Universidade Federal do Rio de Janeiro
Coordenação dos Programas de Pós Graduação em Engenharia

Programa de Engenharia e Sistemas
Área: Redes de Computadores

Sistemas de Certificação e Autenticação

(CPS 762 / COS 871)

Por Alessandro Martins - martins@ravel.ufrj.br
Orientador Prof. Luis Felipe Moraes - moraes@ravel.ufrj.br

Última atualização em 21/12/2000 - Versão: 0.6

Índice

1- Introdução

A rede de computadores que conhecemos hoje com Internet, desde a sua origem, não tinha como base a segurança na comunicação. Isso fica bem claro vendo a história da rede ao longo da sua existência e analisando a estrura dos protocolos, principalmente o mais usado, o TCP/IP. Diversos relatos de ataques foram registrados e apartir do momento que eles passaram a ser nocivos aos sistemas, começou a ser dada atenção ao fator segurança.

Atualmente com a grande expansão da internet, tornando possivel a sua chegada a qualquer pessoas que possua uma I-Box[1] com uma linha telefonica, é enorme a facilidade para a troca de informações, facilitando também a atuação de "hackers". Esses indivíduos podem agir desviando informações, assumindo a indentidade de outras pessoas ou bloqueando serviços, isso só para citar alguns problemas, gerando como consequência altos prejuizos financeiros além do descrédito da própria pessoa ou instituição afetada e inviabilizando a criação de novas formas de comércio utilizando a rede como base.

Muitos antes do surgimento da internet, uma ciência já era conhecida e muito utilizada por alguns grupos com propósitos bem específicos. Falo da criptografia, a arte de escrever de forma oculta. Podemos considerar os Egipcios os primeiros a fazer usso de tecnicas criptograficas, isso a mais de 4000 anos! Desde então, seu principal emprego era militar e/ou voltado para a segurança nacional. Sua base matemática já estava bem solida, quando Shannon deu o primeiro passo para que ela fosse usada na segurança da informação na internet. Apartir desse ponto, um novo enfoque para ela foi dado e novos empregos surgem a cada dia.

Este estudo tem por objetivo analisar os métodos criptográficos disponíveis atualmente para a segurança na internet e os sistema de certificação e autenticação (C/A) baseados em soluções de código aberto (e gratuito) existentes e desse modo buscar resolver o problema de segurança apresentado anteriormente.

1. Podemos considerar uma I-Box como qualquer dispositivo capaz de acessar a internt, não apenas PCs

1.1- Resultados e próximos passos

Após a conclusão desta pesquisa, uma boa base criptográfica terá sido obtida e um senso de qual direção tomar para as próximas ficará claro. Neste momento será possivel detectar alguns novos campos para a utilização dos métodos estudados e do mesmo modo, novos problemas a serem equacionados e resolvidos.

As implentações feitas durante o período de pesquisa poderão servir de base para a criação de softwares para análise de vunerabilidades em vários sistemas, como por exemplo o bancário, englobando tanto o utilizado via internet como o interno a própria instituição, evitando assim fraudes e roubos provenientes de ações internas (funcionários) ou externas (hackers).

A pesquisa pode também nos proporcionar a criação de cartórios digitais sobre a égede do governo, o que tornaria possível ter documentos assinados digitalmente sem a necessidade dos custos e problemas associados aos cartórios hoje existentes.

As leis sobre segurança da informação, violação dos direitos autorais e da privaciade- também pode ser beneficiadas com essa pesquisa. Em muitos campos hoje ainda nãao existem definições precisas sobre as infrações nesses campos.

1.2- Temas para futuras pesquisas

1. Métodos probabilísticos de criptografia
2. Assinaturas de imagens digitais
3. C/A em sistemas móveis como por exemplo celulares segundo o padräo WAP
4. Codificação para transmissão de áudio/vídeo em banda larga por assinatura
5. Sistema de C/A para componentes CORBA
6. Sistema de C/A baseado em CORBA com modulos ajustáveis as necessidades, por exemplo, uso de autenticação de voz para acesso a portas e senha para sistemas bancários ou ainda teste de retina para alteração de dados de alta segurança, tudo integrado em um único banco de “senhas” (seria mais correto chamar de banco de semelhanças)
7. Sistemas de C/A por hardware, usando por exemplo cartões inteligentes

8. Hardware dedicado (possivelmente uma placa para PC) para criptografia, com possibilidade de atualização do código do equipamento via conexão com um micro.

9. Performance de sistemas usando criptografia, por exemplo, comércio eletrônico basedo em HTTP

2- Segurança na Internet

Como superficialmente apresentado no capitulo anterior, existe uma grande necessidade de segurança na internet. A computação na internet tem duas características importantes: o processamento distribuido e a comunicação aberta. Um ambiente de processamento pode variar de um simples PC em uma casa, até uma grande rede em uma universidade, composta por diversas estações com software e hardware variados. A comunicação entre esses e outros ambientes esta sujeita a vários tipos de interferências intencionais (ou ataques).

Nesse capitulo, será apresentado com maiores detalhes a origem dos problemas de segurança e as formas possiveis de solução. O capitulo começa com uma descrição resumida da origem da internet, aborda os problemas decorrentes das escolhas feitas nas implementações, com enfoque nos pontos falhos e muito usados atualmente pelos atacantes. Seguindo o tema, serão apresentados algumas soluções criptográficas capazes de solucionar o problema. Mesmo essas soluções ainda possuem falhas que mais uma vez nos levam a apliacação de uma correcão, agora gerando uma solução completa para o problema, pelo menos, até agora !

2.1- Os Problemas de Segurança na Rede

Grande parte, senão a totalidade, dos problemas de segurança na internet são baseados nas falhas dos protocolos usados. Um parte também importante deve-se a má administração dos sistemas causada pela inexistência ou ineficiência de uma política de senhas adequada, um controle e monitoramento de acesso aos recursos, entre outros fatores. A caracterização dos tipos de atacantes e ataques mais simples segue no próximo tópico.

2.1.1- Atacantes e Ataques

Falando apenas de atacantes, podemos dividí-los em dois grupos: os internos e os externos a um sistema. Essa divisão é bem simples e bastante adotada na literatura. Os dois grupos podem ser sub-divididos em intencionais e acidentais. É claro que as divisões apresentadas são conceituais, o que considerar interno ou externo, ou ainda intencional ou acidental depende de diversos outros fatores. O atacante em si pode ser uma pessoa ou um programa de computador

ou qualquer outro tipo de agente capaz de lesar o sistema, num extremo podemos até considerar um desastre natural como um ataque!

Os tipos de ataque podem também ser divididos em dois grupos: passivos e ativos. Os ataques passivos são aqueles que em que o atacante apenas monitora as comunicações ameçando apenas a confidencialidade dos dados, por outro lado, os ataques ativos são aqueles onde o atacante adiciona, remove ou altera os dados. Esse atacante ameaça a confidencialidade, a autenticidade e a integidade das informações.

