**Logotipo

Descrição gerada automaticamente**

Serviço Nacional de Aprendizagem Industrial

SENAI “Gaspar Ricardo Junior”

Curso

TÉCNICO EM DESENVOLVIMENTODE SISTEMAS

*Criptografia*

Evellyn achnitz

kaique primissia

matheus alves

miguel dos santos

prof leandro Gaudio Rosa

prof vedilson prado dos santos

Sorocaba

maio – 2024

1. O que é Criptografia?

Criptografia é a prática de proteger as informações por meio do uso de algoritmos codificados, hashes e assinaturas. As informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação eletrônica trocada entre duas ou mais partes) ou em uso (durante a computação de dados). Criptografia é a conversão dos dados de um formato legível em um formato de código. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados. A criptografia de dados é muito usada por pessoas e grandes corporações para proteger as informações dos usuários enviadas entre um navegador e um servidor. Essas informações podem incluir de tudo, desde dados de pagamento até informações pessoais.

1. Sua importância na segurança cibernética

A criptografia é um agente de muitos protocolos e procedimentos de segurança cibernética. Por exemplo, se os invasores cibernéticos violarem uma rede, as informações pessoais e confidenciais de fácil acesso poderão correr o risco de serem roubadas, mas se o dispositivo armazenar somente informações criptografadas, os dados que os hackers acessarem se tornarão inúteis, pois eles não poderão ler sem a chave secreta correta. Atualmente, a criptografia é exigida por muitos regulamentos, como parte de conjunto de padrões de segurança cibernética. Isso é fundamental para organizações que armazenam informações pessoais privadas (PPI), como instituições financeiras e de saúde.

1. Funcionamento

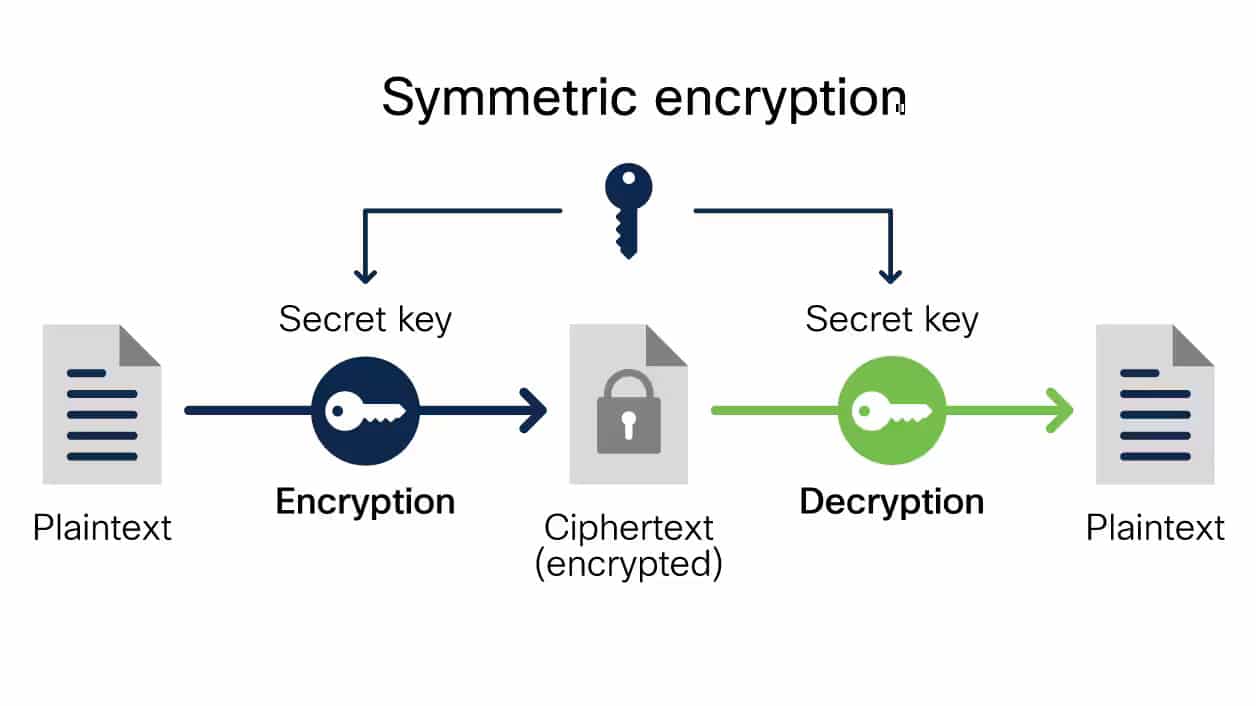
Esse procedimento consiste em codificar uma informação de forma que só pessoas que tenham acesso a ela consigam compreender. Quando informações ou dados são compartilhados na Internet, passam por vários dispositivos em rede espalhados pelo mundo, que fazem parte da Internet pública. À medida que passam pela Internet pública, os dados correm o risco de serem comprometidos ou roubados por hackers. Para evitar isso, os usuários podem instalar um software ou hardware específico para garantir que os dados ou as informações sejam transferidos com segurança.

