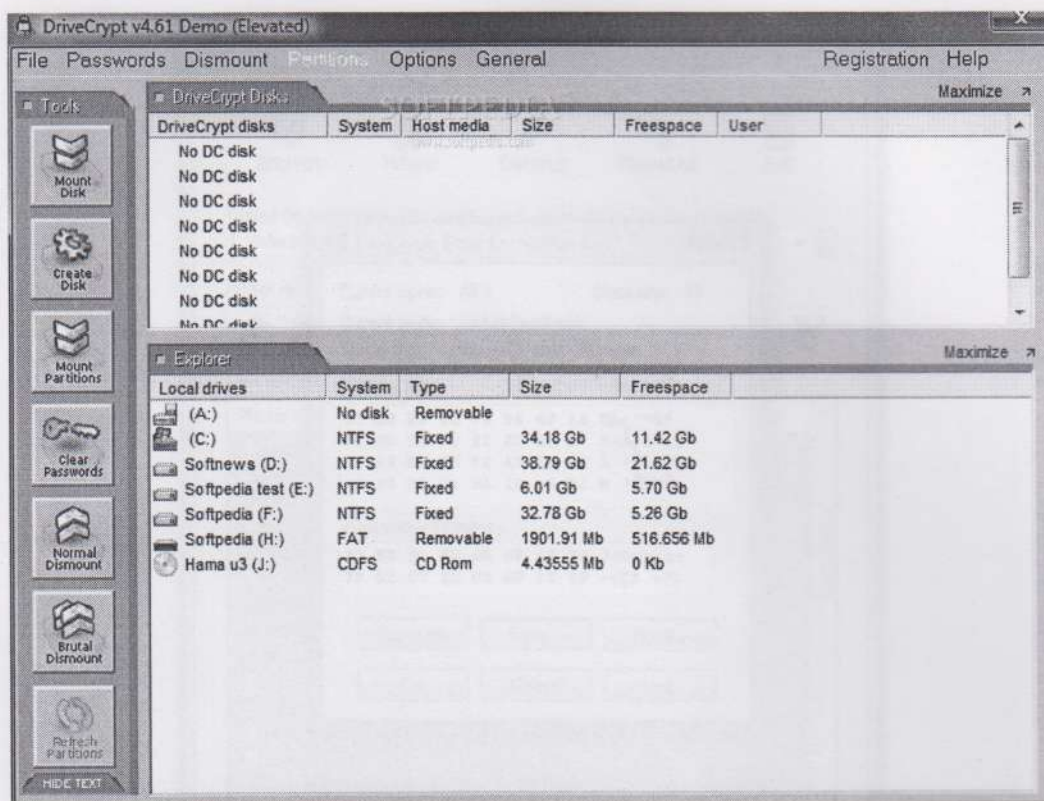


Figura 15. Tela do software DriveCrypt

5.4.2.6.FineCrypt

É uma ferramenta profissional de codificação, gratuita, de idioma inglês, desenvolvida pela Crypto Systems. Possui funcionalidades para codificar com apenas alguns cliques, realiza comunicação de e-mails seguramente, possui um gerente de tarefas, chaves e arquivos e permite codificar pastas ou arquivos inteiros. Disponível para o Windows 98, 2000 e XP, possuindo total integração com o shell do Windows. Esta ferramenta utiliza os quatro modos de funcionamento (ECB, CBC, CFB, OFB) e permite o uso de dez algoritmos de encriptação, incluindo o MARS, RC-6, Rijndael(AES), Serpent e Twofish. A figura 16 apresenta o programa, utilizando o algoritmo AES, na tela de configuração da chave e do vetor de inicialização.

