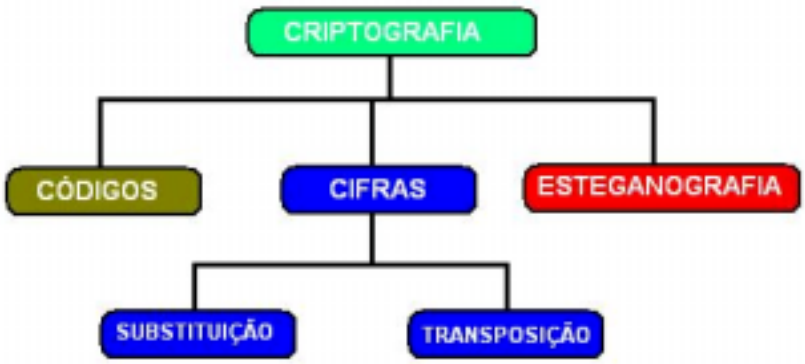
Criptografia

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 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 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 as mensagens incompreensíveis, chamadas 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.

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.

Como Funciona

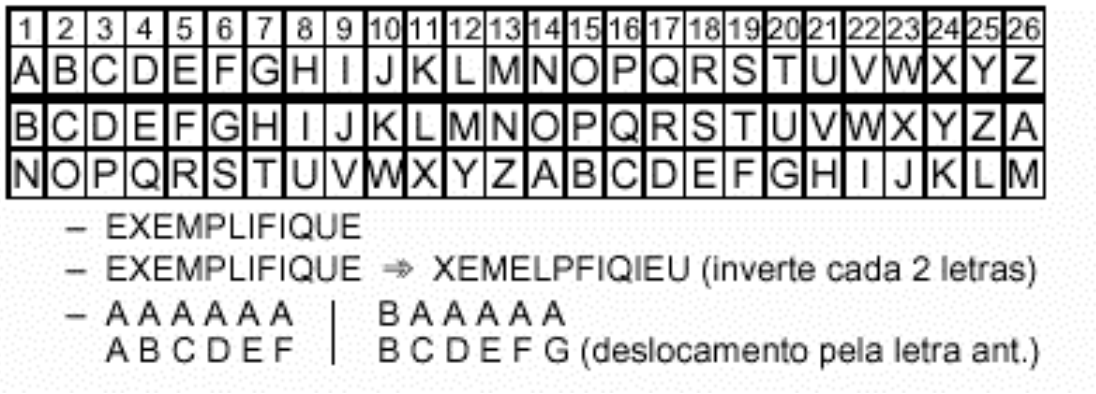
O processo de criptografia consiste em transformar um texto simples, através de uma função parametrizada por uma chave (senha)**,** em um texto inteligível. A saída desse processo de criptografia é chamada texto cifrado ou criptograma. Após o processo de criptografia, o texto é então transmitido ao destinatário. 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.

Os métodos de criptografia podem ser divididos em duas categorias:

- **Cifra de substituição** - cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, a fim de ocultá-la. Por exemplo, pode-se definir que para um texto ser cifrado, as letras que compõe cada palavra desse texto devem ser deslocadas em *k* letras. Nesse caso, *k* torna-se uma chave para o método de criptografia.

- **Cifra de transposição** - as letras são reordenadas mas não ocultas. A cifra é chaveada por uma palavra ou frase que não contém quaisquer letras repetidas.



Tipos de Criptografia

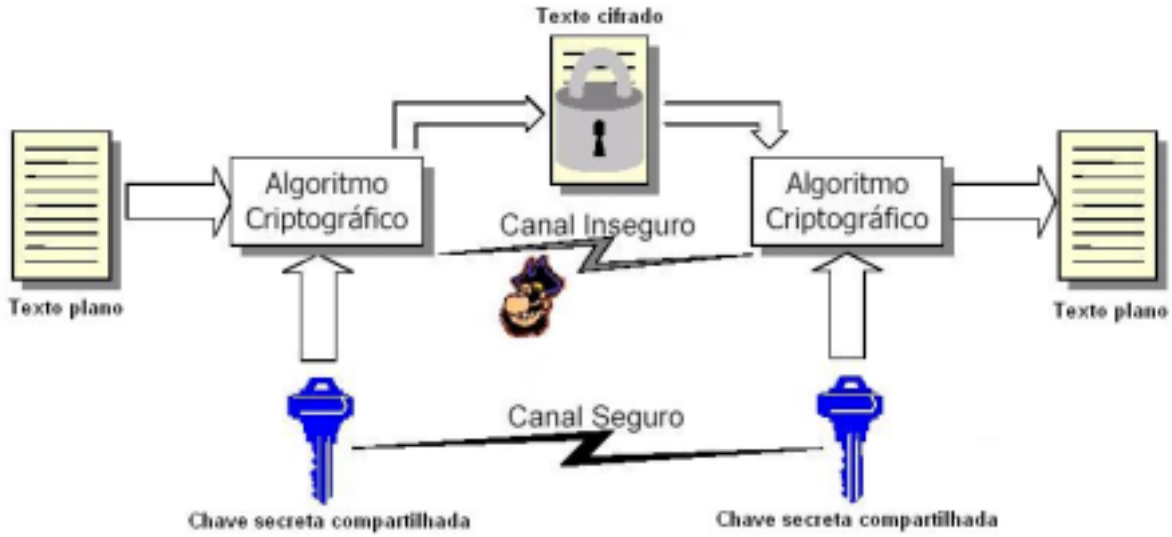
A criptografia é um mecanismo de segurança que permite a implementação de diversos serviços (autenticação, não-repúdio, integridade, confidencialidade). Para tanto existem dois tipos básicos de criptografia: simétrica e assimétrica. Na criptografia simétrica os usuários envolvidos devem ter prévio conhecimento 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 decriptado 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 adivinhar a outra, tendo apenas uma delas.

Sistema de chave simétrica

A criptografia por chave simétrica (ou chave privada) é utilizada para prover a segurança das informações. 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.



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 tamanho da chave é muito importante para a segurança dos algoritmos simétricos. Uma chave de "40 bits de tamanho" significa que existem 240 chaves possíveis. Por exemplo, uma chave de 40 bits pode ser quebrada em 12 minutos, e uma chave de 56 bits em 556 dias. Deve-se observar que 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.

A chave pública, como o próprio nome diz, é de conhecimento público e é divulgada em diversas maneiras. O que for encriptado utilizando uma das chaves somente poderá ser visualizado com a outra.

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 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:

1. O emissor escreve uma mensagem e a criptografa utilizando a chave pública do receptor. Essa chave está disponível para qualquer pessoa;

2. O emissor envia a mensagem através de um meio qualquer, por exemplo, a Internet, para o receptor;

3. O receptor recebe a mensagem e a descriptografa utilizando a chave privada que só ele conhece;

4. 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 1 - 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, basta conhecer a chave pública do receptor, além disto, emissor e receptor não precisam combinar chaves antecipadamente.

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

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. Por exemplo, uma seqüência de letras de cada palavra pode formar a palavra de uma mensagem escondida.

Algumas formas de esteganografia são:

- **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.

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.