Os ataques ativos podem ser subdividos em outros tipos mais específicos de ataques, normalmente baseados no quanto de informação o atacante possui e/ou deseja obter. Alguns exemplos dessa sub-divisão são:

* os ataques de força bruta, onde o atacante possui pouca informação a para obter algum resultado, tenta todas as combinações possíveis

* as ataques de texto fonte conhecido (know plaintext) onde o atacante sabe o que foi codificado e tenta obter outras informações, como uma senha de codificação com base nisso.

Além desses, temos: Denial of Service, Main-in-the-middle, Masquerade, Replay, Spoofing, Trojan Horse, entre diversos outros.

2.2- Segurança da Informação

Para começar o processo de estudo de criptografia, uma base de conhecimentos relacionados com a segurança da informação torna-se também necessária. A segurança da informação manifesta-se de várias formas de acordo com as situações e necessidades. Independente de quem é envolvido, e em que nível, todas as partes em uma transação devem ter certeza que certos objetivos relacionados com a segurança da informação devem ser atendidos. A tabela abaixo apresenta uma lista com alguns deles.

Privacidade e confidencialidade	Mantém a informação secreta para todos, menos para aqueles com autorização para lê-la
Integridade dos dados	Garante que a informação não foi alterada por alguma pessoa ou processo não autorizados
Autenticação das entidades ou identificação	confirmação da identidade uma entidade
Autenticação da mensagem	Confirmação da fonte da informação, também conhecido como autenticação da origem dos dados
Assinatura	uma forma de associar informação a uma entidade
Autorização	veículo, para outra entidade, de permições oficiail para ser ou fazer alguma coisa
Controle de Acesso	restringir acesso aos recusos para entidades privilegiadas
Certificação	confirmação da informação por uma entidade fidedigna
Timestamping	armazena o tempo ou a data da criação da informação
Testemunho	verifica a criação ou existência da informação por uma entidade que não seja a criadora do dado
Recebimento	certeza de que a informação foi recebida
Confirmação	certeza de que o serviço foi feito
Propriedade	uma forma de prover para uma entidade com direitos legais o direirto de usar ou tranferir recursos para outros
Anonimidade	encobrimento das identidades dos envolvidos em um processo
não-repúdio	prevenção da negação de um acordo ou ação já acertada
Revogação	retirada da certificação ou da autorização de um entidade

Tabela 1: Alguns objetivos da Segurança da Informação

Pelos séculos, um grupo elaborado de protocolos e mecanismos foram sendo desenvoldidos para fornecer segurança para as informações que durante todo esse tempo habitavam em documentos (no formato físico). A segurança dessas informações era sempre baseada em alguma entidade resposável por garantir os requisitos de segurança, como o governo.

3- Criptografia

3.1- Um pouco de História

A criptografia tem uma longa e fascinante história. O livro *The Codebreakers* [1] fornece um excelente (senão o mais completo) relato histórico do assunto, iniciando com os Egipcios a 4000 anos, passando por várias épocas da historia mundial e por diversos fatos marcantes relacionado com o emprego da criptografia até a época das grandes guerras mundiais. Kann não deixa de citar os fatos científicos marcantes para a evolução desta ciência.

O primeiro artigo que aborda teoricamente a criptografia foi *Communication theory of secrecy systems* [2] publicado por Shannon em 1949 onde foram dados os primeiros passos na teoria. A proliferação dos computadores e dos sistemas de comunicação na década de 60 cuminou com a demanda de privacidade para o setor, na intenção de proteger a informação no formato digital, e consequentemente, com a necessidade dos serviços de segurança.

O maior impacto no desenvolvimento da criptografia em toda a sua história foi em 1976 quando Diffie e Hellman publicaram o artigo *New Directions in Cryptography* [3]. Este artigo introduz um revolucionário conceito de criptografia de chave pública e também apresenta um novo e ingênuo método para troca de chaves. A segurança desse novo método se baseia na intratabilidade do problema do logarítmo discreto.

A criptografia de chave pública deu uma importante contribuições para a assinatura digital. Em 1991 foi adotado o primeiro padrão internacional para assinaturas digitais (ISO/IEC 9796), este esquema se baseia no padrão de chaves públicas segundo o modelo RSA [4].

3.2- Definições preliminares

Os métodos criptográficos e de C/A possuem um leque muito grande de termos e definições, que nos dão um sinal bem claro da complexidade dos problemas e/ou das soluções. Para iniciar esse processo de estudo, precisamos primeiramente compreender exatamente o foco do

estudo. As definições dos termos fornecem um primeiro passo nesse sentido. Segundo o dicionário Aurélio, temos o seguinte:

Autenticação, s.f. Ação ou efeito de autenticar;

Autenticar, v. tr. dir. Declarar autentico, reconhecer como verdadeiro, legalizar, autorizar;

Autêntico, adj. Verdadeiro, legítimo; que faz fé que é o autor a quem se atribui; que não deixa dúvidas, certo, positivo, fato autentico, legalizado, genuíno, que é do próprio punho da pessoa: assinatura autentica (do latim *authenticu*)

Certificação, s. f. Ato de certificar, reconhecimento. (De certificar.)

Certificar, v. tr. dir. Dar por certo; afirmar a certeza de passar certidão; tr. dir e ind. cientificar; convercer da certeza ou verdade (de alguma coisa); asseverar; pr. convenser-se; ter a certeza. (Do latim *certificare*.)

As definições do Aurélio apresentam os termos num sentido anterior a Era da Informação que hoje vivemos. Porém, a idéia básica fornecida por ele ainda continua valendo. Os dois verbos (autenticar e certificar) deixam clara a necessidade de mais de um personagem, de alguns objetos e algumas regras. A relação entre estes componentes ficará clara na sequência do texto.

Nos tópicos que se seguem, serão apresentados alguns conceitos básicos sobre os métodos de criptografia, alguns exemplos importantes e a sua utilização no comércio via internet.

Três importantes referências sobre esse assunto, a primeira com um enfoque mais matemático, a segunda focada nos algorítmos e a terceira já com enfoque no seu uso em comércio eletrônico são:

* *Handbook of Applied Cryptography* [5]
* *Applied Criptography* [7]
* *Digital Certificates: Applyed do Internet Security* [6], caps 1, 2 e 3

3.3- Taxonomia

A figura abaixo apresenta de uma forma estruturada o que podemos considerar como as primitivas criptograficas básica. A combinação dessas com elas mesmas ou com outras pode gerar novos método de criptografia. O curso desse texto irá deixar claro a razão do nome primitivas criptograficas, por hora, é suficiente saber que a escolha de um ou outro método criptográfico depende de alguns fatores como: facilidade de implementação, nível de segurança, funcionalidade, método de operação e desemplenho.

