Criptografia

Universidade Católica do Salvador
Curso de Bacharelado em Informática
Teleprocessamento e Redes
Data: 14/05/01
Aluno: Leonardo Thomas T. Santos

Índice

Introdução

Neste trabalho, serão mostrados as principais técnicas utilizadas em criptografia e autenticação, frisando suas principais características e seus usos na área computacional.

Muitas vezes se deseja que uma mensagem seja transmitida a alguém sem que ninguém a mais tome conhecimento do seu conteúdo. Uma forma fácil de se fazer isso, seria fazer com que ninguém tenha acesso a esta mensagem, exceto o destinatário. Contudo, num meio como a Internet, não se pode agir desta forma tornando inviável a solução.
Quando uma informação é enviada pela Internet, ela passa por diversas máquinas, até chegar ao destinatário. Assim, uma forma de solucionar o problema seria fazer com que somente o destinatário pudesse compreender a mensagem, ou seja, criptografá-la.

Criptografia

Criptografia (do grego *kriptós* = escondido, oculto *grápho* = grafia) é a ciência que visa escrever em cifra o em código, de maneira que somente o destinatário possa entender o que foi escrito. Em geral, o deciframento se dá através de uma chave, que fica mantida secretamente em poder do destinatário. É uma ciência utilizada desde a antigüidade, no sistema de escrita hieroglífica, dos egípcios.
Hoje, a criptografia é uma ciência relacionada com a segurança de sistemas, estando bastante difundida em ambientes que utilizam redes de computadores. Isto ocorre porque uma rede transmite uma grande quantidade de informações, incluindo informações sigilosas, estratégicas, e vitais para as organizações.
Desta forma, é preciso garantir a segurança destes dados para que a rede não esteja sujeita a ações como a escuta de informações não permitidas ou até mesmo alteração da informação original.

Paralelamente à criptografia, temos a **criptoanálise**, que é a ciência de determinar a chave ou determinar o conteúdo de mensagens cifradas, sem conhecer a chave. Juntando estas duas ciências, temos a **criptologia.**

Características de Sistemas de Criptografia

Um sistema de criptografia segue a premissa fundamental de que a segurança não deve estar calcada nos algoritmos de codificação e decodificação, mas sim na figura da **chave:** O sistema deve garantir que nem mesmo o autor do algoritmo seja capaz de decifrar uma mensagem sem o conhecimento da chave dela. Desta forma, assume-se que um criptoanalista pode conhecer por completo as técnicas utilizadas, mas desconhecendo o valor da chave não terá como decodificar, e o sistema estará seguro.
Além disso, um sistema robusto deve supor que o criptoanalista possui grandes quantidades de mensagens originais e suas correspondentes cifradas. Supõe também que se pode escolher uma mensagem e saber como é a sua correspondente cifrada.

Normalmente criam-se medidas para evitar que estas suposições se tornem realidade, mas um sistema realmente seguro, deve se exigir que um sistema de criptografia leve em consideração esses pressupostos.

Um sistema em que a chave de deciframento é igual à chave de ciframento é denominado **sistema de chave simétrica** ou **privada**. Já no caso destas chaves serem diferentes, temos os **sistemas de chaves assimétricas** ou de **chave pública**.
Os algoritmos se encontram facilmente por toda a internet. Dentre os algoritmos de chave simétrica mais conhecidos temos o **DES**. Para os sistemas assimétricos, o algoritmo mais conhecido é sem dúvida o **RSA**.

A criptografia não impede

- Que apaguem seus dados
- Que um hacker registre arquivos encriptados para uma análise posterior
- Que se quebre a chave: A depender do algoritmo usado, é possível encontrar uma forma relativamente fácil de se quebrar a chave
- Que os dados sejam interceptados no processo de envio

A criptografia se preocupa com

- **Sigilo:** A mensagem só pode ser compreensível para quem for autorizado
- **Integridade da informação:** A mensagem vai ser recebida da mesma forma que foi enviada
- **Autenticação de usuário:** O sistema é capaz de saber se a pessoa com quem se fala é quem alega ser
- **Autenticação de remetente:** Faz com que o usuário tenha certeza que a mensagem recebida foi enviada pelo remetente
- **Autenticação de destinatário:** Certifica de que a mensagem foi enviada de fato para o destinatário
- **Autenticação de atualidade:** Que a mensagem seja atual, não tratando-se de uma mensagem antiga retransmitida

