Criptografia

Conceitos

A criptografia vem do latim (*cryptos* = secreto e *grafia* = escrita) é a arte de transformar informações de forma que a mensagem fique ilegível.

A criptografia pode ser classificada de várias formas e sobre vários aspectos, sendo que as principais são:

- hardware: quando a criptografia é implementada em circuitos eletrônicos, mais rápida porém mais difícil de ser implementada do que a de software;
- software: quando a criptografia é um código de computador, mais lenta que a de hardware, porém mais fácil de ser implementada. Praticamente todos os algoritmos de criptografia são de software;
- fluxo: quando o algoritmo converte me cifra bit a bit a mensagem;
- bloco: quando o algoritmo converte a mensagem a cada bloco de bits (8, 16, 32 e etc.);
- simétrica: quando a chave usada para criptografar é a mesma usada para descriptografar;
- assimétrica: quando a chave usada para criptografar é uma (chave pública) e a chave para descriptografar é outra (chave privada).

Criptografia simétrica

A criptografia (Figura 1) converte o “texto limpo” (mensagem legível) em “texto cifrado” (mensagem ilegível) utilizando um determinada técnica utilizando como elemento principal a chave.

Figura 1. Criptografia de texto limpo em texto cifrado com uso de chave.

A descriptografia (Figura 2), portanto, é o processo reverso ao da criptografia, que permite que o texto cifrado (não legível) seja convertido em texto limpo (legível) utilizando chave, portanto, a criptografia é uma técnica reversível, já que permite que se retorne ao processo inicial para obtenção do texto limpo.

Figura 2. Descriptografia de texto cifrado em texto limpo com uso de chave.

Algoritmos de criptografia simétrica

Os principais algoritmos de criptografia simétrica, suas características e especificações técnicas estão descritas a seguir.

DES (56 bits)

O Data Encryption Standard (DES) foi um dos principais algoritmos simétricos utilizados no mundo, até que o algoritmo DES se tornasse o padrão.

Foi desenvolvido em 1917 pela IBM. Apesar de possibilitar a geração de cerca de 72 quadrilhões de combinações, seu tamanho de chave padrão de 56 bits é considerado fraco atualmente, sendo quebrado por brute force em 1997 em poucas horas.

A agência estadunidense National Institute of Standards and Technology (NIST) fez duas atualizações posteriormente, com o 2DES, ou duplo DES, em que o DES é aplicado duas vezes (2x), e finalmente, em 1993, a última versão, o 3DES (112 ou 168 bits), ou triplo DES, em que o DES é aplicado três vezes (3x), ainda recomendado para uso.

AES (128 bits)

O Advanced Encryption Standard (AES) é um algoritmo de criptografia de bloco, adaptado em 2003 pelo National Institute of Standards and Technology (NIST) como algoritmo padrão para uso do governos dos EUA para criptografia segura de dados. Foi então, a partir de um concurso realizado entre várias empresas, escolhido como padrão para uso geral em substituição ao DES, já considerado inseguro.

O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.

O AES é rápido é um algoritmo que pode ser implementado tanto em software quanto em hardware e rápido em ambos. Outra característica do AES é a facilidade na execução e uso de pouca memória, por isso é utilizado na maioria dos sistemas criptográficos comerciais, como por exemplo, equipamentos de interconexão wireless Access Point.

IDEA (128 bits)

O International Data Encryption Algorithm (IDEA) foi desenvolvido pelos criptógrafos por James Massey e Xuejia Lai em 1991, registrado com patente da suíça ASCOM Systec e recomendado para uso em países europeus (União Europeia).

O IDEA utiliza o modelo de estrutura do DES, mas sua implementação o torna um algoritmo mais rápido que o DES.

O IDEA é utilizado principalmente no mercado financeiro e associado ao PGP, algoritmo de criptografia assimétrica muito utilizado principalmente em e-mails pessoais.

BlowFish (32 a 448 bits)

Algoritmo desenvolvido por Bruce Schneier, a cifra oferece solução tanto para escolha de maior segurança ou então maior desempenho através da utilização de chaves de tamanho variável.

TwoFish (128 bits)

O Twofish é uma implementação do BlowFish e é um algoritmo de chave simétrica que utiliza a criptografia de cifra de bloco de 128 bits. O Twofish não possui registro e ou patente, portanto, está disponível como domínio público e acessível a todos para uso sem restrição.

Também permite a utilização de chaves de tamanhos variáveis, sendo as principais a de 128 a 256 bits. O TwoFish permite realizar 16 interações durante a criptografia, no entanto, é um algoritmo muito rápido.

RC2 (8 a 1024 bits)

Foi desenvolvido pelo famoso criptógrafo Ron Rivest (o R da cifra criada pela empresa RSA Data Security Inc.). É utilizado como padrão no S/MIME, protocolo utilizado na criptografia de e-mail. Também possui chave de tamanho variável. Rivest desenvolveu as variações do RC2 que são: RC4, RC5 e RC6.

CAST (128 bits)

Desenvolvido em 1996 por Carlisle Adams e Stafford Tavares, o CAST é um algoritmo de cifra de bloco. Sua estrutura é a do algoritmo de Feistel, utilizado em muitos algoritmos de criptografia simétrica.

O CAST permite de 12 a 16 iterações na etapa principal, com tamanho de bloco de 64 bits e chave de tamanho variável de 40 a 128 bits, que permite acréscimos de 8 bits, assim, os 16 rounds de iteração são usados quando a chave tem comprimento maior que 80 bits.