Fundação Oswaldo Aranha - FOA
Centro Universitário de Volta Redonda – UniFOA

Campus Universitário Olezio Galotti – Avenida Paulo Erlei Alves Abrantes, 1325
Três Poços – Volta Redonda RJ – Tel: (24) 3340-8400 – www.unifoa.edu.br

Curso Tecnológico de Redes de Computadores
Disciplina: Segurança da Informação
Professor: José Maurício S. Pinheiro **V.01/08**

AULA 4: Criptografia e Esteganografia

Criptografia

A forma mais utilizada para prover a segurança em pontos vulneráveis de uma rede de computadores é a utilização da criptografia. A criptografia é utilizada para barrar as ameaças e os ataques.

A palavra tem origem grega (kriptos = escondido, oculto e grifo = grafia) e define a arte ou ciência de escrever em cifras ou em códigos (Figura 1), 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.

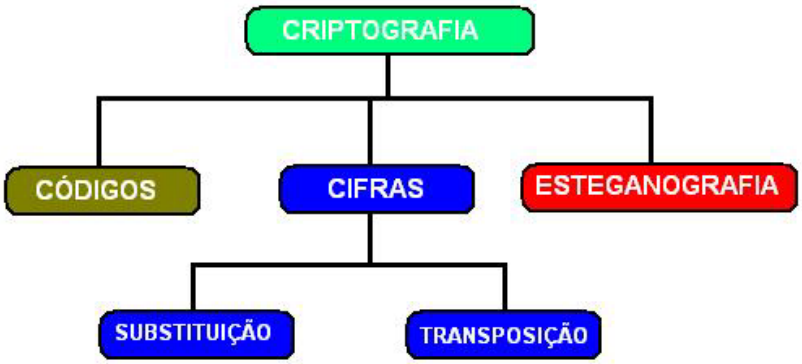

Figura 1 - Criptografia

A criptografia fornece técnicas para codificar e decodificar dados, tais que os mesmos possam ser armazenados, transmitidos e recuperados sem sua alteração ou exposição. Em outras palavras, as técnicas de criptografia podem ser usadas como um meio efetivo de proteção de informações suscetíveis a ataques, estejam elas armazenadas em um computador ou sendo transmitidas pela rede.

A RFC 2828 (Request for Coments nº 2828) define o termo criptografia como a ciência matemática que lida com a transformação de dados para mudar seu significado em algo ininteligível para o inimigo, isto é, esconder seu conteúdo semântico prevenindo sua alteração ou o seu uso sem autorização.

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 dado transmitido, desde um e-mail até um arquivo com dados confidenciais. Também pode ser usada para proteger dados armazenados onde a segurança física é de difícil

implementação ou impossível. Pode-se citar o exemplo dos *laptops*, que, ao serem deixados em um quarto de hotel, poderiam ter as tuas informações lidas 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.

5.1. 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.

Na criptografia simétrica os usuários envolvidos devem ter prévio conhecimento da chave (senha). Isto a torna muito vulnerável a falhas de segurança. Na criptografia assimétrica existem duas chaves relacionadas entre si. Qualquer texto encriptado com uma delas somente poderá ser decriptografado com a outra.

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.

A criptografia utiliza conceitos matemáticos para a construção de seus algoritmos. Assim, um texto cifrado pode ser representado da seguinte maneira:

Y = EK(X), ou seja, um texto plano (X) é encriptado por um algoritmo que contém uma chave (senha) K;

X = DK(Y), para a obtenção do texto plano inicial, deve-se submeter o texto cifrado (Y) ao mesmo algoritmo e a mesma chave (K).

Sistema de chave simétrica

A criptografia por chave simétrica (ou chave privada) é utilizada para prover a segurança das informações (Figura 2). 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 descriptografia 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 já estão disponíveis resultando em maior segurança.

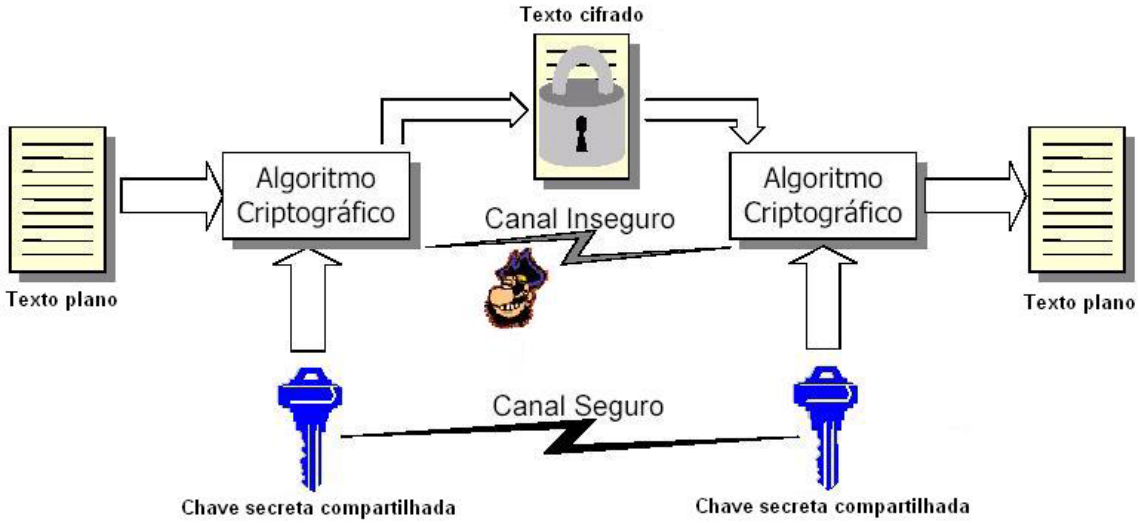

Figura 2 - Exemplo de chave simétrica

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.