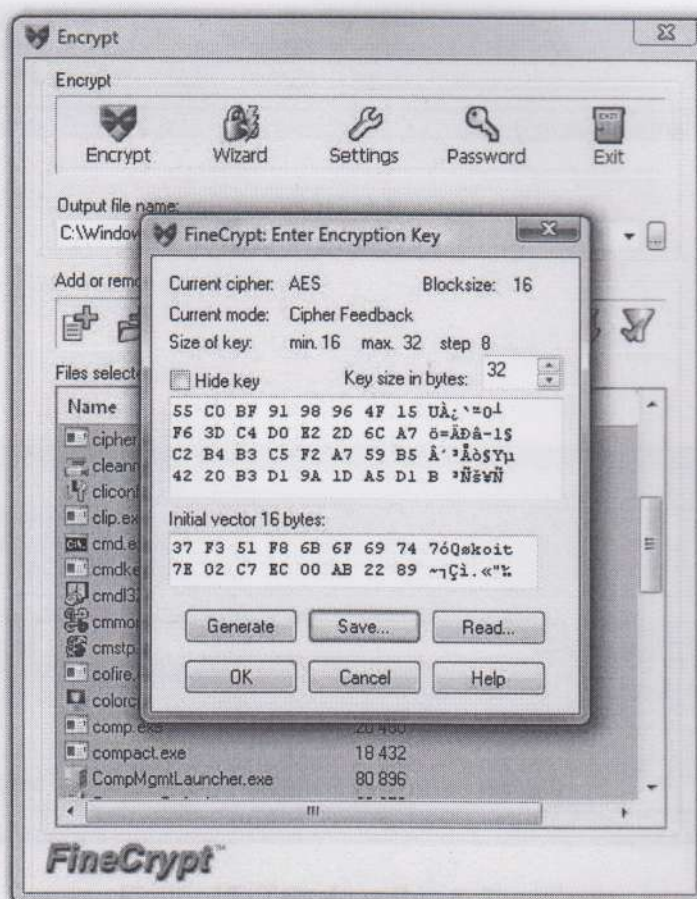


Figura 16. Tela do software FineCrypt

5.4.2.7. TrueCrypt

Trata-se de uma ferramenta de código aberto. Sua encriptação é automática, transparente e em tempo-real. É capaz de codificar arquivos em discos virtuais, criados para montá-los em um disco real. Neste disco, tudo fica protegido com criptografia de até 554 bits. Um recurso inovador é o de criar uma área separada dentro do disco virtual, com senha própria e que fica escondida, caso um invasor descubra a senha da área principal, ainda há proteção do conteúdo da área escondida. O aplicativo também permite codificar partições do disco rígido ou serviços como drives removíveis via USB, como mostra a figura 17. Os algoritmos utilizados na codificação são: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES, e Twofish. Seu modo de operação é LRW (com suporte a CBC). Compatível com Windows 2000/XP/2003. Também roda em Linha de comando do Linux, ambiente gráfico Gnome.