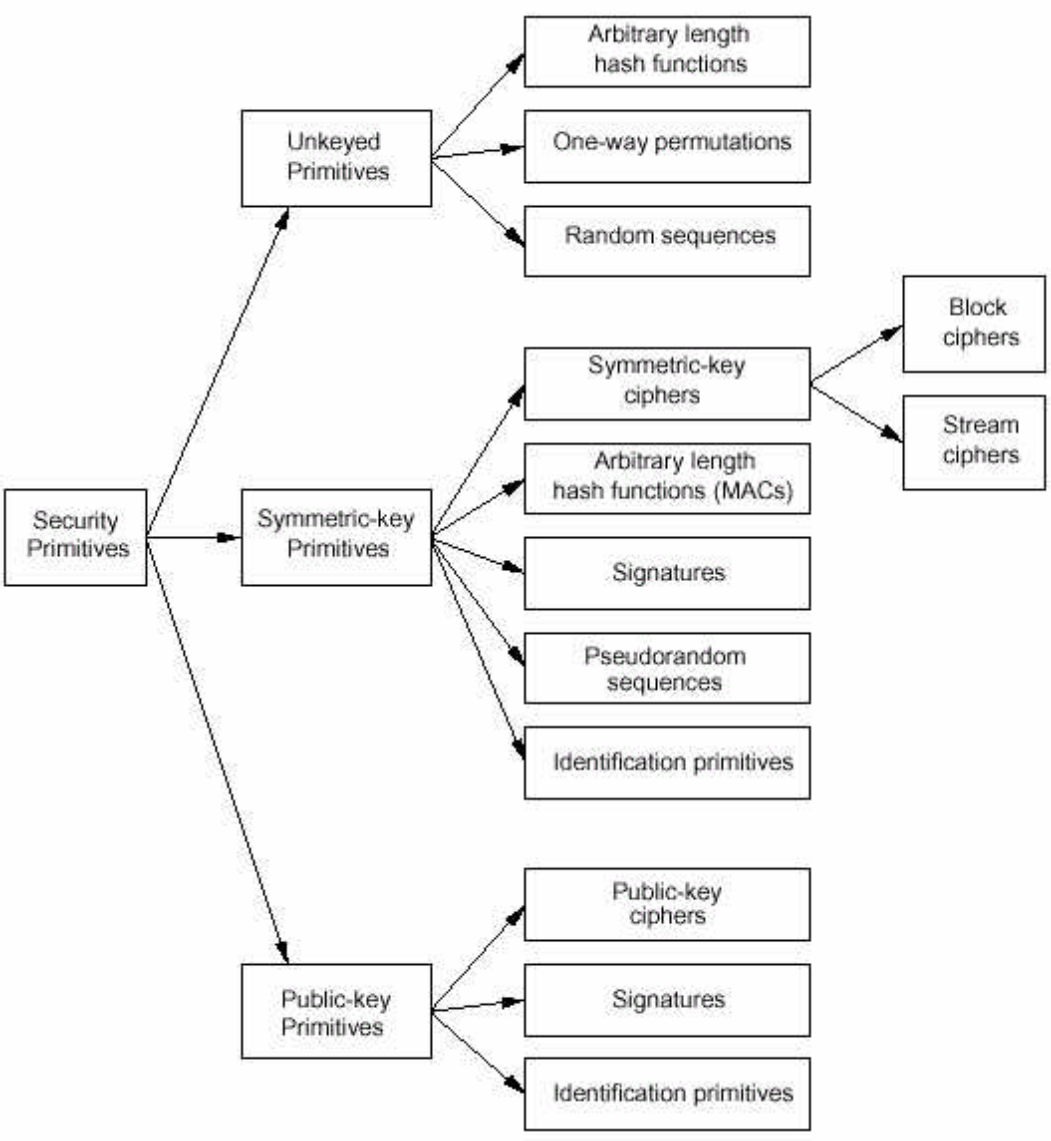

Figura 2.1 - Taxonomia da das primitivas criptográficas, fonte [5], pag. 5

3.4- Funções Básicas

Um pequeno grupo de funções matemáticas são sempre utilizadas nos algoritmos criptográficos. Essas funções se usadas isoladamente, fornecem pouca (ou nenhuma) segurança no sentido criptográfico, porém quando usadas em conjunto, e/ou repetidas vezes podem criar uma forte criptografia. O grupo de funções abaixo constitui uma seleção e as definições partem do pré-suposto que o leitor esteja familiarizado com as definições de domínio, contra-domínio, imagem e função matemática.

3.4.1- Funções 1-1

Uma fumção 1-1 (one-to-one) é aquela onde cada elemento do contra-dominio possui no máximo um elemento associado no dominio.

3.4.2- Funções One-Way

Um função F que mapeia elementos de um conjunto X para um outro Y é chamada One-Way se F(x) é simples de ser calculada para todo x pertencente a X porem, para essencialmente todos os elementos y pertences a Y é computacionalmente irrealizável encontrar um x pertencente a X tal que F(x)=y.

3.4.3- Funções One-Way Trapdoor

Uma função One-Way Trapdoor é uma função One-Way onde uma informação extra torna a função de retorno simple. Ou seja, o mapeamento X -> Y é sempre simples de ser feito, porem, sem o auxilio de uma informação extra, chamado valor *trapdoor*, o mapeamento de Y-> X é computacionalmente irrealizavel, já com o conhecimento do valor, o mapeamento Y-> X assume a mesma complexidade do X->Y.

3.4.4- Involução

De uma forma simples, uma função de involução é uma função 1-1 onde o mapeamento X -> Y é igual ao Y-> X.

3.5- Tipos de Criptografia

Basicamente, existem hoje duas formas bem caracterizadas de criptografia. A que usa apenas uma chave para os dois processos, e a que usa duas chaves, respectivamente criptografia simétrica e assimétrica. Algum métodos fazem uso da combinação da duas e são chamado híbridos, esses métodos não serão abordados aqui. Com base nas funções apresentadas anteriormente, podemos agora ver cada um desses métodos, como segue.

3.5.1- Criptografia Simétrica

Esse método de criptografia, também conhecido como criptografia de chave única ou criptografia de chave secreta, foi o primeiro a ser desenvolvido e por isso, o tempo de estudo sobre ele tornou as suas bases matemáticas muito sólidas. Neste ítem, veremos a estrututra básica dos algoritmos desse metodo além do embasamento matemático e de um exemplo de uso com uma das cifras mais conhecidas.

Uma visão ampla da comunicação entre duas entidades usando esse método de criptografia pode ser visto na figura abaixo:

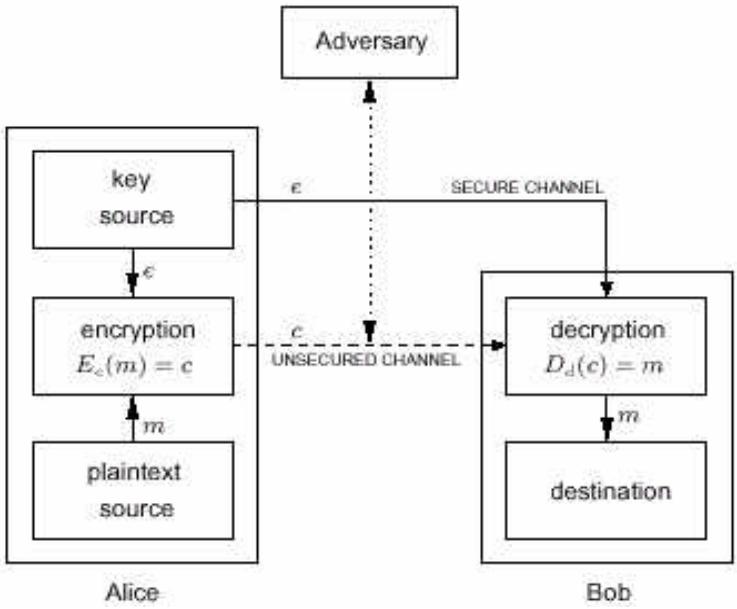

Figura 2.2 - Cenário de atuação dos algorítmos simétricos

Desmembrado um pouco a figura temos:

a) os algorítmos de encriptação (E) e de decriptação (D)
b) a chave de encriptação (e) e de decriptação (d)
c) o texto na forma original a ser transferido em oculto (m)
d) o texto na forma cifrada (c)

