Curso de Ciência da Computação
Disciplina: Segurança e Auditoria da Informação - 8º período
Professor: José Maurício S. Pinheiro

AULA 5: Criptografia e Esteganografia

A criptografia é muito antiga existindo na escrita hieroglífica egípcia, utilizada para codificar os planos de batalha na época do império romano e, na idade média, para proteger documentos escritos em papiros. No início dos anos 1970, a criptografia foi considerada uma área de investigação acadêmica e largamente utilizada na segurança de sistemas de informação computacionais.

1. Criptografia

A forma mais utilizada para prover a segurança da informação numa rede de computadores é a utilização da criptografia. A palavra tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos utilizando um conjunto de técnicas que torna a mensagem incompreensível e chamada comumente de "texto cifrado", através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza. As mensagens legíveis são chamadas de texto plano ou texto limpo e as ilegíveis, são chamadas de texto cifrado (Figura 1).

Figura 1 - Criptografia

A criptografia fornece técnicas para codificar e decodificar informações, tais que as mesmas possam ser armazenadas, transmitidas e recuperadas sem sua alteração ou exposição. Em outras palavras, as técnicas de criptografia podem ser usadas como um meio efetivo de proteção do conteúdo das informações suscetíveis a ataques, estejam elas armazenadas em um computador ou sendo transmitidas pela rede.
A criptografia é o meio primário para oferecer confidencialidade às informações transmitidas entre as redes locais de computadores ou através da Internet. Pode ser usada para qualquer tipo de informação transmitida, desde um e-mail até um arquivo com dados confidenciais. Pode-se citar o exemplo dos *laptops*, que, ao serem deixados em um quarto de hotel, poderiam ter as informações acessadas por pessoas não autorizadas.

O processo criptográfico consiste em transformar um texto simples, através de uma função parametrizada por uma chave (senha), em um texto inteligível. A saída desse processo de criptografia é chamada texto cifrado ou criptograma. Após o processo de criptografia, o texto é então transmitido ao destinatário. Este conhece o método utilizado para a criptografia e também conhece a chave, possibilitando a transformação do texto criptografado em texto simples novamente. Se a mensagem for interceptada por alguém, será necessário descobrir a chave de criptografia bem como o seu método, para que se possa utilizar a mensagem capturada.
Um exemplo de processo criptográfico é o dispositivo conhecido como Criptex (Figura 2), um cofre de forma cilíndrica, composto por 5 anéis com números e letras do alfabeto que, uma vez colocados em certa posição, permitem retirar do seu interior um papiro com uma mensagem secreta. Forçando-se sua abertura, sem alinhar corretamente os anéis (código), quebra-se uma ampola de vidro contendo vinagre no interior do artefato, o qual danifica o papiro, tornando a mensagem ilegível.

Figura 2 - Criptex

1.1. Tipos de Criptografia

A criptografia é um mecanismo de segurança que permite a implementação de diversos serviços (autenticação, não-repúdio, integridade, confidencialidade). Para tanto existem dois tipos básicos de criptografia: simétrica e assimétrica. Embora a criptografia simétrica seja menos segura, ela é mais rápida, sendo atualmente utilizada em conjunto com a criptografia assimétrica para aumentar a eficiência da troca de mensagens seguras. As chaves são criadas através de operações matemáticas de tal forma que, apesar de serem relacionadas, é virtualmente impossível descobrir a outra, tendo apenas uma delas.

1.2. Sistema de chave simétrica

Na criptografia simétrica (ou de chave privada), os usuários envolvidos devem ter prévio conhecimento da chave (senha). Isto a torna muito vulnerável a falhas de segurança (Figura 3). Nesta técnica uma mesma chave (senha) é utilizada para criptografar e decriptografar uma mensagem que, portanto, deve ser de conhecimento tanto do emissor como do receptor da mensagem.
Em cifradores simétricos, o algoritmo de criptografia e decriptografia são os mesmos, mudando apenas a forma como são utilizadas as chaves. Um exemplo de algoritmo simétrico é o DES (*Data Encryption Standard*), cuja

chave possui tamanho de 56 bits. Entretanto algoritmos com chaves maiores estão disponíveis resultando em maior segurança.

