CRIPTOGRAFIA

I. O que é criptografia?

É uma forma de proteger os dados de alguma informação embaralhando os caracteres por uma função algorítmica ou chave criptográfica, de modo que apenas as partes que possuam as chaves possam ler o que está escrito.

II. Como funciona a criptografia?

A criptografia codifica o texto desejado para um novo texto criptografado. Este texto será enviado, e precisará ser decodificado utilizando um algoritmo/chave de descriptografia (a mesma utilizada para descriptografar. Como existem infinitas formas de criptografar um texto, pessoas indesejadas não terão como saber qual chave foi utilizada.

III. Tipos de chaves.

Os dois tipos mais comuns de chaves utilizados na criptografia são:

- **Chave simétrica:** usa a mesma chave para criptografia e descriptografia. As criptografias de chave simétrica são consideradas mais baratas para produzir e não usam tanta força de computação para conversão, o que significa que há menos atraso na decodificação dos dados. A desvantagem é que se uma pessoa não autorizada colocar as mãos na chave pode-se descriptografar todas as mensagens e dados enviados entre as partes. Por isso, a transferência da chave compartilhada precisa ser criptografada com uma chave criptográfica diferente.

- **Chave assimétrica:** usa duas chaves separadas para criptografar e descriptografar dados. Uma é uma chave pública compartilhada entre todas as partes para criptografia. Qualquer pessoa com a chave pública pode enviar uma mensagem criptografada, mas apenas os detentores da segunda chave privada poderão descriptografá-la. A criptografia assimétrica é considerada mais cara para ser produzida e precisa de mais capacidade computacional para descriptografar, já que a chave pública costuma ser grande, entre 1.024 e 2.048 bits. Por isso, a criptografia assimétrica muitas vezes não é adequada para grandes pacotes de dados.

IV. Algoritmos comuns utilizados.

- **Advanced Encryption Standard (AES):** é um algoritmo de criptografia de chave simétrica usado para proteger dados. Ele criptografa os dados em blocos de 128 bits, utilizando chaves de 128, 192 ou 256 bits. É amplamente adotado como padrão para criptografia de dados eletrônicos e é considerado seguro contra todos os ataques conhecidos.

- **RSA:** é uma forma original de criptografia assimétrica. A chave pública é criada fatorando dois números primos mais um valor auxiliar. Qualquer pessoa pode usar a chave pública RSA para criptografar dados, mas apenas uma pessoa que saiba os números primos pode descriptografar os dados. As chaves RSA podem ser muito grandes (2.048 ou 4.096 bits são tamanhos típicos) e, portanto, são consideradas caras e lentas.