De uma forma simples, o processo é o seguinte: os dois participantes, aqui representados por Alice e Bob, querem se comunicar em secreto. Alice de uma forma segura enviar para Bob a chave necessária para obter o texto original (veremos mais adiante que é aqui que reside o problema desse método). Enquanto esse chave é levada a ate Bob, Alice usando um algoritmo criptográfico simétrico como DES[12] cifra o texto e envia para Bob por email. Bob ao ler o seu email vê um texto crifado por Alice e ao receber a chave, usa o mesmo algoritmo DES para obter o original.

Nesse caso, por ser simétrico o algorítmo, a chave (e) e a (d) são identicas. O método criptografico usado (DES) gera uma forte criptografia (i.e bem resistente a ataques de análise) e se baseia na confusão e difusão da informação no texto originial através de permutações e substituições (através de tabelas chamas S-Box). DES é a cifra de blocos de 64 bits com chave

de 56 bits (mais 8 bits de paridade, 1 para cada bloco de 7 da chave) com altíssima performance, sendo possivel a codificação a uma taxa de 40 Mbit/s [11].

De uma forma simplificada, podemos descrever o funcionamento do DES com a ajuda da figura abaixo.

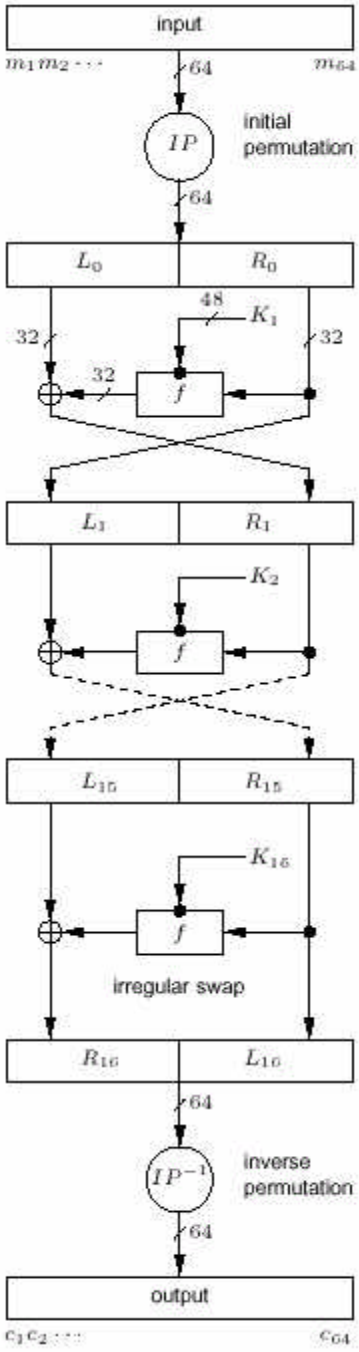

Figura 2.3 - DES em Blocos

Como já foi mencionado, a segurança do algoritmo esta na sequencia de substituições e permutações executadas. O que o torna particularmente bom para ser implementado em hardware. Seguindo a figura temos:

1- Uma permutação inicial de 64 bits, feita com o auxilio de uma tabela que possui uma inversa (uma S-Box), após isso o bloco de 64 bits é dividido em duas partes iguais de 32 bits, chamada de L e R.

2- Definindo Mi como a saida do estágio i, temos:

$$L(Mi) = R(Mi-1) \text{ e}$$
$$R(Mi-1) = L(Mi-1) \text{ XOR } f(L(Mi),Ki)$$

A função f recebe 32 bits de dados, e 48 bits derivados da chave de 56. As próximas figuras tornam mais simples a compreenção da operaçao da função f em questão.

Esse ítem 2 ocorre 16 vezes (chamados rounds). Note que ao final dele um permutação de 64 bits ocorre novamente sem que haja a inversão dos blocos, isso é necessário para que o algoritmo seja usado tanta para a cifragem com para a decifragem

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

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

Tabela 2.1 - Exemplo de tabela de transposição IP e IP^{-1} usada no ítem 1 descrito acima

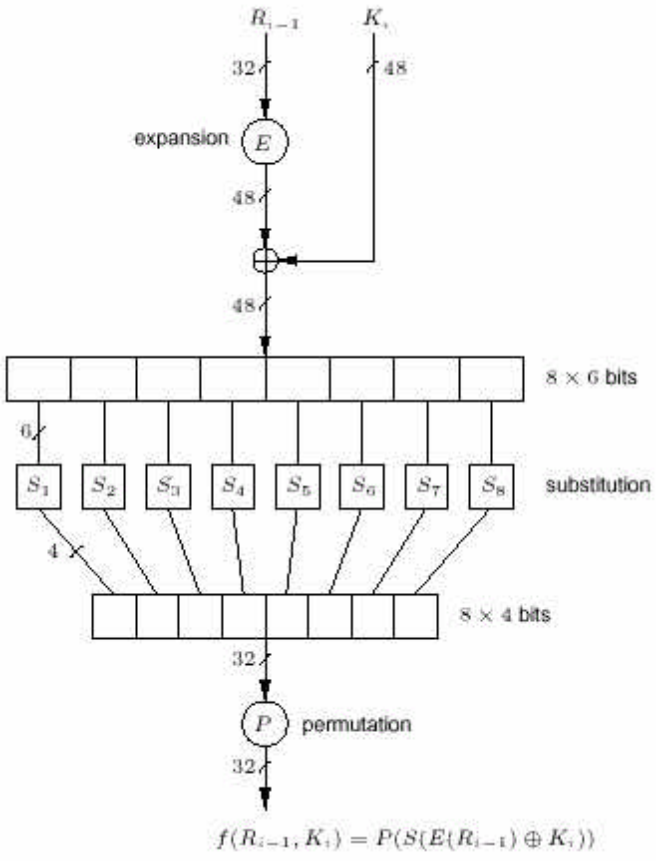

Figura 2.4 - Esquema de operação da função f

A expansão E mapeia 32 em 48 bits por reutilização dos bits de origem. O mapeamento P faz apenas uma permutação segundo uma tabela dada. As S-Box que mapeiam blocos de 6 em blocos de 4 também operam sobre tabelas, não apresentadas aqui por simplicidade.