Criptografia tradicional

Cifras de substituição

Baseia-se na substituição de um caracter ou um grupo de caracteres por outro, tomando como base uma tabela de substituição. Este código pode ser quebrado com uma análise da freqüência dos caracteres do texto cifrado com relação aos caracteres que aparecem em determinado idioma.
Podemos enumerar algumas formas de substituição:

- **Monoalfabética:** cada letra do texto original é substituída por uma outra, conforme a tabela. Um exemplo seria trocar cada letra por outra 5 letras na frente, seguindo a ordem alfabética (toda vez que aparecesse um A na mensagem, seria cifrado como F). Considerando o nosso alfabeto, com 26 letras, este método ofereceria apenas 26 chaves possíveis, podendo ser facilmente quebrado.
- **Por deslocamento:** A chave indica o quanto se deve deslocar para fazer cada substituição. Diferente da anterior, as letras não são substituídas por uma letra sempre n posições à frente. Uma chave na forma 010402 indicaria que a primeira letra deve ser deslocada de 1, a Segunda de 4 e a terceira, de 2. Para cifrar as demais letras, a chave seria usada novamente.
- **Por polígramos:** Utiliza se um grupo de caracteres ao invés de um único caracter.

Cifras de transposição

Baseia-se na troca da ordem da mensagem, parametrizada por uma chave, que pode ser uma senha, uma seqüência de números ou mesmo uma frase secreta.
Exemplo:
Senha: “ACHEI”
Frase: “OI TUDO OK”
Parametrização: pela ordem alfabética das letras da senha

0	1	3	2	4
A	C	H	E	I
O	I		T	U
D	O		O	K

Frase cifrada, montada pela leitura ordenada das colunas da tabela:
“ODIOTO UK”

Sistemas de chave única (simétricos)

São chamados desta forma porque utilizam a mesma chave para criptografar e descriptografar. O algoritmo DES (*data encription standard*) bastante conhecido neste tipo de sistema, é um ciframento composto de blocos de 64 bits, em blocos de 64 bits. Sua chave é composta de 56 bits e mais 8 bits que são usados para a paridade. Para cifrar uma mensagem, o algoritmo realiza uma série de transposições, substituições dentre outras operações.

O DES tem basicamente os seguintes passos:

1. Uma transposição de 64 bits do texto original
2. Os16 estágios seguintes são transposições feitas com diferentes funções da chave
3. Depois troca-se os 32 bits da esquerda com os 32 bits da direita (do bloco de 64 bits)
4. Inversão da transposição inicial.

Existem muitas variações do DES. Uma delas é o DES triplo, que é a aplicação três vezes sobre o dado original.

Segurança do DES

Várias tentativas de quebra (criptoanálise) já foram feitas neste algoritmo, inclusive tentativas bem sucedidas. O DES pode ser quebrado pelo método da "força bruta" tentando-se todas 2^{56} combinações possíveis. Existem diversos trabalhos publicados com técnicas mais avançadas que se propões a quebra do DES.
Desde sua criação, sempre se levantou questionamentos sobre a segurança do DES. Existem inclusive suspeitas de que existam "portas dos fundos" no algoritmo, de forma a facilitar o deciframento pelo governo americano.

Sistemas de chave pública (assimétricos)

Utilizam pares de chaves da seguinte forma: Cada usuário possui um par de chaves, sendo que uma das chaves é publicada ou tornada acessível aos usuários, denominada **chave pública**. Outra, é de uso particular de cada um, e não é revelada a ninguém. Esta é a **chave privada**. Quando a chave pública é usada para codificar uma mensagem, esta só poderá ser decodificada pela chave privada e vice-versa.

O RSA (Rivest-Shamir-Adleman) é o algoritmo que se tornou mais conhecido para este tipo de sistema. Sua segurança é baseada na dificuldade de se fatorar um produto entre dois números primos extensos.

Funcionamento do algoritmo:

Para a determinação das chaves, o algoritmo age da seguinte forma:

1) Escolhe dois números p e q primos extensos (na ordem de 1^{100})
2) Calcula-se n = p * q e z = (p - 1)*(q - 1)
3) Escolhe-se o número primo d em relação a z
4) Encontra-se e na forma (e * d)mod z = 1

Para criptografar a mensagem A, é calculado $C = A^e \pmod n$. Para descriptografar C, basta calcular $A = C^d \pmod n$. Com isto, nota-se que para criptografar , é necessário o "e" e o "n" e para descriptografar, utiliza-se o "d" e o "n". Logo, a chave pública é o par (e,n) e a chave privada, o par (d,n). Se fosse possível fatorar o valor de n (público), seria possível chegar à d, porém, fatorar números extensos é muito custoso.

