CRIPTOGRAFIA NA SEGURANÇA DE REDES

Nome
Curso - Disciplina

A criptografia é uma das mais populares estratégias de segurança de dados, uma vez que a segurança das informações passou a ser prioridade para diversas empresas. (FERNANDES, 2013)

Ramos (2002) destaca que essa técnica consiste na utilização de algoritmos para realizar a codificação e a decodificação das informações transmitidas na rede, onde apenas emissor e receptor possuem acesso à chave utilizada no processo.

Lopes(2019) acrescenta ainda que um dos modelos de criptografia utilizada na segurança das redes é o hash que é um algoritmo transforma qualquer bloco de dados em uma série de caracteres de comprimento.

Além do modelo hash, também existem os modelos de chaves simétricas ou assimétricas. Atualmente, a base da programação utilizada na criptografia simétrica e assimétrica são as chaves, que podem ser utilizadas para criptografar e também para descriptografar informações. (VOITECHEN, 2015)

Pimenta (2004) destaca que quando a chave é simétrica, pode ser usada nas duas pontas da transmissão. Já quando é assimétrica isso significa que as chaves de criptografia e descriptografia são diferentes.

Existem diversas aplicações para a criptografia, entre elas é possível destacar a proteção de computadores pessoais e empresariais e as informações contidas neles por meio de um controle de acesso, muitas vezes o firewall. (MACEDO, 2018)

Macedo (2018) ainda apresenta que a criptografia também é muito usada para a execução de trocas de dados através internet, com o objetivo de que informações permaneçam sigilosas mesmo que capturadas por algum programa malicioso.

Essa técnica permite também a criação de áreas de segurança dentro de um computador, onde todas as informações gravadas são automaticamente criptografadas. Além disso, essa tecnologia também é utilizada em tecnologia de blockchain, servindo para assinar criptograficamente todas as transações em uma rede. (MACEDO, 2018)

Percebe-se que a técnica de criptografia promove a confidencialidade e a proteção da integridade dessas informações, promovendo uma maior segurança na rede.

REFERÊNCIAS

FERNANDES, Nélia Campo. **Segurança da Informação**. 2013. Disponível em http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y. Acesso em 27 set. 2021.

LOPES, Luiz Ranyer de Araújo. **Implementação do Algoritmo Criptográfico Papílio Versátil na Biblioteca OpenSSL**. 2019. Disponível em https://repositorio.ufrn.br/bitstream/123456789/27971/1/Implementa%C3%A7%C3%A3oalgoritmocriptogr%C3%A1fico_Lopes_2019.pdf. Acesso em 27 set. 2021.

MACEDO, Ricardo Tombesi. **Redes de computadores**. 2018. Disponível em https://www.ufsm.br/app/uploads/sites/358/2019/08/MD_RedesdeComputadores.pdf. Acesso em 27 set. 2021.

PIMENTA, Andréa Lira Ribeiro. **Segurança nos Contratos Internacionais de compra e venda na Internet: criptografia e assinatura digital**. 2004. Disponível em https://repositorio.uniceub.br/jspui/bitstream/235/9411/1/20065157.pdf. Acesso em 27 set. 2021.

RAMOS, Karla Darlene Nepomuceno. **PAPÍLIO: Proposta de um Algoritmo de Criptografia Baseado no Algoritmo Viterbi e Codificação Convolucional**. 2002. Disponível em https://www.dimap.ufrn.br/~bedregal/Tese-alunos/Karla.pdf. Acesso em 27 set. 2021.

VOITECHEN, Dainara Aparecida. **Análise e comparação de algoritmos para criptografia de imagens**. 2015. Disponível em http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/6438/1/PG_COADS_2015_2_03.pdf. Acesso em 27 set. 2021.