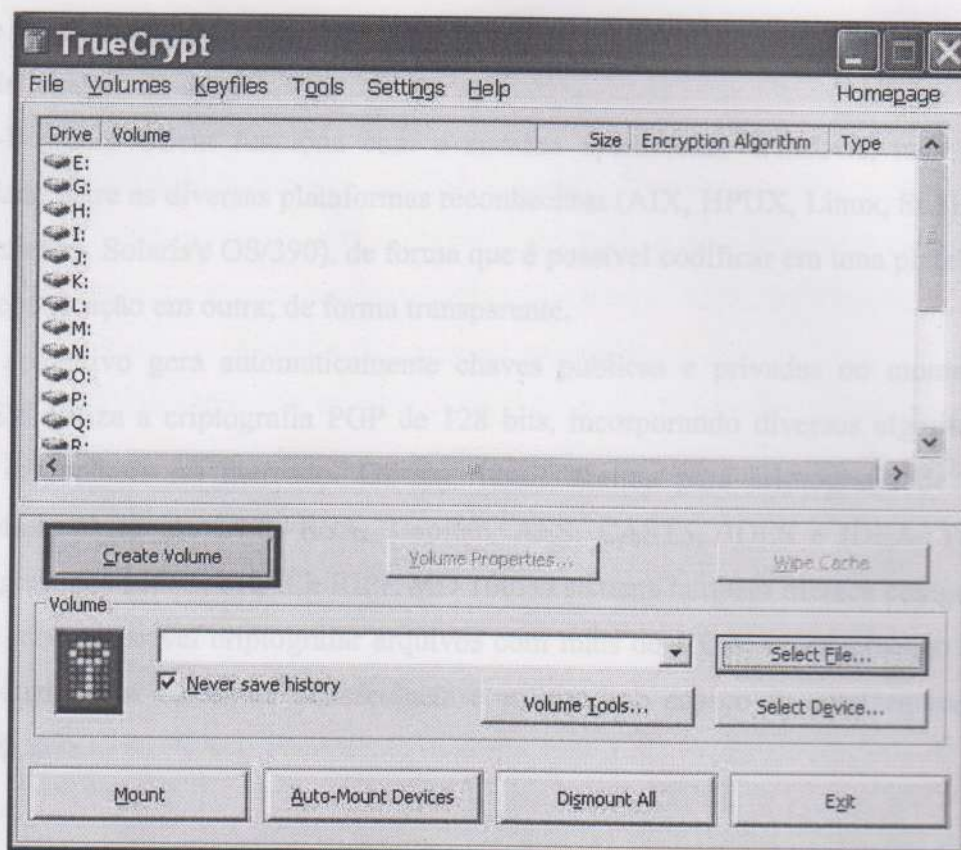


Figura 17. Tela do software TrueCrypt

5.5. Criptografia em ambientes corporativos

Normalmente, as empresas trocam informações confidenciais ou propriedade intelectual de clientes com filiais, fornecedores e parceiros de negócios. Todos os envolvidos nessa troca precisam manter protegidos e seguros os dados e aplicativos confidenciais. Há várias soluções dessa natureza, que colocam à disposição dos seus usuários ferramentas de criptografia e transmissão de dados, diretamente nos seus desktops, oferecendo facilidade e transparência aos serviços de criptografia.

Uma solução desenvolvida para o ambiente corporativo é o McAfee E-Business Client. Este software permite a proteção de dados críticos armazenados e/ou em trânsito. Como ele utiliza o FTP e SMTP, a transferência dos arquivos ocorre automaticamente, protegendo os dados corporativos nos aplicativos e nos emails, durante a transferência de arquivos e o processamento das transações. Ele possui uma ferramenta de arrastar e soltar para criptografar, decodificar e verificar os documentos, de forma que não há necessidade de treinamento para uso do sistema. Além disso, a empresa e os seus parceiros de negócios podem incluir logotipos em documentos, para fins de marcação e identificação. Todas as

transações e confirmações são registradas para ajudar a empresa a cumprir exigências de conformidade legal ou do setor.

O E-Business Client funciona com o sistema operacional Windows, mas oferece compatibilidade entre as diversas plataformas reconhecidas (AIX, HPUX, Linux, SuSE Linux em S/390 e zSeries, Solaris e OS/390), de forma que é possível codificar em uma plataforma e realizar a decodificação em outra; de forma transparente.

Este aplicativo gera automaticamente chaves públicas e privadas no momento da instalação. Ele utiliza a criptografia PGP de 128 bits, incorporando diversos algoritmos de criptografia disponíveis no mercado. Os algoritmos aceitos para criptografia de chaves simétrica e assimétrica são DSS, RSA, Twofish, AES, CAST5, 3DES e IDEA. Também suporta os algoritmos MD-5, SHA1 e RIPE MD 160. O sistema também oferece compactação incorporada, sendo possível criptografar arquivos com mais de 4 GB, economizando largura de banda, reduzindo os custos de transferência e utilizando o espaço de armazenamento de com maior eficácia.

Capítulo 6 – Conclusão

A segurança da informação é um dos objetivos básicos da criptografia. A informação tornou-se um elemento fundamental na vida das pessoas e das empresas. Hoje utiliza-se cada vez mais recursos computacionais para armazenar, produzir e distribuir informações. Com isso, aumenta-se também a preocupação com a segurança desta informação e com a vulnerabilidade dos sistemas computacionais que as gerenciam.

