Certificação Digital é um conjunto de assinaturas digitais.

Certificação Digital -> Gera uma Assinatura Digital -> Precisa de Criptografia

Criptografia nada mais é do que embaralhar uma mensagem tornando-a ilegível, visando proteger os dados a quem não tiver a chave de codificação correta.

É uma **ferramenta** fundamental da segurança cibernética, protegendo dados contra ataques como roubo e alteração.

A criptografia é **fundamental** para manter:

- ➔ Confidencialidade: garante que as informações sejam acessadas somente por peoples autorizadas;
- ➔ Integridade garante que os dados não sejam alterados durante a transmissão;
- ➔ Autenticação: permite verificar a identidade de remetentes e destinatários;
- ➔ Não repudio: Evita que remetentes neguem ter enviado uma mensagem ou realizado uma ação;

Exemplos de criptografia

Proteção de senhas;
Comunicação segura;
Transmissão de dados online;
Armazenamento de dados na nuvem;

Existem dois tipos de Criptografias que nada mais é do que a forma que você vai entregar a chave a outrem.
1 – Chave Simétrica
2 – Chave Assimétrica

A CRIPTOGRAFIA SIMÉTRICA também conhecida como chave compartilhada ou algoritmo de chave privada, 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 criptografar e descriptografar, 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, ela pode 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, levando a um ciclo de dependência.

A CRIPTOGRAFIA ASSIMÉTRICA também conhecida como criptografia de chave pública, 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.

ALGORITIMOS DE CRIPTOGRAFIA COMUNS

SIMÉTRICA

DES foi o primeiro sistema de criptografia desenvolvido no início da década de 70. Foi adotado pelos EUA em 1977. O tamanho da chave era de 56 bits, o que o tornou obsoleto no ecossistema de tecnologia atual.

3DES é a evolução do DES, pegou o bloco de criptografia do DES e aplicou 3 vezes a cada bloco de dados. O método aumentou o tamanho da chave, dificultando a descriptografia. No entanto é considerado inseguro e foi descontinuado a partir de 2023.

AES é o método de criptografia mais usado hoje. Foi adotado pelo governo dos EUA em 2001. Foi projetado com base em um princípio chamado de rede se substituição-permutação, que é uma criptografia de blocos de 128 bits e pode ter chaves de 128, 192 ou 256 bits.

Blowfish/Twofish: usado em hardware e software, é considerado o método de criptografia simétrica mais rápido. O Twofish é gratuito, mas não é patenteado nem de código aberto. No entanto, ele é usado em aplicativos de criptografias conhecidos, como a PGP (pretty Good Privacy). Ele pode ter até 256 bits.

ASSIMÉTRICA

RSA é o mais conhecido e muito utilizado para a troca de chaves e assinaturas digitais.

ECC usa curvas elípticas, sendo mais eficiente que RSA em termos de segurança por bit e muito utilizado em dispositivos moveis e aplicações modernas (ex. Bitcoin);

DSA usado para assinaturas digitais, variante moderna da ECDSA (utiliza curvas elípiticas).

HASH CRIPTOGRÁFICO

Não é uma criptografia propriamente dita, mas importante em segurança.
É uma função que transforma uma entrada (como um texto, arquivo ou senha) em uma sequência fixa de caracteres (chamada de hsh, digest ou resumo). Suas principais características são:

- ➔ Determinístico: a mesma entrada sempre gera o mesmo hash;
- ➔ Unidirecional: é praticamente impossível reverte o hash para descobrir a entrada original;
- ➔ Resistente a colisões: é muito difícil encontrar duas entradas diferentes que resultem no mesmo hash;
- ➔ Sensível a mudanças: uma pequena alteração na entrada gera um hash totalmente diferente;
- ➔ Rápido de calcular, mas impossível de inverter sem força bruta;

Os usos mais comuns são:

- ➔ Armazenamento de senhas: em vez de guardar senha diretamente, salva seu hash;
- ➔ Verificação de integridade de arquivos: comparar o hash original com o calculado ajuda a detectar alterações;
- ➔ Assinaturas digitais: o hash do conteúdo é assinado com a chave privada;
- ➔ Blockchain: usado para ligar blocos e garantir integridade e imutabilidade.

SHA2 (SHA-256, SHA-512, ...)

Muito utilizado em criptografia moderna, sendo considerado seguro.

SHA-1
Sistema antigo, hoje considerado inseguro

MD5
Muito usado no passado, mas inseguro.