Vejamos um exemplo ilustrativo de uso do algoritmo:
Escolhem-se: **p = 3** e **q = 11**
Calculam-se: n = p * q e z = (p - 1)*(q - 1)
n = 3 * 11 z = (3 - 1)*(11 - 1)
n = 33 z = 20

O número d escolhido foi 7, já que 7 e 20 são primos entre si, assim **d = 7**
O valor de e se identifica com 3 pois
(3 * 7) mod 20 = 1, então **e = 3**

Admitindo que cada letra do alfabeto será dada por um número, temos

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cifrando teremos:

	A	A^3	$C = A^3 (\text{mod } 33)$
Caracter	Número		
R	18	5832	24
E	5	125	26
D	4	64	31
E	5	125	26
S	19	6859	28

Recuperando o original, teremos:

$C = A^3 (\text{mod } 33)$	A^7	$C = A^7 (\text{mod } 33)$	Caracter
24	4586471424	18	R
26	8031810176	5	E
31	27512614111	4	D
26	8031810176	5	E
28	13492928512	19	S

Como este é um exemplo ilustrativo, foram escolhidos números pequenos. Na implementação deste algoritmo, deve ser considerado que serão trabalhados números grandes, tomando-se cuidado para não ocorram erros devido a estouro da capacidade das variáveis envolvidas.

É importante frisar também que na prática, um método pode ser utilizado em combinação com outro sem problemas. Uma mensagem pode ser cifrada inicialmente pelo DES e em seguida, a mensagem cifrada pode se codificada usando o RSA. Neste caso, para desencriptar a mensagem, seria preciso utilizar a chave usada no RSA. Em seguida, seria preciso aplicar a chave usada no DES, recuperando a informação original.

Assinatura digital

Outra forma de utilizar o par de chaves seria codificar a mensagem com sua chave privada e disponibilizar a mensagem para que algum usuário pudesse desencriptá-la usando a chave pública de quem encriptou.
Neste caso, teremos uma mensagem que pode ser decifrada por qualquer um, mas que só pode ter sido cifrada por uma única pessoa. Este efeito de assinatura deu o nome de **assinatura digital** a este processo.

Protocolos de autenticação em sistemas distribuídos

O processo de autenticação é o que garante a verificação da **identidade** das entidades quando se estabelece uma comunicação. Trata-se de um mecanismo que funciona de forma a garantir que o receptor da mensagem possa confiar na identidade do transmissor e na integridade da mensagem.
Baseiam-se em sistemas de criptografia e podem usar DES (como o sistema Kerberos, do MIT) ou RSA.

Os protocolos que serão explicados são voltados para sistemas que usem um conjunto de máquinas ligadas através de uma rede. Admitem que não há memória compartilhada e que a comunicação entre as máquinas é feita apenas através de mensagens pela rede.
Por fim, destinam-se tanto a sistemas que funcionem com chave única quanto a sistemas que funcionem com duas chaves, podendo prover os seguintes serviços:

- Comunicação interativa
- Comunicação sem conexão
- Assinatura digital

Previamente, cada usuário deposita sua chave com segurança no servidor de autenticação **AS.**

Os serviços de autenticação levam em consideração os seguintes ítens quanto ao intruso:

- O intruso pode ter acesso a qualquer ponto de rede, podendo copiar ou alterar uma mensagem.
- É possível retransmitir uma mensagem, tentando se passar por outra pessoa.
- Pode não entender o conteúdo de uma mensagem, embora se saiba o protocolo usado.
- Um intruso pode saber as mensagens que estão sendo usadas na comunicação, inclusive quando a comunicação foi iniciada.
- Pode interferir na comunicação das duas entidades, atrapalhando o andamento

Comunicação interativa

Ocorre entre **A** e **B**, duas máquinas que realizam uma conversa sincronizada pela rede.

Protocolo de chave privada

Para que a comunicação entre **A** e **B** se realize, é preciso que seja fornecida uma **chave de conversação**. A obtenção de chaves de conversação deve se dar de forma confiável, com o intermédio do servidor **AS**.