Podemos definir segurança em rede como o processo de prevenir e detectar qualquer uso não autorizado de uma rede de computadores. Mesmo sistemas que aparentam despertar pouco interesse aos hackers, como os de uma universidade ou de usuários domésticos ligados à Internet, são constantemente alvos de ataques. Isto por que, muitas vezes a intenção é usar os sistemas para lançar ataques em outros recursos computacionais. Desta forma, a segurança da informação é relevante para toda sociedade.

É importante que indivíduos e organizações se aprofundem nos conceitos relacionados à segurança de dados e adotem medidas que garantam níveis razoáveis de segurança em seus sistemas computacionais. Este trabalho se apresenta como um auxílio nesta busca, fornecendo um vasto conhecimento sobre o assunto, no que diz respeito ao uso da criptografia na garantia da segurança da informação.

Referências Bibliográficas

- COSTA, Celso José da; FIGUEIREDO, Luiz Manoel Silva de. **Introdução à Criptografia**. Rio de Janeiro: UFF/CEP - EB, 2006.
- COSTA, Celso José da; FIGUEIREDO, Luiz Manoel Silva de. **Criptografia Geral**. 2. ed. Rio de Janeiro: UFF/CEP - EB, 2006.
- PUTTINI, Ricardo Staciari; JÚNIOR, Rafael Timóteo de Sousa. **Criptografia, Autenticação e Assinatura Digital**. Brasília: [s.n.], 2000. Disponível em: <<http://www.redes.unb.br/security/cripto.pdf>>. Acesso em: 27 fev. 2007.
- BRAGA, Hugo Rodrigues. **História da Criptologia**. Brasília: [s.n.], [200-?]. Disponível em: <<http://www.contemporaneo.eti.br/CorpoCriptologia.htm>>. Acesso em: 18 dez. 2007.
- REZENDE, José F. de. **IPSec-Protocolo de Segurança IP**. Rio de Janeiro: [s.n.], [200-?]. Disponível em: <<http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/ipsec.html>>. Acesso em: 18 dez. 2007.
- RHATTO, Silvio. **Manual de Criptografia**. [s.l.]: [s.n.], 2006. Disponível em: <http://docs.indymedia.org/view/Sysadmin/GnuPGpt#4_Criptografia_e_internet> Acesso em: 18 dez. 2007.
- AZAMBUJA, Wagner. **Wi-Fi Protected Access WPA**. Ponta Grossa: [s.n.], 2007. Disponível em: <<http://www.vivasemfio.com/blog/wi-fi-protected-access-wpa/>>. Acesso em: 18 dez. 2007.
- LINHARES, André Guedes; GONÇALVES, Paulo André da S. **Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Recife: [s.n.], 2006. Disponível em: <<http://www.unibratrec.com.br/jornadacientifica/diretorio/UFPEAGL.pdf>>. Acesso em: 13 mar. 2008.
- PERES, André; WEBER, Raul Fernando. **Considerações sobre Segurança em Redes Sem Fio**. Rio Grande do Sul: [s.n.], [200-?]. Disponível em: <<http://www.ppgia.pucpr.br/~maziero/pesquisa/ceseg/wseg03/07.pdf>>. Acesso em: 18 dez. 2007.
- SERPREST, Isidro Vila Verde. **Segurança versus acessibilidade**. Porto: [s.n.], [200-?]. Disponível em: <<http://paginas.fe.up.pt/~jvv/Assuntos/Secur/full.html>>. Acesso em: 02 fev. 2008.
- The International Telegraph and Telephone Consultative Committee (CCITT). **Recommendation X.800: Data communication networks: Open systems interconnection, security, structure and applications**. Geneva, 1991. Disponível em: <<http://fag.grm.hia.no/IKT7000/litteratur/paper/x800.pdf>>. Acesso em: 02 fev. 2008.
- HINZ, Marco Antônio Mielke. **Um estudo descritivo de novos algoritmos de criptografia**. Pelotas: [s.n.], 2000. Disponível em: <www.ufpel.tche.br/prg/sisbi/bibct/acervo/info/2000/Mono-MarcoAntonio.pdf>. Acesso em: 02 fev. 2008.