Criptografia

A criptografia é um conceito técnico usado para codificar uma determinada informação, de tal forma que somente o seu destinatário e o emissor da mensagem consigam acessá-la. O objetivo é evitar que terceiros interceptem e desvendem o código.

Na atualidade, as técnicas de criptografias mais conhecidas envolvem o conceito das chaves criptográficas, que são formadas por bits, com base em algarismos com capacidade de interpretar as informações, isto é, capaz de decodificar. A chave do emissor deve ser compatível com a do receptor, para assim, as informações serem extraídas com êxito.

Existem dois tipos de chaves: as públicas e privadas. Cada uma com sua especificação e objetivo dentro do sistema de criptografia. A chave pública é usada para codificar determinadas informações e a privada para decodificar as informações anteriores.

A chave pública todos conseguem ter acesso a um determinado conteúdo, porém para se conseguir os dados com as informações, é preciso a chave privada, que apenas o emissor e o receptor possuem. A criptografia é considerada um método 99 % seguro, isso significa que

quem utiliza esse processo para envio de e-mails, por exemplo, está bem protegido de fraudes.

A segurança depende da quantidade de bits, quanto mais bits, maior será a segurança criptográfica. Para se referir à segurança, usam-se os termos 64 ou 128 bits para expressar o tamanho da chave, que enquanto maior mais segura.

Um algoritmo de oito bits, por exemplo, possui 256 combinações de chaves, que é o resultado de 2 elevados a 8. Assim, se alguém tentar gerar 256 combinações, para decodificar a mensagem, embora seja complicado, é possível. Por isso, quanto maior o número de bits, maior a segurança, que ainda tem as do tipo simétricas e a assimétricas.

Além disso, a criptografia simétrica é um tipo de chave simples, usada para codificação e decodificação. E entre os algoritmos que usam essas chaves, estão: DES (Data Encryption Standard): usa 56 bits, que corresponde a cerca de 72 quatrilhões de combinações.

Embora o número seja inalcançável, em 1997, em um desafio de internet conseguiram quebrar o algoritmo, pelo método de tentativa e erro. RC (Ron's Code ou Rivest Cipher): é mais utilizado em e-mails, usa chaves

entre oito e 1024 bits. Possui várias versões, que se definem pelo tamanho das chaves. EAS (Advanced Encryption Standard): é um dos mais populares algoritmos de criptografia da atualidade. O tamanho de sua chave varia entre 128, 192 ou 256 bits. IDEA (International Data Encryption Algorithm): Parecido com a DES, seu ponto forte é a fácil implementação no software. Utiliza a chave de transição de 128 bits. Pelo fato do emissor e receptor terem o conhecimento da mesma chave, as criptografias simétricas não são muito seguras, quando se trata de informações muito valiosas.

Agora, a criptografia assimétrica utiliza as duas chaves: pública e privada. A pública codifica; a privada decodifica. E utiliza os seguintes algoritmos: RSA (Rivest, Shamir and Adleman): é um dos assimétricos mais usados. Aqui se usa dois números primos (números que só são divididos por um e por ele mesmo) que são multiplicados, para se obter um terceiro valor.

Assim, é preciso fazer a fatoração, para descobrir os dois primeiros números a partir de um terceiro. Se números grandes forem utilizados, é praticamente impossível descobrir o código. Assim as chaves privadas são os números multiplicados; a pública, o valor obtido. "ElGamal" – Por se usar logaritmo discreto é ainda mais seguro, sendo assim, muito utilizado em assinaturas digitais.

Por último, a segurança dos serviços de internet é muito importante. Para garantir que tudo funcione dentro dos mais seguros sistemas, é fundamental a escolha correta de um bom serviço Hospedagem de Sites.

Ficou interessado?

atendimento@blenneros.net