Se utilizam dos método de criptografia simétricos, assumindo que **AS** possui as chaves de todos usuários.

Obtenção da chave de conversação:

A deve obter a chave de conversação com **AS**. **A** envia uma mensagem para **AS** informando que deseja comunicar-se com **B**, e fornecendo um identificador **IA** para a mensagem. Representa-se da seguinte forma:

1. **A -> AS: A, B, IA**

Com isto , **AS** consulta seu molho de chaves e pega as chaves privadas **KA** e **KB**, computando uma nova chave de conversação **Ck**, que será usada na conversação.

AS envia a mensagem para **A** encriptada com a chave de **A**.

2. **AS -> A: EKA(IA, B, Ck, EKB(Ck, A))**

Somente **A** poderá desencriptar esta mensagem e obter a chave de conversação **Ck.**

Comunicando a chave de conversação:

Para comunicar-se com **B**, usando a chave **Ck**, primeiro **A** envia a mensagem

3. **A -> B: EKB(Ck, A)**

A partir daí, somente **B** pode desencriptar a mensagem e utilizar **Ck** para comunicar-se interativamente com **A**.

Assim, **A** e **B** têm certeza que as mensagens cifradas com **Ck** são compreensíveis apenas entre eles.

No entanto, ainda deve ser tratado um problema: um intruso pode reter uma mensagem **3** para retransmitir posteriormente. A menos que **B** tenha um histórico com todas mensagens de **A**, não será possível saber se é uma retransmissão ou não.

Uma forma de se dificultar isso seria fazer com que **AS** incluísse uma marca de tempo nas mensagens em que há a passagem da chave **Ck,** aumentando a segurança.

Protocolo de chave pública

É usado em sistemas que utilizem a criptografia assimétrica. Assume-se que o servidor de autenticação **AS** possui as chaves públicas de todos usuários.

Para cada usuário **X**, sua chave pública é **PKX** e sua chave privada é **SKX**.

Primeiro, se **A** deseja comunicar-se com **B**, **A** envia a mensagem solicitando início de conversação:

1. **A -> B : EPKB(IA, A)**

Somente **B** poderá ler a mensagem e entender que tem como origem **A**, com o identificador **IA**.
Já que a mensagem **1** pode se tratar de uma mensagem feita por um intruso, é feito a confirmação do inicio da conversação de **B** com **A**:

2. B -> A: EPKA(IA, IB)

3. A -> B: EPKB(IB)

Ao desencriptar **2**, **A** recebe a confirmação de **B**. Com o envio bem sucedido de **3**, estabelece-se a conexão.
Caso **A** não tenha a chave pública de **B**, necessária para iniciar a comunicação, **A** pode solicitar para **AS**.

A -> AS: (A, B)

Que é respondido com :

AS -> A : ESKAS(PKB, B)

A , que é possuidor da chave pública de **AS**, desencripta a mensagem assinada por **AS**, acessando a chave pública de **B**.

Comunicação sem conexão

Este tipo de comunicação tem como exemplo típico a comunicação via e-mail. Nela, a comunicação não depende da disponibilidade do receptor nem do emissor.

Protocolo de chave privada

Para que **A** envie uma mensagem **M** para **B**, é preciso que antes seja informada a chave de conversação da mesma forma que é feita na comunicação interativa.

A – AS: A, B, IA

AS -> A: EKA(IA, B, CK, EKB(CK, A))

Assim, **A** pode enviar a mensagem codificada com **CK**. No cabeçalho da mensagem, manda **CK** encriptada com **KB**.

A -> B: EKB(CK, A); ECK(M)

Feito isto, **B** pode desencriptar **EKB(CK, A)** , extraindo **CK** para em seguida obter o conteúdo de **ECK(M)** aplicando **CK**.

Protocolo de chave pública

Sendo que **A** e **B** possuem meios de obter a chave privada do outro com auxílio de **AS**. A mensagem de **A** para **B** fica da seguinte forma:

A ->B: EPKB(A, I, ESKA(B))

O parâmetro **A** indica o emissor, **I** indica um identificador para a mensagem que é usado para ligar o cabeçalho da mensagem ao seu corpo, **ESKA(B)** coloca **A** como emissor legítimo, pois só **A** pode gerar esta expressão.