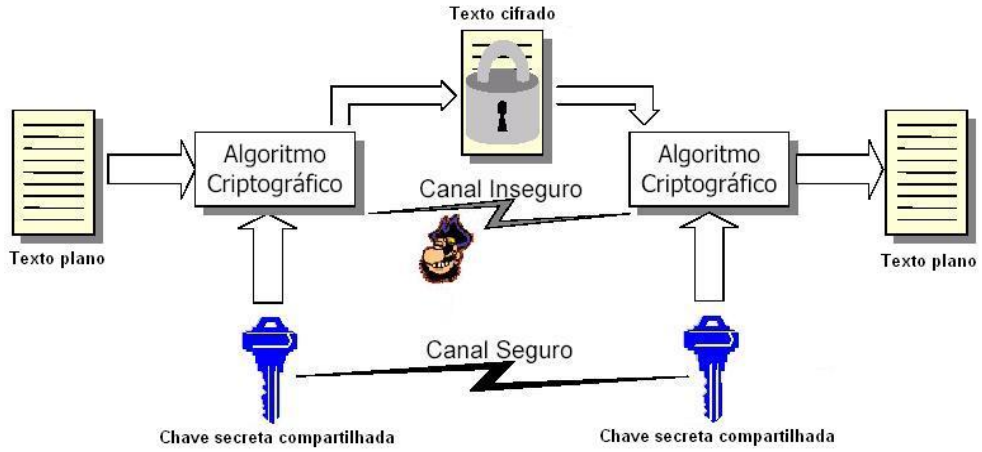

Figura 3 - Exemplo de chave simétrica

Uma mensagem para ser enviada é encriptada pelo emissor, com uma chave secreta compartilhada que é de seu conhecimento. Para o receptor conseguir decifrar esta mensagem, deve ter a mesma chave secreta utilizada pelo transmissor. Esta chave secreta compartilhada é então enviada por um canal seguro para o receptor.
Com este modelo pode-se garantir a confidencialidade da mensagem, porque somente o transmissor e o receptor têm conhecimento da chave secreta. O texto cifrado não sofre alteração quanto ao seu tamanho. É importante salientar também que o texto cifrado não contém qualquer parte da chave.
Existem vários algoritmos que usam chaves simétricas, como o DES, o IDEA, e o RC.

- **DES** (*Data Encryption Standard*): criado pela IBM em 1977, faz uso de chaves de 56 bits. Isso corresponde a 72 quatrilhões de combinações. Em 1997, esse algoritmo foi quebrado por técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet;
- **IDEA** (*International Data Encryption Algorithm*): criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES;
- **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.

Existem ainda outros algoritmos como o AES (*Advanced Encryption Standard*) - que é baseado no DES, o 3DES, o Twofish e sua variante Blowfish, entre outros.

1.3. Sistema de chave assimétrica

Na criptografia assimétrica (ou de chave pública) existe um par de chaves relacionadas entre si. Qualquer informação encriptada com uma delas somente poderá ser decriptografada com a outra. Uma chave é usada para cifrar a informação e uma outra chave diferente para decifrar a informação. O que for encriptado utilizando uma chave somente poderá ser visualizado com a outra.
Entre os algoritmos que usam chaves assimétricas, têm-se o RSA (o mais conhecido) e o Diffie-Hellman:

- **RSA** (*Rivest, Shamir and Adleman*): criado em 1977 por Ron Rivest, Adi Shamir e Len Adleman nos laboratórios do MIT (*Massachusetts Institute of Technology*) Dois números primos são multiplicados para se obter um terceiro valor. Porém, descobrir os dois primeiros números a partir do terceiro (fatoração) é complexo. Se dois números primos de grande valor forem usados na multiplicação, será necessário forte processamento para descobri-los, tornando essa tarefa praticamente inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido;
- **ElGamal:** criado por Taher ElGamal, esse algoritmo faz uso de um problema matemático conhecido por "logaritmo discreto" para se tornar seguro. Sua utilização é frequente em assinaturas digitais.

Existem ainda outros algoritmos de chave assimétrica, tais como o DSA (*Digital Signature Algorithm*), o Schnorr (praticamente usado apenas em assinaturas digitais) e Diffie-Hellman.
A chave pública, como o próprio nome diz, é de conhecimento público e é divulgada em diversas maneiras. Com a chave pública é possível prover os serviços de confidencialidade, autenticação e distribuição de chaves. A garantia da confidencialidade é que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede. Já a autenticação é a garantia de identificação das pessoas ou organizações envolvidas na comunicação.
Em um sistema de chave assimétrica (Figura 4) cada pessoa tem duas chaves: uma chave pública que pode ser divulgada e outra privada que deve ser mantida em segredo. Mensagens cifradas com a chave pública só podem ser decifradas com a chave secreta e vice-versa. Se duas pessoas quiserem se comunicar secretamente usando a criptografia com chave assimétrica, elas terão de fazer o seguinte:

