Criptografia

Criptografia

- Basicamente, é a conversão de dados de um formato legível em um formato codificado.
- Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.
- A criptografia é um elemento fundamental da segurança de dados.
- É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos.

Criptografia

- A criptografia de segurança de dados é amplamente usada por usuários individuais 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.

- Os softwares de criptografia de dados, também conhecidos como algoritmo de criptografia ou codificação, são usados para desenvolver um esquema de criptografia que teoricamente pode ser desvendado apenas com uma grande capacidade de processamento.

Como funciona a criptografia?

- Quando informações ou dados são compartilhados, passam por uma série de 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.
- Esses processos são conhecidos como criptografia em segurança de rede.

Como funciona a criptografia?

- A criptografia envolve a conversão de texto simples legível por humanos em texto incompreensível, o que é conhecido como texto cifrado
- Essencialmente, isso significa pegar dados legíveis e transformá-los de forma que pareçam aleatórios.
- A criptografia envolve o uso de uma chave criptográfica, um conjunto de valores matemáticos com os quais tanto o remetente quanto o destinatário concordam.
- O destinatário usa a chave para descriptografar os dados, transformando-os de volta em texto simples legível.

Como funciona a criptografia?

- Quanto mais complexa for a chave criptográfica, mais segura será a criptografia, pois é menos provável que terceiros a descritografem por meio de ataques de força bruta (ou seja, tentar números aleatórios até que a combinação correta seja adivinhada).

Técnicas de criptografia

- Os dois métodos mais comuns são a criptografia simétrica e assimétrica.
- Os nomes se referem a se a mesma chave é usada ou não para criptografia e descriptografia.

Técnicas de criptografia

- Chaves de criptografia simétrica:
  - Também conhecidas como criptografia de chave privada.
  - A chave usada para codificar é a mesma usada para decodificar, sendo a melhor opção para usuários individuais e sistemas fechados.
  - Caso contrário, a chave deve ser enviada ao destinatário.
  - Isso aumenta o risco de comprometimento se for interceptada por um terceiro.
  - Esse método é mais rápido do que o método assimétrico.

Técnicas de criptografia

- **Chaves de criptografia assimétrica**
  - Esse tipo usa duas chaves diferentes, uma pública e uma privada, que são vinculadas matematicamente.
  - Essencialmente, as chaves são apenas grandes números que foram emparelhados um ao outro, mas não são idênticos, daí o termo assimétrico.
  - A chave privada é mantida em segredo pelo usuário, e a chave pública também é compartilhada entre destinatários autorizados ou disponibilizada ao público em geral.

Exemplos de algoritmos de criptografia

- **Criptografia DES**
  - DES significa *Data Encryption Standard*.
  - Trata-se de um algoritmo de criptografia simétrica desatualizado, não considerado adequado para os usos atuais.
  - Portanto, outros algoritmos de criptografia sucederam o DES.

Exemplos de algoritmos de criptografia

- **Criptografia 3DES**
  - 3DES significa *Triple Data Encryption Standard*.
  - Esse é um algoritmo de chave simétrica, e a palavra "*triple*" (triplo) é usada porque os dados passam pelo algoritmo DES três vezes durante o processo de criptografia.
  - O Triple DES está sendo lentamente substituído, mas continua sendo uma solução de criptografia de hardware confiável para serviços financeiros e outros setores.

Exemplos de algoritmos de criptografia

- Criptografia AES
  - AES significa *Advanced Encryption Standard* e foi desenvolvido para atualizar o algoritmo DES original.
  - Entre alguns dos aplicativos mais comuns de algoritmo AES incluem-se aplicativos de mensagens, como o Signal ou WhatsApp, e o programa de compactação de arquivos WinZip.

Exemplos de algoritmos de criptografia

- Criptografia RSA
  - O RSA foi o primeiro algoritmo de criptografia assimétrica amplamente disponibilizado ao público.
  - O RSA é popular devido ao tamanho da sua chave e, por isso, amplamente utilizado para transmissão de dados segura.
  - RSA significa **Rivest, Shamir e Adleman**, os sobrenomes dos matemáticos que descreveram esse algoritmo.
  - O RSA é considerado um algoritmo assimétrico por usar um par de chaves.

Exemplos de algoritmos de criptografia

- Criptografia Twofish
  - Usado tanto em hardware quanto em software, o Twofish é considerado um dos mais rápidos do seu tipo.
  - O Twofish não é patenteado, sendo gratuitamente disponibilizado para quem quiser usá-lo.
  - Como resultado, você o encontrará em pacotes de programas de criptografia como PhotoEncrypt, GPG e o popular software de código aberto TrueCrypt.