Assinatura digital

Em geral, o envio de mensagens ligadas a operações bancárias são um ponto crítico, que requer um ambiente seguro. Surge então o esquema de assinatura digital, obedecendo uma série de premissas:

1. A assinatura tem que ser única para cada usuário
2. O emissor não pode fazer com que uma mensagem seja enviada sem sua assinatura
3. Uma mensagem não pode ter sua assinatura modificada pelo receptor
4. Não pode ser possível retirar a assinatura de uma mensagem para colocar em outra

Protocolo de chave privada

Para que 4 seja satisfeita, a assinatura incorpora características da própria mensagem. Assim, se A deseja enviar uma mensagem para B, o valor característico **CS** é calculado e enviado para **AS.**

A -> AS: A, EKA(CS)

AS fornece a assinatura da mensagem, que será criada em função de **A** e **AS**. Observa-se que **CS** é encriptada por **AS**:

AS -> EKAS(A, CS).

A anexa a assinatura no rodapé de sua mensagem em envia para **B**. Ao receber a mensagem, **B** deve verificar se a mensagem é legítima:

B -> AS: B, EKAS(A, CS)

AS -> B: EKB(A, CS)

Com isto, **B** confere o valor de **CS** e em caso de sucesso, a mensagem é legítima.

Protocolo de chave pública

Tomemos como exemplo o envio da mensagem **M** de **A** para **B**:

S = ESKA(M)

S é a assinatura da mensagem **M**, encriptada usando a chave privada de **A**. Em seguida, **A** encripta **S** usando a chave pública de **B**:

C = EPKB(S)

C é enviada para **B**, que ao receber desencripta com sua chave privada, chegando a **S**.

S = DSKB(C)

Com **S**, **B** aplica a chave pública de **A**, recuperando **M**.

M = DPKA(S).

B garante que a mensagem foi criada por **A**, uma vez que só **A** poderia ter gerado **ESKA(M).**

Aplicações

PGP

O e-mail é um recurso que todos usam, porém toda a sua facilidade tem um preço: não oferece segurança. Como se sabe, no processo de envio de uma mensagem, é preciso se conectar a um servidor SMTP. Depois esta mensagem é retransmitida, passando por vários roteadores até chegar até seu destino, ficando armazenada lá. Em qualquer ponto deste caminho, um administrador de sistema ou hacker pode muito bem ver ou alterar o conteúdo da mensagem. Com a senha de acesso, é possível também ler o e-mail sem que se tome conhecimento. Ainda é possível que qualquer pessoa mande uma mensagem com a identidade de outra.

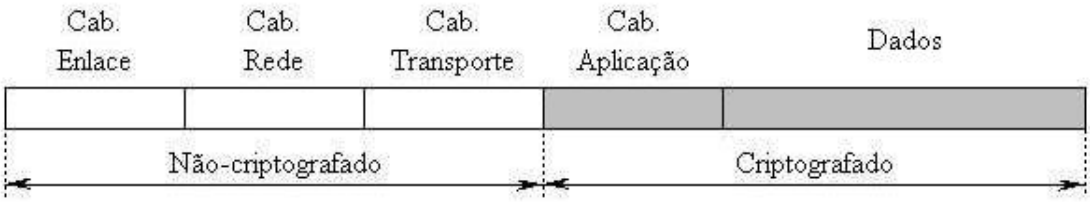
Uma forma de garantir que uma transmissão de dados seja segura, de forma que apenas o receptor esteja apto a ler a mensagem e sabendo que o transmissor é realmente quem diz ser e se a mensagem foi ou não alterada é com o uso de um programa denominado PGP.
Este programa disponibiliza à um baixo custo um serviço de cripto da seguite forma:
A mensagem é criptografada com o algoritmo IDEA (do tipo simétrico, que cifra blocos de 64 bits com chave de 128 bits) usando uma chave K e esta chave K é codificada pelo RSA usando a chave pública do destinatário.
A seguir, ambos são enviados para o destinatário.
Ao chegar no destinatário, o mesmo desencripta a chave K usando sua chave privada e em poder de K, desencripta a mensagem.

O PGP (Pretty Good Privacy) é um programa bastante conhecido, e se tornou polêmico, uma vez que seu criador (Phil Zimmermann) chegou a ser investigado pelo FBI, acusado de infringir a patente do algoritmo RSA.