- O emissor escreve uma mensagem e a criptografa utilizando a chave pública do receptor. Essa chave está disponível para qualquer pessoa;
- O emissor envia a mensagem através de um meio qualquer, por exemplo, a Internet, para o receptor;
- O receptor recebe a mensagem e a decriptografa utilizando a chave privada que só ele conhece;

- O receptor lê a mensagem e se quiser responder ao emissor deverá fazer o mesmo procedimento anterior com a diferença de que dessa vez a chave pública do emissor é que será utilizada.

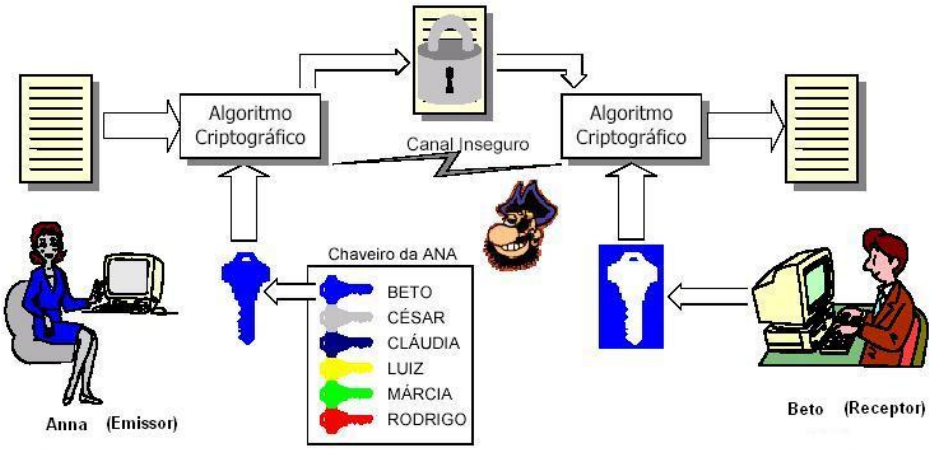

Figura 4 - Exemplo de chave assimétrica

Como apenas o receptor da mensagem tem acesso a sua chave privada, somente ele pode decifrar a mensagem. A grande vantagem é que não só emissor pode enviar mensagens criptografadas para o receptor, mas qualquer pessoa, bastando conhecer a chave pública do receptor, além disto, emissor e receptor não precisam combinar chaves antecipadamente.
Pode-se também criar uma assinatura digital com chaves assimétricas. Para isso basta inverter o processo: o emissor criptografa a mensagem com sua própria chave privada e envia ao receptor. Para decriptografar deve-se usar a chave pública de emissor. Agora qualquer pessoa pode ler a mensagem, mas tem-se a certeza de foi o emissor que a enviou (acreditando-se que somente ele conhece sua chave privada).

1.4. Objetivos da Criptografia

A criptografia computacional protege o sistema quanto à ameaça de perda de confiabilidade, integridade ou não repudio, é utilizada para garantir:

- **Sigilo**: somente os usuários autorizados têm acesso à informação;
- **Integridade:** garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.
- **Autenticação do usuário**: é o processo que permite ao sistema verificar se a pessoa com quem se está comunicando é de fato a pessoa que alega ser.
- **Autenticação de remetente:** é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem.
- **Autenticação do destinatário:** consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.

- **Autenticação de atualidade:** consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

Entretanto, não adianta imaginar que a criptografia irá solucionar todos os problemas de segurança de uma rede de comunicação. Existem variáveis que, por melhor que sejam os processos de criptografia, não se consegue proteger:

- A criptografia não impede um atacante de apagar a informação;
- Um atacante pode comprometer o programa de criptografia modificando o algoritmo para usar uma chave diferente ou gravar as chaves em arquivo para análise posterior;
- Um atacante pode encontrar uma forma de decriptografar a mensagem dependendo do algoritmo utilizado;
- Um atacante pode acessar os arquivos antes de serem criptografados ou após a decriptação.

Por tudo isso, a criptografia deve fazer parte da estratégia de segurança computacional, mas não deve ser a única técnica de segurança.

