1- O que é criptografia? A criptografia é a prática de garantir a segurança da comunicação e dos dados através da transformação das informações em um formato ilegível para pessoas não autorizadas. Existem dois principais tipos: simétrica, que usa uma única chave para cifrar e decifrar dados, e assimétrica, que usa um par de chaves (pública e privada). A criptografia é fundamental para proteger a privacidade, integridade e autenticidade das informações em transmissões e armazenamentos de dados sensíveis.

2- Qual é a finalidade da criptografia na segurança da informação? A finalidade da criptografia na segurança da informação é proteger a confidencialidade, integridade e autenticidade dos dados. Ela transforma informações em um formato ilegível para pessoas não autorizadas durante a transmissão e armazenamento, garantindo que apenas destinatários autorizados possam acessar e compreender os dados protegidos.

3- Cite um exemplo de uso comum da criptografia no cotidiano. Um exemplo comum de uso da criptografia no cotidiano é durante a navegação na internet através do protocolo HTTPS. Esse protocolo utiliza criptografia para proteger as informações transmitidas entre o navegador do usuário e o servidor web, garantindo que dados como senhas, informações de pagamento e outras informações pessoais não sejam interceptados por terceiros enquanto estão em trânsito pela rede.

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

Criptografia Simétrica:

Definição: Utiliza uma única chave para cifrar (criptografar) e decifrar (descriptografar) os dados.

Vantagens:

É mais rápida e eficiente que a criptografia assimétrica.

Bem adequada para cifrar grandes volumes de dados.

Desvantagens:

Requer um método seguro para a distribuição da chave secreta entre remetente e destinatário.

Não oferece suporte à autenticação ou garantia de origem dos dados sem mecanismos adicionais.

Criptografia Assimétrica:

Definição: Usa um par de chaves: uma pública (para cifrar) e uma privada (para decifrar).

Vantagens:

Elimina a necessidade de compartilhar chaves secretas, o que simplifica a distribuição de chaves.

Suporta autenticação e garantia de origem através da assinatura digital.

Desvantagens:

É mais lenta e consome mais recursos computacionais que a criptografia simétrica.

Menos eficiente para cifrar grandes volumes de dados devido à sua natureza computacionalmente intensiva.

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 único e secreto usado para cifrar e decifrar dados durante o processo de criptografia. Ela é essencial para garantir a segurança dos dados criptografados porque determina como os dados são transformados em formato ilegível (cifrado) e posteriormente restaurados ao formato original (decifrado). A segurança da chave de criptografia é crucial, pois apenas quem possui a chave correta pode acessar os dados de forma legível. Sem uma chave adequada e segura, os dados criptografados podem ser comprometidos e acessados por terceiros não autorizados, comprometendo a confidencialidade e a integridade das informações protegidas.