Introdução a Segurança da Informação – Parte 6

13 de abril de 2015 / maximoz

Criptografia

A criptografia desempenha um papel importante em proteger informações de caírem em mãos erradas atraúes de codificação de texto simples em forma não legível ou texto cifrado. O remetente encripta a informação usando um algoritmo criptográfico antes de transmití-lo na internet. O receptor, na outra extremidade, usa chaves de decifração para trazer a informação para sua forma original de texto simples. Isso garante que os dados sejam decifrados em trânsito.

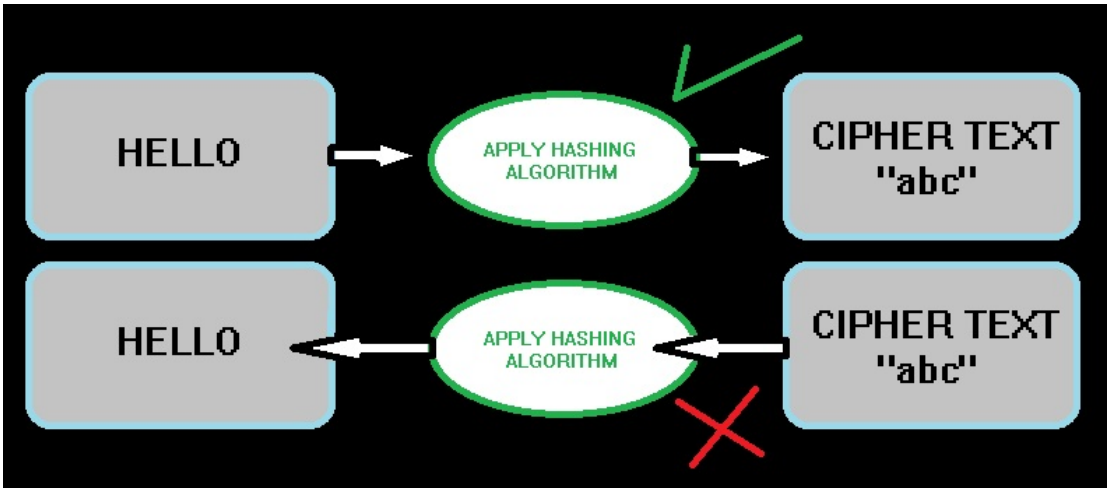
Esses são os três principais algoritmos criptográficos:

Algoritmo Hashing

Esse algoritmo é usado principalmente para criptografar e descriptografar as assinaturas digitais e senhas. Uma mensagem de comprimento variável é convertida para uma função de hash. Podem haver dois tipos de algoritmos hashing:

Unidirecional

O algoritmo de hash unidirecional é também conhecido como função de hash criptográfico (message digest). Ele executa uma forma de criptografia e não permite a mensagem ser decodificada e o texto original não pode ser determinado baseado na hash. A figura a seguir mostra que aqueles texto “Hello” convertido ao texto cifra “abc” não pode ser convertido de volta ao texto “Hello.”



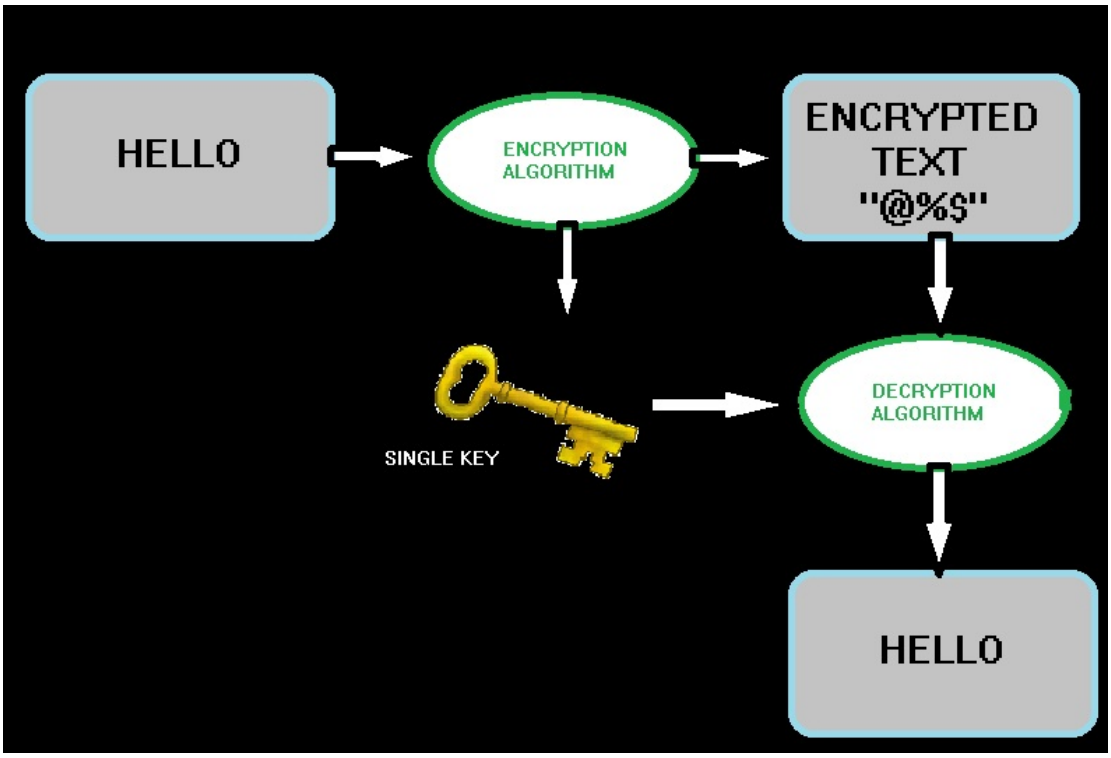
A única forma de checar o valor é verificar a hash. Então, para saber o valor, a senha digitada é comparada a uma hash armazenada em uma rede ou banco de dados.

