UNIVERSIDADE FEDERAL DA GRANDE DOURADOS

FÁBIO HENRIQUE SANTOS DA SILVA

DES: IMPLEMENTAÇÃO, APLICAÇÃO E ANÁLISE

DOURADOS

2010

FÁBIO HENRIQUE SANTOS DA SILVA

DES: IMPLEMENTAÇÃO, APLICAÇÃO E ANÁLISE

Trabalho de Conclusão de Curso de graduação apresentado para obtenção do título de Bacharel em Sistemas de Informação.
Faculdade de Ciências Exatas e Tecnologia
Universidade Federal da Grande Dourados
Orientador: Prof. Dr. Lino Sanabria
Co-Orientador: Prof. M.Sc. Rodrigo Porfírio da Silva Sacchi

DOURADOS

2010

FÁBIO HENRIQUE SANTOS DA SILVA

DES: IMPLEMENTAÇÃO, APLICAÇÃO E ANÁLISE

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação na Universidade Federal da Grande Dourados, pela comissão formada por:

_____

Orientador: Prof. Dr. Lino Sanabria
FACET – UFGD

_____

Prof. M.Sc. Rodrigo Porfírio da Silva Sacchi
FACET – UFGD

_____

Prof. Dr. Joinvile Batista Junior
FACET-UFGD

Dourados, 03 de dezembro de 2010.

RESUMO

Neste trabalho busca-se apresentar um estudo sobre a segurança computacional, na forma da criptografia, por meio da implementação e análise do padrão *Data Encryption Standard* (DES). São mostrados os preceitos e fundamentos da criptografia simétrica e do padrão DES, que, mesmo sendo considerado inseguro para algumas aplicações atualmente, foi utilizado em larga escala e auxiliou o entendimento da criptoanálise moderna. O padrão de criptografia DES foi criado no início da década de 1970 e se baseia em uma combinação de técnicas de substituição e permutação. Assim como todo algoritmo de criptografia moderno, utiliza uma chave para cifragem dos dados. O trabalho trata também sobre assinaturas de arquivos – padrões que existem em arquivos de mesmo tipo – que podem facilitar a criptoanálise. Pesquisou-se também sobre o cabeçalho dos tipos de arquivo DOC, XLS, PDF e JPEG, com o objetivo de, no momento da implementação, verificar os padrões nos arquivos que forneceriam brechas para criptoanálise e a conseqüente quebra do algoritmo. Criou-se uma aplicação, executada via linha de comando, que utiliza o DES para criptografia e decriptografia de arquivos, utilizando uma chave de oito caracteres e realizando tratamentos nos tipos de arquivos mais comuns, buscando reforçar a segurança do aplicativo. Trata-se, portanto, de uma pesquisa que objetiva observar os conceitos da criptologia, utilizando o DES como objeto de estudo.

Palavras-chave: Criptologia, *Data Encryption Standard***,** Implementação.