Uma excelente e completa explicação de como esse algoritmo funciona pode ser obtida no livro *Handbook of Applied Criptography* [5], página 250 ou em *Cryptography and Data Security* [10], página 93. Outros exemplos de algoritmos simétricos são: Blowfish, IDEA, RC2, RC4, RC5, e 3DES.

As vantagens desse método podem ser vistas com base na figura anterior. Como mostra o esquema, a mesma chave é usada para cifrar e decifrar. Isso torna a execução do algoritmo bem rápida, e sua implementação mais simples. Além disso, o tamanho da chave necessária para um bom nível de segurança gira na ordem de meia centenas de bits.

Curiosiamente, a maior desvantagem desse metodo esta no fato da chave ser única. A unicidade da chave faz com que a sua distribuição por canais inseguros seja um grande problema. Na tentativa de resolver essa questão, Diifie e Hellman [3] em 1976 criaram um novo paradigma criptográfico, a criptografia assimétrica, junto com um método simples de se distribuir as chaves [8]. Em 1978 R.L. Rivest, A. Shamir, and L.M. Adleman criaram um dos mais conhecidos algoritmos criptográficos de chave pública, o RSA.

3.5.2- Criptografia Assimétrica

Ao contrário da sua irmã mais velha, a criptografia simétrica, a assimétrica é bem recente, e ainda existem muitos estudos sobre os seus métodos, os problemas matemáticos e as formas de gerenciar e trocas as chaves. Ela recebe esse nome pois sua principal característica está no fato de serem usadas duas chaves diferentes no processo. Uma é usada para a cifragem e outra para a decifragem. A chave de decifragem é derivada da chave de cifragen, porém o inverso não é possivel, ou seja, dada uma chave de decifragem, não é possivel obter a chave de cifragem. Para uniformizar a nomeclatura usada, desse ponto em diante a chave de cifragem será chamada de chave privada e a de decifragem, chave pública. Os termos ficaram claros no decorrer do texto.

A criptografia assimétrica fica mais bem mais simples de ser compreendida com a figura abaixo:

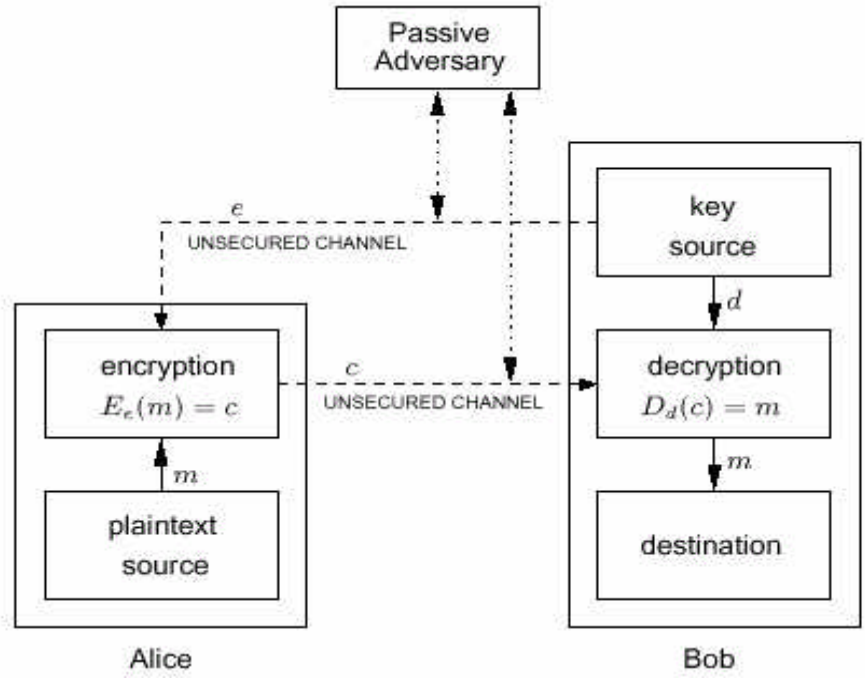

Figura 2.5 - Cenário de atuação dos algorítmos assimétricos

Da figura podemos obter:

a) os algoritmos de encriptação (E) e de decriptação (D)

b) a chave de encriptação (e) e de decriptação (d)

c) o texto na forma original a ser transferido em oculto (m)

d) o texto na forma cifrada (c)

Comparando com o caso simétrico podemos detectar as seguintes diferenças:

a) no caso simétrico a chave de decriptação tem que ser enviada por um canal seguro, o que nesse método não é mais necessário.

b) no caso simetrico as chaves eram iguais, já no assimetrico elas sao obrigatoriamente diferentes.

c) a mudança do bloco *Key Source*, que ficará clara na explicação do funcionamento.

O processo de comunicação é o seguinte:

a) tanto Alice quanto Bob usando algum método assimétrico para gerar suas chaves públicas e privadas (note que o metodo usado TEM que ser o mesmo para os dois e partimos do pré suposto que isso ocorre com eles)

b) Alice deseja obter a chave de Bob e par tal a solicita por email.

c) Após Bob enviar a sua chave pública para Alice, ela usa o algoritmo assimétrico para criptografar o seu texto para Bob e envia esse texto para ele.

d) Bob ao receber esse texto cifrado, usa a sua chave privada para obter o texto original.

As diferenças entre os métodos podem ser sutis, mas são muito importantes. Note que:

a) Alice não possuia a chave de Bob antes da comunicação

b) A chave publica de Bob foi enviada por um canal inseguro (e-mail)

c) As chaves de Alice não aparecem para Bob, ou seja, Alice poderia até não ter chaves!

Esse método resolve o problema da troca de chaves por canais inseguros, mas não resolve o problema de gerenciamento delas! Isso será visto mais tarde.

Os problemas matemáticos nos quais os métodos mais comuns de criptografia assimétrica se baseiam são os seguintes:

a) logaritmo discreto:

Na aritmética de modulo n (n >0), dois inteiros são equivalentes se eles geram o mesmo resíduo quando divididos pelo fator n. Por exemplo, 6 e 16 possuem o mesmo resto quando divididos por 10. Com essa base, podemos criar um exponenciação modular (a^x mod n). A volta dessa função, o logaritmo discreto, é um problema de dificil solução. Ou seja, encontrar x tal que $a^x = b$ mod n é computacionalmente dificil, ainda que gerar $b=a^x$ mod n seja bem simples. Um exemplo de uso desse problema é o sistema de troca de chaves criado por Diffie e Hellman [8].

b) a fatoração de números primos:

Esse é um problema bem antigo e ainda não existe soluções analiticas para ele. A dificuldade reside na determinação de um entre dois número primo muito grande (vamos chamá-lo de p e q) dado apenas o produto deles n. Matematicamente, n=p.q . Só podemos determinar p

ou q dado n e o outro primo em questão. Por bem grande entende-se que o número possua muitos digitos, na prática, mais de 100.

Existe uma fórmula, que torna possível calcular a quantidade de números primos que existem entre dois numeros quaisquer: O (n) = (p-1)*(q-1)

Por esta fórmula podemos ver que dados p e q com muitos dígitos, a quantidade de inteiros primos cresce quase com o quadrado dos valor de p ou q. Exemplo, para p=327 e q=413 obtemos O(n) = 134.312 (p^2 = 106.929 e q^2= 170.569)

Um exemplo do emprego desse problema é o algoritmos RSA.

