SEGURANÇA DA INFORMAÇÃO

ALUNA: ROANE MENDES

1- A criptografia é um dos elementos fundamentais da segurança da rede. Ela é usado para proteger dados contra roubo, adulteração ou vazamento. Ela funciona embaralhando os dados em uma senha que só pode ser desbloqueada usando uma chave digital exclusiva. Os dados criptografados podem ser protegidos na máquina, em trânsito entre máquinas ou em repouso durante o processamento, seja local ou em um servidor remoto na nuvem.

2- A criptografia é um método de embaralhar dados para que não possam ser lidos por ninguém além da parte autorizada. O processo de criptografia usa uma chave de criptografia para converter texto simples em texto cifrado. Uma chave de criptografia é um conjunto de valores matemáticos conhecidos e acordados entre o remetente e o destinatário.

Qualquer pessoa com a chave correta pode descriptografar ou traduzir os dados criptografados. É por isso que os especialistas em criptografia continuam a desenvolver chaves mais complexas. A criptografia mais segura usa chaves complexas o suficiente para que os hackers considerem um processo de descriptografia exaustivo (também conhecido como “força bruta”) funcionalmente impossível.

3- A criptografia assimétrica é uma tecnologia mais avançada que usa duas chaves diferentes para criptografar e descriptografar informações. Uma das chaves é pública e pode ser compartilhada com qualquer pessoa, enquanto a outra chave é privada e deve ser mantida em segredo.

Dessa forma, torna-se um processo mais seguro, pois a chave privada é extremamente difícil de vazar. No entanto, isto é contrariado pela sua lentidão, uma vez que a encriptação e a desencriptação requerem mais processamento do que a encriptação simétrica.

4- *Criptografia simétrica:*

Como funciona: Uma única chave é usada para criptografar (criptografar) e descriptografar (descriptografar) informações.

Chaves: As chaves usadas para criptografia e descriptografia precisam ser mantidas em segredo entre as partes que se comunicam (chamado pré-compartilhamento de chave).

Vantagens:

Velocidade: Geralmente mais rápida que a criptografia assimétrica.

Eficiência: Requer menos recursos computacionais.

Simplicidade: Mais fácil de implementar e entender.

Desvantagens:

Distribuição de chaves: É necessário um método seguro para distribuir e gerenciar chaves simétricas entre as partes.

Segurança escalável: À medida que o número de participantes aumenta, aumenta também a complexidade do gerenciamento de chaves.

Criptografia assimétrica (ou criptografia de chave pública):

Como funciona: utiliza um par de chaves diferentes, mas matematicamente relacionadas: uma chave pública (para criptografia) e uma chave privada correspondente (para descriptografia).

Chaves públicas e privadas: As chaves públicas podem ser distribuídas gratuitamente, enquanto as chaves privadas devem ser mantidas em segredo pelos seus proprietários.

Vantagens:

Segurança de Chave: Elimina problemas de distribuição de chaves, pois as chaves privadas não precisam ser compartilhadas.

Autenticação: Facilita a verificação de identidade digital e assinaturas digitais.

Desvantagens:

Desempenho: Geralmente é mais lento que a criptografia simétrica

devido à complexidade dos algoritmos envolvidos.

Complexidade: Implementar e gerenciar sistemas que utilizam criptografia assimétrica pode ser mais complexo.

Uso Combinado:

Muitas vezes, sistemas de segurança utilizam ambos os tipos de criptografia em conjunto para aproveitar as vantagens de cada um. Por exemplo, a criptografia simétrica pode ser usada para cifrar dados grandes de forma eficiente, enquanto a criptografia assimétrica pode ser usada para distribuir chaves simétricas de forma segura.

5- Criptografia é a prática de proteger 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). A criptografia tem quatro objetivos principais:

Confidencialidade: disponibiliza as informações somente para usuários autorizados.

Integridade: garante que as informações não tenham sido manipuladas.

Autenticação: confirma a autenticidade das informações ou a identidade de um usuário.

Não repúdio: impede que um usuário negue compromissos ou ações anteriores.

A criptografia usa vários algoritmos criptográficos de baixo nível para atingir um ou mais desses objetivos de segurança das informações. Essas ferramentas incluem algoritmos de encriptação, algoritmos de assinatura digital, algoritmos de hash e outras funções.