Sistema de chave assimétrica

A criptografia por chave assimétrica (ou chave pública) utiliza um par de chaves, sendo uma chave 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.

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.

Esse sistema tem como principal padrão o RSA. As chaves são criadas através de operações matemáticas de tal forma que, apesar de serem relacionadas, é virtualmente impossível adivinhar a outra, tendo apenas uma delas.

Em um sistema de chave assimétrica (Figura 3) 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 descriptografa 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.

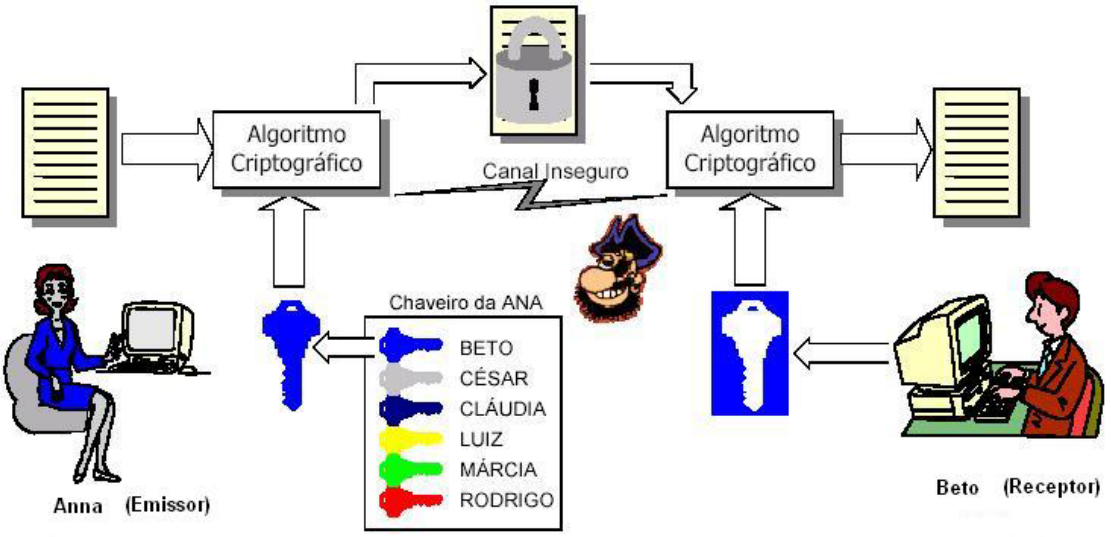

Figura 3 - Exemplo de chave assimétrica

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).

Objetivos da Criptografia

A criptografia computacional protege o sistema quanto à ameaça de perda de confiabilidade, integridade ou não repudiação, 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.

O que a criptografia não protege

Não adianta imaginarmos que a criptografia irá solucionar todos os nossos problemas de segurança. Existem coisas que por melhor que sejam os processos de criptografia, não conseguiremos proteger:

- A criptografia não impede um atacante de apagar todos os seus dados.
- Um atacante pode comprometer o programa de criptografia modificando o programa 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 sua estratégia de segurança, mas não deve ser a substituta de outras técnicas de segurança.

Tabela 1 - Comparações entre chave privada e chave pública

CHAVE PRIVADA	CHAVE PÚBLICA
Um algoritmo e uma chave	Um algoritmo e duas chaves
Os usuários compartilham o algoritmo e a chave	Os usuários compartilham um par de chaves
Chave secreta	Apenas uma das chaves é secreta
Impossibilidade de decifrar a mensagem	Impossibilidade de decifrar a mensagem
O algoritmo e as amostras do texto cifrado não devem ser suficientes para determinar a chave	O algoritmo, as amostras do texto cifrado e uma das chaves não devem ser suficientes para determinar a outra chave.

5.2. 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 (Figura 4). Por exemplo, uma seqüência de letras de cada palavra pode formar a palavra de uma mensagem escondida.

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.

Figura 4 - Exemplo de esteganografia por bits não significativos

Os dois métodos (criptografia e esteganografia) podem ser combinados para aumento da segurança. 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 transmitir 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 descriptografia.

Questionário

1. Por que utilizar a criptografia em redes de computadores?
2. Qual a diferença entre “texto limpo” e “texto cifrado”?
3. Qual a definição da RFC 2828 para criptografia?
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 descriptografia 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?