A vantagems básica método é a disvantagem do anterior, a facildade na troca de chaves. Porem tudo tem o seu preço. Esse metodo necessita de chaves mais longas, de 10 a 100 vezes mais, e é computacionalmente mais lento.

Com a criptografia assimétrica, o problema da troca de chave em canal inseguro fica parcialmente resolvido. Parcialmente, pois como mostrado no exemplo anterior, Alice não precisa nem ter um par de chaves, por isso como Bob vai saber que foi Alice que realmente enviou a mensagem? E como Alice vai saber se a chave que ela recebeu por email é realmente de Bob? Esse sistema garante a confidencialidade da mensagem, mas ainda não garante a autenticidade da chave de Bob e nem da pessoa da Alice. O problema da autenticidade da chave de Bob pode ser resolvido usando certificados digitais, que serão apresentados mais adiante, bem como a assinatura digital, que resolve o problema da confirmação de envio feito pela Alice (nota: ela tb precisará de um certificado)

Tendo em vista as novas necessidade, sistemas para troca de chaves (IKE) e certificação digital (CA) estão sendo desenvolvidos. No proximo capítulo, esses sistemas serão apresentados com mais detalhes.

3.6- Assinatura Digital e Funções hash

Um dos problemas apresentados anteriormente era o de Bob não ter a certeza de que foi Alice quem realmente enviou a mensagem. Esse problema pode ser resolvido de forma simples com o uso da assinatura digital. A assinatura Digital é um processo onde é associada a identidade de um individuo a uma mensagem, por exemplo. Se aceitarmos o par de chaves (a pública e a privada) como sendo uma identidade, pode-se criar esse tipo de assinatura. O processo seria o seguinte:

a) Alice e Bob possuem pares de chaves, as públicas estao disponiveis em um local central, acessível a qualquer pessoa que as deseje. Porém a s privadas estão ocultas apenas com os seus respectivos donos.

b) Alice ao enviar uma mensagem para Bob, primeiramente obtem a chave pública de Bob, e em seguida encripta a mensagem com esse chave (novamente o algoritmo é o mesmo para Alice e Bob). Até aqui tudo como antes.

c) Alice então encripta a mensagem usando a sua chave privada e então, anexa a sua assinatura do documento e envia os dois criptogramas para Bob.

d) Bob por sua vez, usando a sua chave privada decripta a mensagem e para conferir se ela realmente pertence a Alice, ele obtem a chave publica de Alice, e usando um algoritmos de checagem, confere se foi a chave privada de Alice que criou a assinatura da mesnsagem.

O processo descrito acima pode ser revisto, de forma ilustrada e mais explicada no texto da NAI, denominado *An Introduction to Cryptography* [9], as figuras 2.6 e 2.7 foram obtidas deste artigo.

Apenas um pequeno problema existe neste processo. Se a mensagem tiver, digamos 10k, termos mais 10k de assinatura ! Isso não é prático e por algums razões, até indesejável. Para resolver isso, foram criadas funções especiais chamadas Funções Hash que mapeiam quantidades variáveis de caracteres em outras quantidades fixas. Com esses funções, antes de assinar o documento, o programa de Alice cria um *hash value* da sua mensagem, e após isso assina esse *hash value*. Quando Bob obtem a mensagem cifrada, ele a deficra como antes, computa o hash value dela com o mesmo algoritmo de Alice e com a chave pública de Alice verifica se esse hash foi codificado com a chave privada dela. Como apenas Alice possui a sua chave privada, esse

processo garante que só ela poderia ter assinado a mensagem e consequentemente, enviado a mesma.

Essas funções de hash tambem podem ser usadas para se criar *hash values* de um arquivo, funcionando apenas com uma forma de checar alterações de integridade, como por exemplo, quando infectado por um virus. O tamanho do *hash value* depende do algoritmo. Exemplos de funções de hash são : MD4, MD5 e SHA e SHA-1

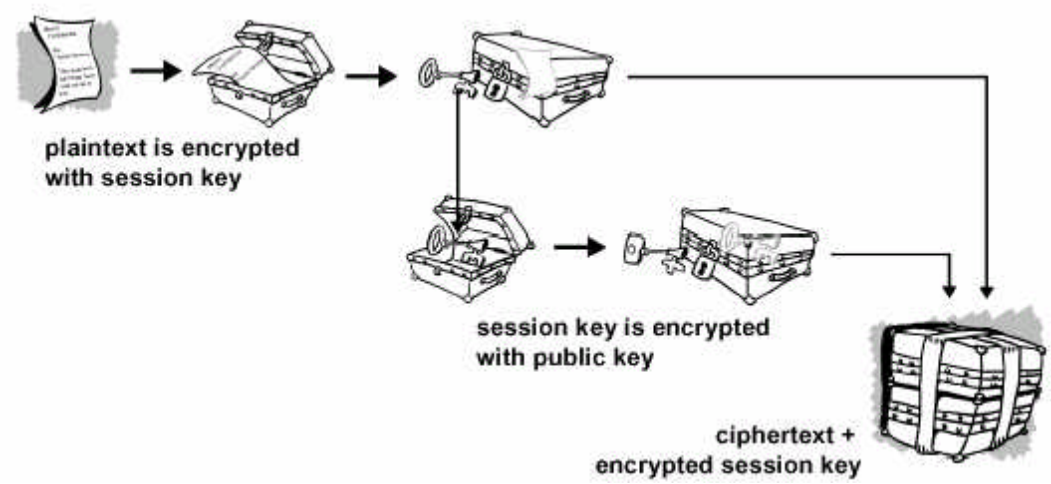

Figura 2.6 - Processo de criptografia com assinatura

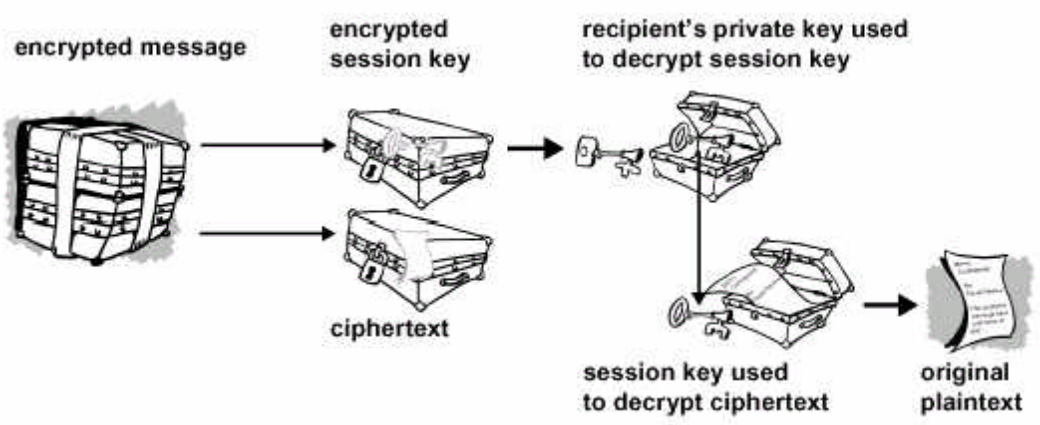

Figura 2.7 - Processo de decriptografia com assinatura

3.7- Áreas de emprego: comércio eletrônico e email

Todas as áreas que relacionem duas ou mais entidades que desejam trocar informações com alugum nível de seguranca são candidatas em potencial para o uso do metodo assimétrico com apoio de uma entidade certificadora (CA). Nosso enfoque nesse trabalho é o seu emprego no suporte ao comércio eletrônico e a troca de informações por email. Outros usos como assinatura de imagens, certificação de componentes de software tambem podem