É através de um algoritmo de encriptação que uma mensagem é convertida, de um texto não criptografado para um texto cifrado criptografado. Os algoritmos modernos usam matemática avançada e uma ou mais chaves criptografadas. Isso torna relativamente fácil criptografar uma mensagem, mas praticamente impossível descriptografá-la sem conhecer as chaves.

As técnicas de encriptação se dividem em duas categorias, simétricas e assimétricas, com base em como suas chaves funcionam:

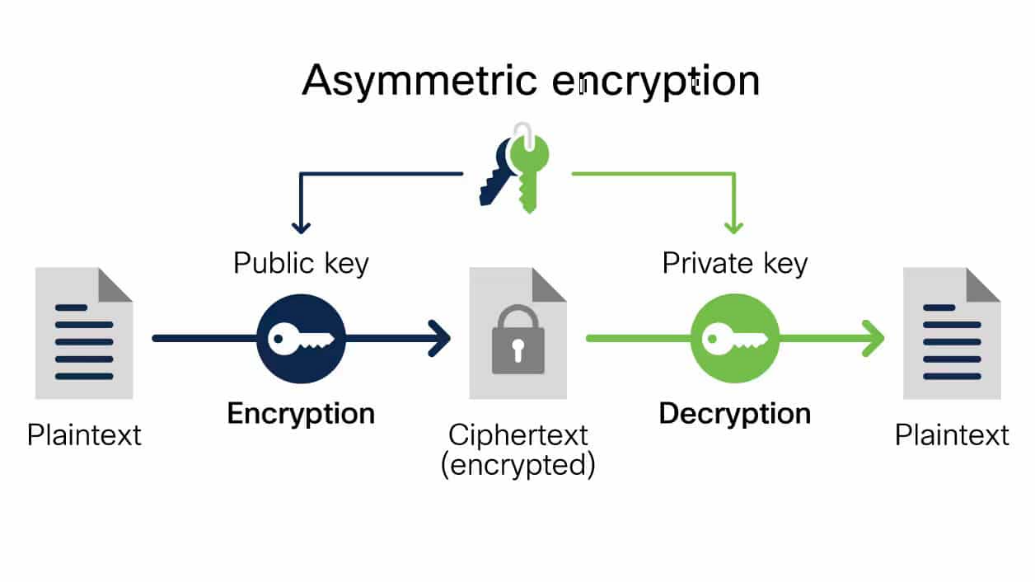
3.1 Criptografia Simétrica (Chave Privada)

Imagine dois cadeados que utilizam a mesma chave. Esta chave criptografa (bloqueia) e descriptografa (desbloqueia) os dados. É rápido, mas exige que as duas partes compartilhem a mesma chave secreta com segurança.



3.2 Criptografia assimétrica (chave pública)

Usa um par de chaves como duas fechaduras com chaves diferentes. Uma chave (pública) é amplamente compartilhada para criptografia, enquanto a outra (privada) é mantida em segredo para descriptografia. É mais lento que o simétrico, mas ótimo para comunicação segura sem chaves pré-compartilhadas.



3.3 Criptografia Hash

Esta não é realmente criptografia para mensagens. Ele cria uma impressão digital exclusiva (hash) dos dados. Quaisquer alterações nos dados resultarão em um hash diferente, tornando-o útil para verificar a integridade dos dados.

1. Tecnologias utilizadas (cifras)

Códigos de criptografia (ou cifras) são algoritmos específicos que implementam esses tipos. Exemplos: DES, AES são cifras usadas para criptografia simétrica.

Cifras Específicas:

DES (Data Encryption Standard): Uma cifra simétrica mais antiga, não mais considerada segura para a maioria dos usos.

DES-X: Uma variante do DES, não tão comum.

Triple DES (3DES): usa criptografia DES três vezes para melhorar a segurança, mas é mais lento que as opções mais recentes.

AES (Advanced Encryption Standard): O padrão atual para criptografia simétrica, considerado muito seguro.

1. Conclusão

A criptografia é uma necessidade do mundo atual em que existe tanta informação valiosa e sensível circulando pelos meios digitais, como forma de garantir níveis crescente e satisfatórios de segurança aos usuários e aos detentores dessa informação circulante.

1. Importância

O uso da criptografia é uma camada extra de proteção e segurança para proteger você dos riscos de invasão e vazamento de seus dados pessoais ou arquivos importantes e privados.

BIBLIOGRAFIA

**infowester.com** - Disponível em: < <https://www.infowester.com/criptografia.php> > Acessado em: 02/05/2024.

**ibm.com** - Disponível em: < <https://www.ibm.com/br-pt/topics/encryption> > Acessado em: 02/05/2024.

**amazon.com** - Disponível em: < <https://aws.amazon.com/pt/what-is/cryptography/> > Acessado em: 02/05/2024.

**kinsta.com** - Disponível em: < <https://kinsta.com/pt/base-de-conhecimento/o-que-e-criptografia-de-dados/> > Acessado em: 02/05/2024.