

Atividade Criptografia

1. O que é criptografia?

Criptografia é o estudo e prática de técnicas que permitem a comunicação segura em presença de terceiros não autorizados. Ela envolve a transformação de informações (texto, dados, etc.) em um formato ilegível, chamado de "texto cifrado", de forma que apenas destinatários autorizados, que possuem a chave correta, possam decifrá-lo e obter novamente os dados originais.

2. Qual é a finalidade da criptografia na segurança da informação?

A criptografia visa proteger informações sensíveis contra acesso não autorizado e garantir a integridade e confidencialidade dos dados.

3. Cite um exemplo de uso comum da criptografia no cotidiano.

É amplamente utilizada em transações financeiras online para proteger informações confidenciais, como números de cartão de crédito.

4. Explique a diferença entre criptografia simétrica e criptografia assimétrica. Quais são as vantagens e desvantagens de cada abordagem?

Na **criptografia simétrica**, a mesma chave é usada tanto para criptografar quanto para descriptografar os dados, e exige que o emissor e o receptor compartilhem essa chave.

Vantagens:

- Eficiência e rapidez.
- Bem adequada para comunicação em tempo real e grandes quantidades de dados.

Desvantagens:

- Dificuldade na gestão das chaves (distribuição segura da chave secreta).
- Não oferece autenticação por si só (pode ser necessário um protocolo adicional para garantir a identidade das partes).

Já na **criptografia assimétrica**, são empregadas duas chaves diferentes: uma **chave pública** para criptografar os dados e uma **chave privada** correspondente para descriptografá-los. Isso permite uma comunicação segura entre duas partes, mesmo que nunca tenham se encontrado antes.

Vantagens:

- Gestão simplificada das chaves (não é necessário um canal seguro para distribuição da chave secreta).
- Oferece autenticação e garantias adicionais de segurança.

Desvantagens:

- Mais lenta que a criptografia simétrica.
- Menos eficiente para grandes volumes de dados
- Requer maior poder computacional para operações criptográficas.

5. Descreva o que é uma chave de criptografia e por que é importante para garantir a segurança dos dados criptografados.

Uma chave de criptografia é um valor usado para controlar o processo de criptografia e descriptografia de dados. Ela funciona como um elemento crucial na segurança dos dados criptografados porque determina como os dados serão transformados de seu estado original para um estado ilegível (criptografado) e de volta ao estado original (descriptografado) quando necessário. É importante para Confidencialidade, Integridade, Autenticação e Segurança contra ataques.