Referências

[1] D. Kahn, *The CodeBreakers*
Macmilan Publishing Company, New York, 1967

[2] C. E. Shannon, "*Communication theory of secrecy systems*",
Bell System Technical Journal, 28 (1949), 656-715

[3] W. Diffie and M.E. Hellman, "*New Directions in Cryptography*",
IEEE Trasactions on Information Theory, 22 (1976). 644-654)

[4] R.L. Rivest, A. Shamir, and L.M. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems*", Communications of ACM, 21 (1978), 120-126

[5] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applyed Cryptography*, CRC Press, October 1996, http://www.cacr.math.uwaterloo.ca/hac/

[6] Feghhi, Jalal and Jalil and Williams, Peter, *Digital Certificates: Applied Internet Security*,Addison-Wesley Publishing, 2000

[7] Schneier, Bruce, *Applied Cryptography: Protocol, Algorithms and Source Code in C*
Addison-Wesley Publishing, 1996

[8] Diffie Hellman key exchange

[9] NAI, An Introduction to Cryptography, http://www.nai.com/???

[10] D.E. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing, 1983

[11] National Institute of Standards and Technology (NIST), PUBLIC-KEY CRYPTOGRAPHY - NIST Special Publication 800-2, April 1991

[12] DATA ENCRYPTION STANDARD (DES), FIPS 46-3, Outubro de 1999 (em substituição da FIPS 46-2)

3- Certificação Digital

O problema principal do uso da criptografia de chave pública, é a necessidade constante de se garantir que a chave pública realmente pertence a quem de direito. O tráfego desse chave por canais inseguros pode sofrer diversos tipos de ataques, um dos mais comuns e o chamado *men-in-the-middle*. Esse ataque pode ser melhor descrito com o auxilio da figura abaixo:

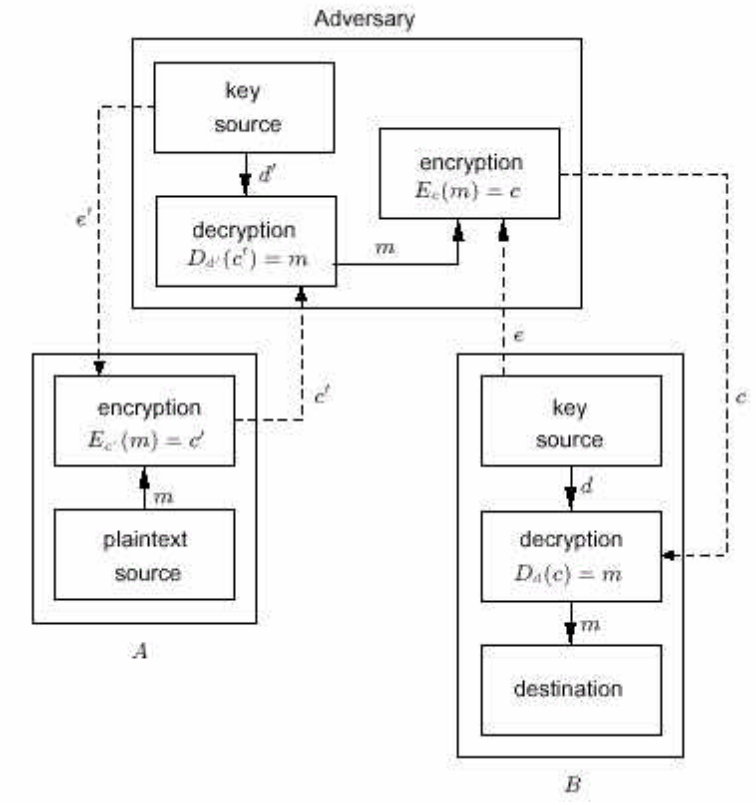

Figura 3.1 - Cenário de um ataque do tipo *men-in-the-middle*

Nesse tipo de ataque, o adversário intermedia toda a comunicação entre as entidades A e B. Para efeito de comunicação, quando A envia uma mensagem para B ele esta na verdade enviando para o adversário pensando que esse é a entidade B, ou seja, o adiversário personifica a entidade B e do mesmo modo o faz quando B quer se comunicar com A, nesse caso ele personifica a entidade A. Desse modo TODAS as informações trocadas por A e B passam pelo adversário que dessa forma pode altera a informação como lhe bem o convier.

Para que esse cenário ocorra, uma das possibilidades é que a solicitação da chave publica de B por A seja interceptada pelo adversário e o mesmo tem que ocorrer quando B solicitar

a chave de A. Isso pode ser feito on-the-fly caso o adversário possua controle sobre um roteador por onde as mensagem devem passar, por exemplo. Nesse caso ele precisa monitorar com bastante atenção essa comunicação (um programa especial pode desempenhar esse função).

No exemplo de interceptação dado, as solicitações são feitas diretamente a outra parte. Existem várias formas de evitar esse cenário. Um método simples é ir pessoalmente a outra parte obter a sua chave pública. Ou pedir a uma outra entidade em quem se confie uma copia de quem se deseje. Ir pessoalmente é uma ótima solução quando não se ve a muito tempo um amigo, mas não resolve o problema se ele não esta fisicamente acessivel (por exemplo, do outro lado do mundo). Pedir a uma pessoa confiável é uma boa solução, ainda mais se essa pessoa possui muitas chaves consigo e está sempre acessível, como um servidor de chaves.

Mas nesse sistema todo onde entra o certificado digital ? Como a carteira de motorista, o certificado digital associa a pessoa que o possui, um direito e algumas informações garantidas por uma outra entidade em que todos confiam, no caso o orgão emissor da carteira. Se um entidade possui um certificado digital, ao se comunicar com uma outra, basta avisar a esse outra da existencia do seu certificado. Essa segunda entidade vai ao orgão emissor e confere os dados do certificado de quem deseja entrar em contato com ele e verifica suas credencias e principalmente a veracidade de sua chave pública.

