Sistemas Computacionais e Segurança

Professor Robson Calvetti

Turma:

USJT-SINSP1AN-BUA2-SIST.COM.SEGURANÇA

Alunos:

Annely Desireé Junemann – 824217739

Francisco Alexandre Santos Melo- 824219751

Larissa da Silva Maschio – 824221401

Ano 2024

ATIVIDADE PRÁTICA 04

CRIPTOGRAFIA

- Citar 2 exemplos históricos do uso de criptografia:

1. Criptografia de *Blockchain* (corrente de blocos):

É um mecanismo de banco de dados avançada, no qual permite o compartilhamento de informações dentro da rede. É um banco de dados interligados em forma de cadeia. Para realizar modificação não é tão simples, os dados são cronologicamente consistentes, pois não é possível excluir nem modificar a cadeia sem o consenso da rede. O *Blockchain é muito utilizado em sistemas financeiros, para criar um ledger inalterável ou imutável para monitorar pedidos, pagamentos, contas e outras transações.*

2. Criptografia de Hash:

É uma técnica que possui uma sequência única de caracteres, a partir de um conjunto de dados. É usada em diversas aplicações, como em sistemas de autenticação e verificação de integridade de arquivos.

- Criptografia Simétrica: É o tipo em que só existe apenas uma única chave secreta que é usada para ambas as partes do processo, na criptografia e na descriptografia.

  Exemplos

  1. Data Encryption Standart(DES): é um algoritmo de criptografia simétrica que foi desenvolvido por volta da década de 1970. O DES realiza apenas duas operações sobre sua entrada, o chamado deslocamento de bits e substituição de bits. Ao repetir essas operações inúmeras vezes e de uma forma não-linear, chega-se a um resultado que não pode ser revertido sem o uso da chave, esse algoritmo trabalha com 64 bits. Ele foi desenvolvido há mais de 20 anos e até hoje não se sabe o caminho para quebra-lo, exceto por força bruta.

  2. Blowfish: esse algoritmo foi desenvolvido por Bruce Schneier em 1993. Esse tipo de criptografia é muito conhecido na área de negócios de e-commerce, devido a garantia de segurança ao lidar com métodos de pagamento. Ele foi criado para substituir o DES, ele

utiliza chaves de 32 a 446 bits, segmentando as informações em blocos de 64 bits e criptografando cada um deles individualmente. O blowfish é conhecido pela sua velocidade de encriptação e confiabilidade, muitos especialistas afirmam que o código é virtualmente inquebrável, ainda se destaca por estar na lista de algoritmos não patenteados e licença livre.

- Criptografia Assimétrica: É o tipo que existe duas chaves secretas, uma para cada parte do processo, sendo uma chave para criptografar e a outra para descriptografar.

  Exemplos:

  1. Rivest Shamir Adleman (RSA) atualmente é a base da maioria das aplicações de usam criptografia assimétrica, surgindo por volta de 1977. É um algoritmo de chave pública, a criptografia de RSA permite que os usuários criptografem mensagens com um código chamado chave pública que podem ser compartilhadas abertamente. Devido às propriedades matemáticas específicas do algoritmo RSA, uma vez que um usuário criptografa uma mensagem com uma chave pública, somente uma chave privada pode descriptografá-la. Os usuários têm um par de chaves públicas e privadas e este último são mantidos em segredo. Geralmente esse tipo é indicado usar em conjunto com outros sistemas de criptografia, a fim de comprovar a integridade e autenticidade das mensagem, geralmente, os usuários criptografam um arquivo com um algoritmo de chave assimétrica e utilizam a criptografia RSA para criptografar a chave simétrica. Assim, apenas uma chave privada RSA pode descriptografar a chave simétrica usada e sem ela, não é possível decifrar a mensagem.

  2. ElGamal: Foi fundado pelo egípcio Taher Elgamal, em 1984. É um algoritmo de chave pública, esse, diferente do RSA, envolve a manipulação de grandes quantidades numéricas. A segurança consiste em um algoritmo matemático discreto e de corpo finito-simular a uma fatoração.

Sites de pesquisa

https://www.veritas.com/pt/br/information-center/rsa-encryption

https://www.mjvinnovation.com/pt-br/blog/tipos-de-criptografia/

https://www.gta.ufrj.br/grad/99_2/marcos/des.htm

https://medium.com/prognosys/criptografia-sim%C3%A9trica-6b4271ff697c

https://www.clicksign.com/blog/tipos-de-criptografia-como-funcionam

https://academiatech.blog.br/exemplos-de-criptografia/