2. Esteganografia

A palavra esteganografia vem do grego e significa "escrita coberta". Trata-se de um ramo particular da criptografia que consiste, não em fazer com que uma mensagem seja ininteligível, mas em camuflá-la, mascarando a sua presença. A esteganografia não é algo novo, muitas técnicas são conhecidas há milhares de anos. Na Grécia Antiga, por exemplo, tabletes de madeira cobertos com cera eram utilizados para escrita e comunicação - as informações eram escritas na cera, e quando elas não eram mais necessárias, a cera era derretida e uma nova camada era colocada sobre a madeira. Para esconder mensagens, utilizava-se um método que consistia em escrever essas mensagens na madeira e, uma vez que a madeira fosse coberta por uma camada de cera, não seria possível saber da existência de tais mensagens. Algumas formas de esteganografia:

- **Marcação de caracteres**: utilização de uma tinta com composto diferente que ao ser colocada frente à luz faz com que os caracteres fiquem de forma diferente, compondo a mensagem secreta;
- **Tinta invisível:** pode-se utilizar uma tinta invisível para a escrita da mensagem em cima de outra pré-existente, aonde, somente com produtos químicos poderíamos obter o conteúdo;
- **Bits não significativos:** A moderna esteganografia utiliza o uso de bits não significativos que são concatenados a mensagem original e faz uso também de área não usada.

Por exemplo, utilizando-se a técnica do bit menos significativo onde, em uma imagem JPEG, pode-se mudar a intensidade de um pixel em no máximo 1%.

Isto faz com que a imagem fica praticamente inalterada, principalmente no que diz respeito à percepção visual do ser humano (Figura 5).

Figura 5 - Exemplo de esteganografia por bits não significativos

Além de imagens, arquivos de áudio também podem ser usados para ocultar mensagens, de maneira que estas não sejam percebidas por quem estiver ouvindo o som. Outros métodos usam também arquivos de texto, arquivos HTML e pacotes TCP para esconder informações.

3. Criptografia e Esteganografia

Os dois métodos podem ser combinados para aumento da segurança da informação. Por exemplo, pode-se criptografar uma mensagem e em seguida, utilizar a técnica de esteganografia, trocando-se os bits menos significativos de uma imagem digitalizada pelos bits da mensagem criptografada, e então anexar a imagem. Se a imagem for interceptada, primeiro será necessário descobrir a mensagem oculta entre os bits da imagem, e, somente após isso, poderá ocorrer a tentativa de decriptografia. Outro campo para aplicação dos dois métodos é na confecção de documentos legais como carteiras de identidade, passaportes, carteiras de motorista (Figura 6)

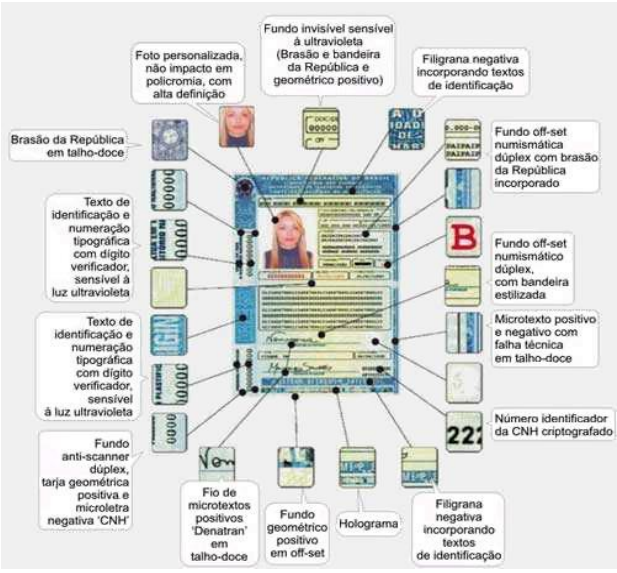

Figura 6 - Aplicação de Criptografia e Esteganografia

CENTRO UNIVERSITÁRIO DE BARRA MANSA

Questionário

1. Por que utilizar a criptografia em redes de computadores?
2. Qual a diferença entre “texto limpo” e “texto cifrado”?
3. O que é PKI e qual a sua importância?
4. Descreva o processo criptográfico.
5. Quais os tipos básicos de criptografia?
6. Em que consiste a “chave” criptográfica?
7. Qual a diferença entre os algoritmos de criptografia e decriptografia no sistema de chave simétrica?
8. A chave de criptografia pública é encontrada em qual sistema criptográfico?
9. Cite três objetivos da criptografia.
10. O que é Esteganografia? Como ela pode ser usada por hackers?