Um certificado digital é um arquivo que possui basicamente 3 áreas:

a) a chave pública
b) Informações do certificado como, validade, nome da pessoa, orgão emissor, etc
c) um ou mais assinaturas dos orgãos que garantem o certificado

3.1- Formato do Certificado

Como mencionado anteriormente, um certificado digital é uma coleção de informações e assinaturas segundo um molde que garanta a qualquer orgão ler e emitir um certificado. A necessidade de interoperabilidade levou a criação de basicamente dois padrões principais de certificados:

** Padrão X-509*

Esse padrão foi criado pela ITU-T com parte do sistema X-800 de segurança. Algumas RFC referentes ao padrão X-509 são:

a) 2528 - Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates

b) 2510 - Internet X.509 Public Key Infrastructure: Certificate Management Protocols

c)2511 - Internet X.509 Certificate Request Message Format

d)2527 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

e)2459 - Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

f) 2560 - X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

** Padrão PGP*

O formato de certificado usado pelo PGP[2] tornou-se um padrão de-facto pelo seu grande uso na troca de mensagens por e-mail. O software PGP baseia-se no X-509 e expande o campo de certificados para um estrutura mais coerente para o seu propósito. Isso será visto mais adiante.

3.1.1- Campos Principais

No padrão criado pelo PGP os campos principais são os seguintes:

a) O número da versão do soft PGP - identifica a versão do soft que criou o certificado

b) A chave pública do proprietário do certificado - a chave pública aliada ao algortimo que a gerou

c) A informação pessoal do propriétario - consiste na identidade do usuário, como seu nome, ID ou foto

d) A assinatura digital do proprietário - também chamado de auto-assinatura, esta é a assinatura usando a chave privada correspondente a pública existente no certificado

e) O periodo de validade do certificado - a data de inicio e fim da validade do certificado

f) O algorirtmo preferido para codificação - estabelece em qual algoritmo o possuidor do certifido prefere que as mensagem sejam codificadas

O padrão X.509 é mais amplo e define os seguintes campos:

a) Número da versão - define qual a versão usada no certificado, atualmente na versão 3

b) A chave pública do proprietário do certificado - a chave pública aliada ao algortimo que a gerou

c) Número de série do certificado - gerado pela CA criadora do certificado de forma a identificá-lo unicamente. Esse valor em importante em diversas situações como na passagem de um certificado para a lista de certificados revogados (Certification Revogation List)

d) O indenficador único do dono do certificado - este campo é idealizado para ser único em toda a Interntet, ele é composto de várias partes, como por exemplo:

CN=Bob Allen, OU=Network Security Division, O=Network Associates, Inc., C=US

(Os campos são: Common Name, Organizational Unit, Organization, and Country.)

e) O periodo de validade do certificado - a data de inicio e fim da validade do certificado

f) o nome da CA que publicou o certificado - do mesmo modo que em d) só que em referência a CA.

g) a assinatura digital da CA - a assinatura usando a chave privada da CA

h) o identificador do algoritmo usado para assinatura - define qual o algoritmo usado em g)

Existem alguma diferenças importantes entre os dois padrões, são elas:

- X.509 suporta apenas um dono para a chave pública presente no certificado
- X.509 suporta apenas uma única assinatura digital atestando a validade da chave
- qualquer um pode criar seu próprio certificado no formato PGP porem com X.509 o certificado tem que ser requisitado a um CA .

A seguir, a figura mostra como é gerado e quais os campos de um certificado X.509 v3

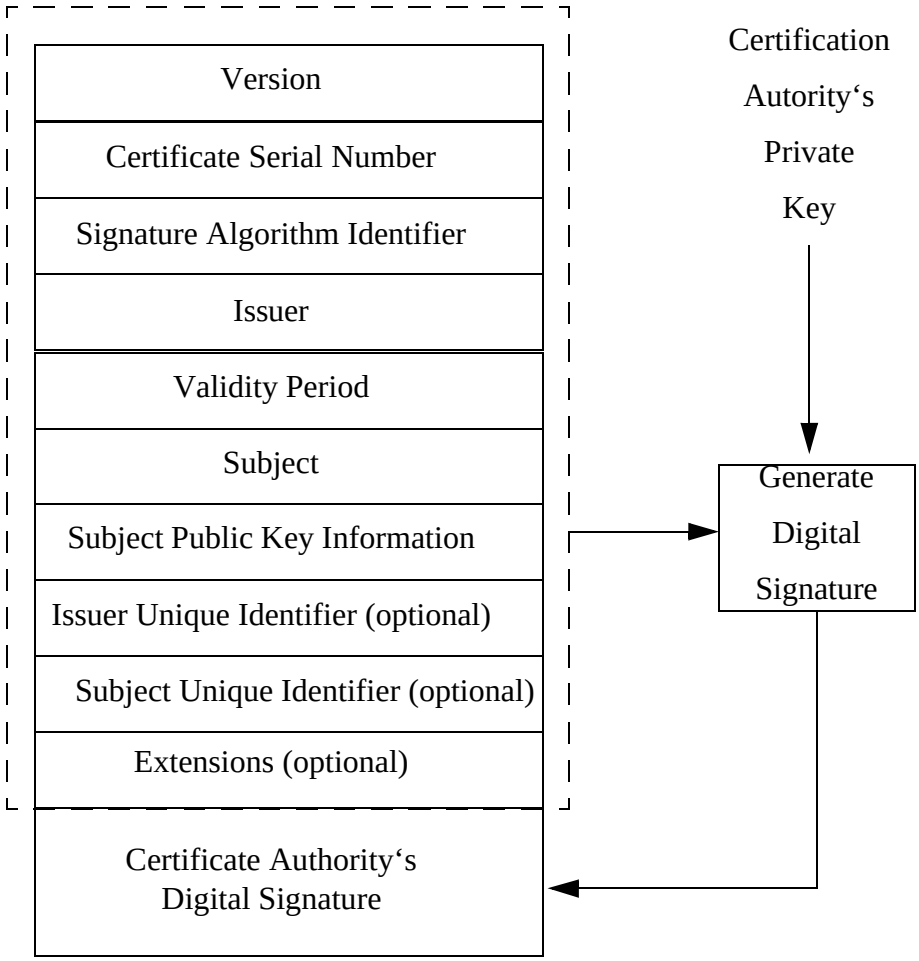

Figura 3.2: Formato de Certificado do padrão X.509 versão 3

3.2- Campos Importantes

a) Indenficador único e nome da CA

O objetivo desse campo é definir unicamente na Internet tento o nome do usuário como o nome da CA, o modo adotado é o seguinte:

Common Name -> CN=Martins, Alessandro,
Organizational Unit -> OU=RAVEL Lab,
Organization -> O=COPPE-UFRJ,
Country ->C=BR

b) Campo de Extensões

Proporcionar um meio para associar dados adicionais para informações pessoais, chaves públicas e gerencia de chaves e etc.

Define 3 sub campos:

Tipo da extensão

Indicador de importância

Valor do campo

O indicador de importância pode ser usado para deterinar se uma aplicação aceita ou não um certificado caso a aplicação não compreenda o campo tipo da extensão

Referências

[1] National Institute of Standards and Technology - www.nist.gov

[2] Preaty God Privaty - www.pgpi.org

[3] Feghhi, Jalal and Jalil and Williams, Peter, *Digital Certificates: Applied Internet Security*,Addison-Wesley Publishing, 2000

[4] Diffie Hellman key exchange