Criptografia e Certificação Digital

**- Principais técnicas de criptografia.**

**DES - Data Encryption Standard** é um dos primeiros modelos a serem criados(1977) por isso é um dos mais difundidos mundialmente, além disso é também um dos modelos mais básicos fornecendo proteção também básica de aproximadamente blocos de 56 bits, oferecendo até 72 quatrilhões de combinações e realiza 16 ciclos de codificações para proteger uma informação.

O DES pode ser decifrado com a técnica de “força bruta”, onde um programa testa todas as possibilidades de chaves de forma automatizada pelo tempo que for necessário.

**AES -** **Advanced Encryption Standard** é um dos algoritmos de criptografia mais seguros da atualidade, tão seguro que é usado pelo governo dos estados Unidos e várias outras organizações; muito eficiente e confiante, fornece proteção em blocos de 128 bits, mas também é possível utilizar chaves de 192 e 256 bits para informações que necessitem de uma maior segurança.

O AES é considerado totalmente imune a todos os tipos de ataques, exceto aos ataques utilizando a técnica “força bruta”, onde um programa testa todas as possibilidades de chaves(sejam em 128, 192 ou 256 bits) de forma automatizada pelo tempo que for necessário, mas apesar de poder acontecer é muito difícil na atualidade.

**SAFER** – **Secure and Fast Encryption** é uma criptografia de blocos em 64 bits, o que origina o nome pelo qual é conhecido “SAFER SK-64” mas encontram-se diversas falhas e então em decorrência disso foram desenvolvidas as novas opções SK-40 e SK-128 bits que são versões mais complexas.

OBS. Quanto maior o número de Bits maior é a proteção.

**- Tipos de certificados digitais existentes, e quais mídias criptográficas são utilizadas.**

**Certificado tipo A – *Assinatura Digital*** é o mais popular e utilizado dos certificados digitais, seu principal benefício é realizar assinaturas digitais, identificando o titular, atestando a autenticidade da operação e confirmando a integridade do documento assinado sendo assim tem validade jurídica. É de uso flexível já que pode ser efetuada cópias de segurança e ser instalada em diversos computadores.

* A1 - A1 é emitido diretamente no computador, pode ser armazenado em seu navegador de internet ou na nuvem, este tipo de certificado possibilita que seja feita **cópias de segurança** e posteriormente a instalação em outros computadores. Pode ser acessado de qualquer dispositivo, de qualquer lugar do mundo, com total segurança e com muita praticidade. E tem validade de 1 ano.
* A3 - A3 pode ser **armazenado em um dispositivo criptográfico**, que pode ser um cartão inteligente (necessita de uma leitora), token, e agora, também na nuvem, ambos protegidos por senha e uma alta camada de criptografia. E tem validade podendo variar de 1 até 5 anos.

**Certificado tipo S** – ***Certificado de Sigilo*** é utilizado para garantir o sigilo de transações, pois por meio dele é possível criptografar dados de um documento que só poderá ser acessado por meio de um certificado de autorização, sendo assim, evitando vazamento desses dados criptografados, assegurando as informações ali contidas.

**Certificado tipo T** - ***Certificado de Sigilo tipo T*** é mais conhecido como carimbo de tempo, por ser como um selo, que atesta a existência de um documento eletrônico ou assinatura digital em uma determinada data ou hora para comprovação de veracidade pois como esses dados poderiam facilmente serem manipulados para beneficiar uma das partes, então a terceira parte é utilizada para atestar as informações e evitar fraudes.

**Certificado tipo A CF-e-SAT** - ***Certificado tipo A CF-e-SAT*** só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico – SAT-CF-e, seguindo a regulamentação do CONFAZ.

**Certificado tipo OM-BR - Certificado do tipo Objeto Metrológico** - ***Certificados do tipo Objeto Metrológico-OM-BR*** só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro.

**e-CPF** - O CPF, principal documento de identificação de pessoa física, também tem uma versão digital para garantir a autenticidade das transações eletrônicas realizadas por pessoas físicas funcionando com criptografia de dados, oferecendo segurança, sigilo e integridade de dados. Utiliza-se da mesma tecnologia do certificado A, podendo ser emitido com o tipo A1 ou A3.

**e-CNPJ** – O CNPJ principal identificação de pessoa jurídica no Brasil, também tem uma versão digital que garante a autenticidade e a integridade de transações de empresas no meio eletrônico e por exigência da Receita Federal, apenas o responsável direto pelo CNPJ da empresa poderá responder pelo e-CNPJ. Utiliza-se da mesma tecnologia do certificado A, podendo ser emitido com o tipo A1 ou A3.

**NF-e** - ***NF-e*** é um dos mais importantes quando falamos em certificados digitais para empresas é o NF-e, arquivo que garante a autoria e a validade jurídica das emissões de notas fiscais pela empresa aos órgãos responsáveis. O certificado digital NF-e pode ser atribuído diretamente a um funcionário, sem a necessidade de compartilhar o e-CNPJ da empresa, trazendo mais segurança para a operação.

Ele é utilizado para assinar as notas fiscais eletrônicas emitidas, garantindo, assim, maior segurança contra qualquer tipo de fraude e cumprindo com todas as exigências dos órgãos fiscalizadores. Entre os documentos que podem ser emitidos e assinados com o NF-e, estão:

* NF-e: nota fiscal eletrônica;
* NFA-e: nota fiscal avulsa eletrônica;
* NFC-e: nota fiscal de consumidor eletrônica;
* NFS-e: nota fiscal de serviço eletrônica.