HTTPS e SSL

O HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) junto ao protocolo SSL (Secure Sockets Layer). Trata-se de uma aplicação de segurança utilizada no ambiente Web. Sistemas de Home Banking e compras on-line são exemplos típicos em que este protocolo é utilizado.
O SSL foi idealizado por um grupo liderado pela Netscape Comunications, Verisign e Sun. Foi feito para operar como uma camada de segurança entre a camada de transporte e os protocolos de aplicação (modelo TCP) como HTTP, FTP, SMTP dentre outros.

Formato de um quadro SSL:



O SSL é flexível, podendo aceitar uma série de algoritmos tanto simétricos e assimétricos. A escolha do algoritmo é feita no início da sessão e é negociado entre o cliente e o servidor.

O SSL é implementado no próprio browser, e oferece uma série de serviços, dentre eles:

- Autenticação – Verificando o autor da mensagem
- Integridade – Verificando se os dados foram alterados
- Criptografia – Garante sigilo
- Troca de chaves criptográficas – Torna a segurança ainda maior

Como foi feito de forma a atender o usuário comum, o SSL é praticamente transparente ao usuário, que não precisa fazer a manipulação de chaves criptográficas: Quando é feita uma conexão à uma url com https (um site de Home Banking por exemplo), o browser utiliza uma porta diferente da 80 (como seria em uma url com http) e o SSL é ativado. O usuário pode ficar sabendo disso verificando um aviso que é enviado pelo browser (no caso do Internet Explorer, aparece um cadeado).

Conclusões

Diante de todo avanço que houve na criptografia, não se pode afirmar que existe uma forma 100% segura de criptografar. Neste ramo, entende-se por segurança a dificuldade que o método impõe para que o criptoanalista consiga chegar à chave.
Um método que funcione muito bem em determinadas aplicações pode não ser adequado para outras.
O DES é adequado para pessoas que desejem guardar arquivos criptografados, enquanto o PGP, é uma boa alternativa para quem deseja criptografar um e-mail.
O caso mais crítico seria em ambientes em que o tráfego de informações é muito intenso, e muitos dados sigilosos como senhas de cartão são transmitidos. Nestes casos, recomenda-se o uso do RSA.
Segundo pesquisas, a fatoração de um número de 200 dígitos requer 4 milhões de anos para ser processada. Fatorar um número de 500 dígitos levaria 10^{25} anos. Mesmo que um computador consiga chegar a tal marca, seria muito custoso em relação à facilidade com que se escolhe os números, bastando escolher números maiores.

Questões

1. O que a criptografia pode fazer ?

2. Porque a segurança de um sistema de criptografia não pode estar baseada simplesmente no algoritmo?
   Por que como algoritmo foi feito por alguém, é preciso que se garanta que nem mesmo este alguém seja capaz de decifrar o código. Com isto transfere-se o poder de deciframento do código para o usuário, através do uso de chaves.
3. O que significa dizer que um sistema é seguro?
   Significa dizer que oferece dificuldade o suficiente para frustar as tentativas de invasão.
4. Existem funções que apresentam a característica de serem praticamente impossíveis de se inverter. Como isto pode ser utilizado na criptografia ?
   Uma função unidirecional é com segredo se existe uma informação que torna a computação da sua inversa possível. A função produto de dois primos é unidirecional sem segredo.
   Há casos em que uma função unidirecional sem segredo é útil, um exemplo típico é na proteção de senhas. O arquivo de senhas apresenta as senhas cifradas por uma função unidirecional sem segredo (e de inviável deciframento). Quando o usuário inicia sua sessão, fornece a senha que é então cifrada e comparada com a senha cifrada armazenada. Desta maneira, exige-se apenas a integridade do arquivo de senhas, não mais exigindo

controle de acesso ao arquivo.

5. Num processo de autenticação, como é possível impedir que um intruso retransmita mensagens ?
   O processo não impede a retransmissão. No entanto, é capaz de checar se uma mensagem é retransmitida ou não verificando marcas de tempo inserida pelo servidor de autenticação confiável AS.

Bibliografia

Criptografia e autenticação
http://infojur.ccj.ufsc.br/arquivos/artigos/criptografia.html
http://www.inf.ufrgs.br/gpesquisa/procpar/disc/cmp134/trabs/T2/981/autenticacao.html
http://www.iweb.com.br/criptografia.htm

Informações sobre o PGP
http://www.terravista.pt/fernoronha/1339/BRAND5.htm

SSL
http://www.gta.ufrj.br/~eric/ssl/introducao.htm