Algoritmo de Huffman e Suas Aplicabilidades em Criptografia de Dados nas Redes Corporativas

Roney D. Freitas[1,2], Rhyan X. de Brito[1,3] , Janaide N. de Sousa[1,3]

[1]Faculdade Ieducare – Campus Tianguá, [2]Discente do Curso de Sistemas de Informação, [3]Professor(a) Orientador(a).

Palavras Chave: *Algoritmo. Segurança. Dados.*

INTRODUÇÃO

O algoritmo de Huffman é um método de codificação e compressão de dados, desenvolvido pelo engenheiro elétrico David Albert Huffman. O método é realizado através de uma árvore binária baseada nas probabilidades de ocorrência de cada símbolo onde na árvore as folhas representam os símbolos presentes nos dados, associados com suas respectivas probabilidades de ocorrência. [1]

Nesse enfoque a principal aplicação prática do algoritmo de Huffman é o cálculo de códigos binários para compressão de arquivos, ou seja, a transformação de um arquivo de caracteres em um arquivo de bits que ocupa pouco espaço. A ideia da compressão é usar poucos bits para representar os caracteres mais frequentes e mais bits para representar os mais raros.[2,3]

Nesses termos o trabalho tem como objetivo relatar a eficiência do algoritmo de Huffman como solução à segurança de dados em redes corporativas no processo de criptografia de dados.

METODOLOGIA

Este trabalho foi direcionado a pesquisas bibliográficas, fundamentadas na exploração, explicação e descrição de forma a enfatizar as contribuições do algoritmo de Huffman na criptografia de dados em redes corporativas, objeto de constantes ataques cibernéticos, dessa maneira evidenciando-se a preocupação com a segurança dos dados que trafegam pela rede.

RESULTADOS E DISCUSSÃO

Tendo em vista a criptografia como um fator primordial na segurança das redes corporativas, pôde-se destacar que o algoritmo de Huffman é uma excelente técnica não só na hora de criptografar, mas também para a compressão dos dados manipulados, deixando-os mais compactos e seguros. Levando-se em consideração o fato do mesmo transformar arquivos de caracteres em bits que ocupem pouco espaço, constatou-se a contribuição dele de forma substancial durante o processo criptográfico.

CONSIDERAÇÕES FINAIS

Observa-se que a aplicação de métodos à segurança de dados são algo primordial para garantir a privacidade de acesso a dados em redes corporativas. Diante de tal fato fica evidente a necessidade de busca por melhores técnicas que impeçam ataques a essas bases de dados. Dessa forma o trabalho enfatiza uma dessas técnicas como contra medida para evitar o vasto volume de ameaças constantemente sofridas pelos sistemas informáticos no segmento corporativo.

AGRADECIMENTOS

A Faculdade Ieducare, aos coordenadores de campus e de curso e em especial aos docentes orientadores da instituição que colaboraram para a realização desse trabalho. Motivando-nos e incentivando-nos a entrar no espaço da ciência, despertando a curiosidade e a necessidade de busca por respostas diante do desconhecido.

[1]CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; STEIN, C. **Introduction to algorithms**. 2ª edition. The MIT Press, 2001.
[2]Algoritmo de Huffman Disponível em < http://www.ime.usp.br/~pf/analise_de_algoritmos/aulas/huffman.html#file-compression>Acessado em: 03.09.2014.
[3]C. H. Papadimitriou e K. Steiglitz. Combinatorial Optimization: Algorithms and Complexity. Prentice-Hall, Inc.,1982.