Bidirecional

O algortimo de hash bidirecional permite a mensagem ser reconstruída a partir de hash. O Hashing permite você determinar a integridade de um determinado bit de dados. Mesmo se um valor pequeno da hash é modificado, você saberá que os dados foram mudados. Os dois principais padrões de criptografia são SHA (Secure Hash Algorithm) e MDA (Message Digest Algorithm) ou MD5 (Message-Digest Algorithm 5), ambos são formas de algoritmos de hash.

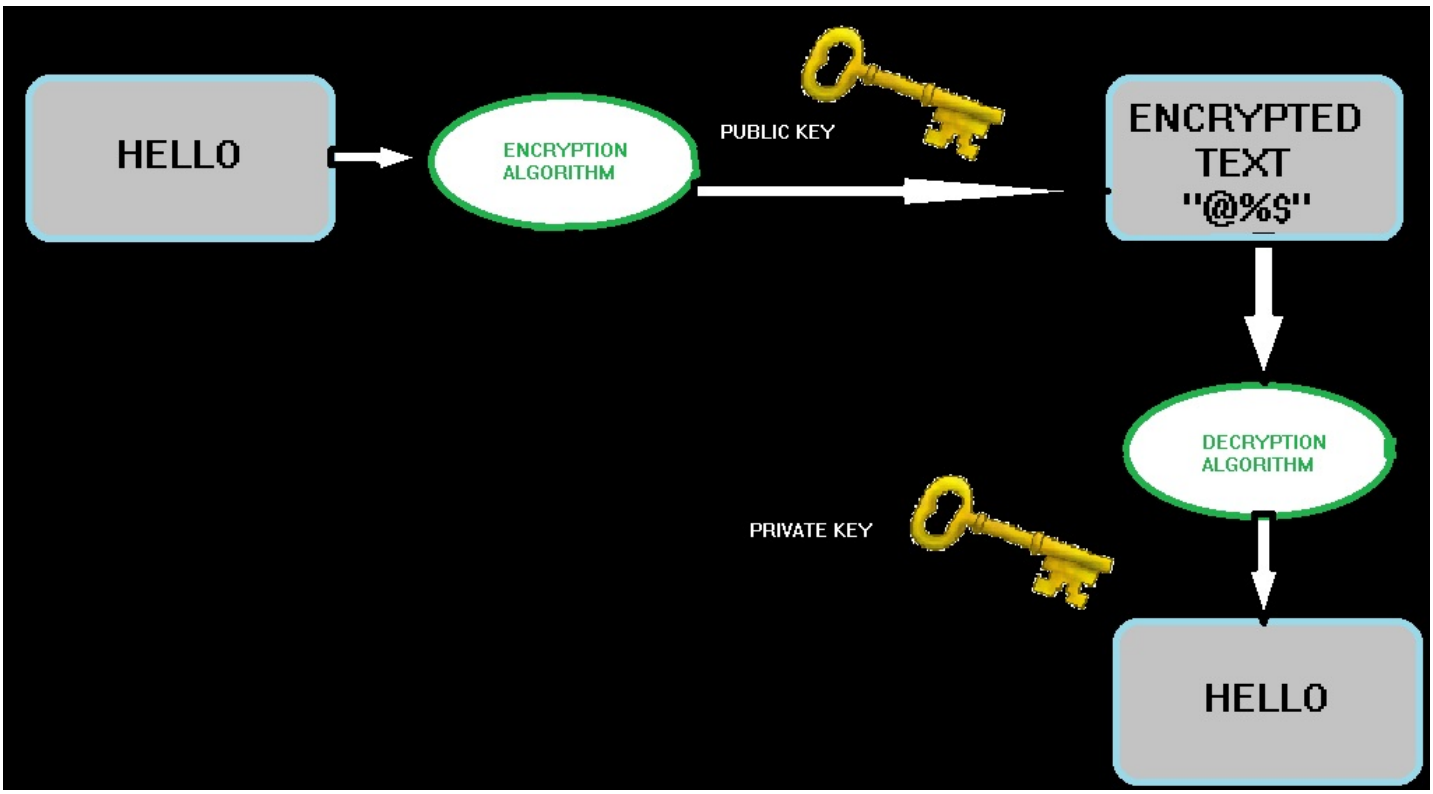
Algoritmo Simétrico

Algortimos de chave simétrica usam uma única chave criptográfica para encriptar e desencriptar. A chave também é chamada de chave compartilhada porque ela é compartilhada entre duas ou mais entidades que precisam para criptografar ou descriptografar a informação. A chave secreta também é conhecida como a chave privada. Apesar de este tipo de algoritmo ser muito mais rápido, a chave compartilhada é considerada uma desvantagem porque é preciso ser compartilhada. Além disso, se chave for perdida, todo o processo falha.



Algoritmo Assimétrico

Algoritmos de chave assimétrica são mais seguros mas lentos comparados ao algoritmo de chave simétrica. Eles usam diferentes chaves para criptografia e descriptografia. Essas chaves são chamadas de chaves públicas e chaves privadas, como mostrado na figura 2. A chave pública é usada para criptografar a mensagem e a chave privada para descriptografar a mesma. A chave pública é compartilhada entre duas ou mais entidades mas a privada é somente de conhecimento do receptor.



Próximo capítulo >>>

Traduzido e adaptado por: Maximoz Sec
Artigo original: http://learnthat.com/introduction-to-network-security/