Universidade Federal de Mato Grosso Instituto de Computação Criptografia e Segurança de Dados

Neste trabalho o aluno deverá desenvolver um programa para geração de um resumo criptográfico (hash) de 64 bits. A linguagem de programação será C ou Python (escolher) e seu funcionamento será da seguinte forma:

Entrada:

Path para o arquivo (absoluto ou relativo)

O arquivo deve ser lido em binário

Processamento:

Dividir o arquivo em blocos de 64 bits, fazendo “bit stuffing” do último bloco para que este contenha 64 bits. O “bit stuffing” deve ser feito com valores 1.

1º Bloco XOR 2º Bloco XOR 3º Bloco ....

Para aumentar a dificuldade deste hash, cada bloco deve ter uma rotação de n bits a esquerda de forma circular, em que n é o número do bloco.

Saída:

Resumo de 64 bits mostrado em hexadecimal (16 caracteres)

Exemplo com bloco de 8 bits

Entrada: <path do arquivo>

Exemplo do arquivo em binário: 10101101 01000110 11010110 10101111

Processamento: XOR (XOR (XOR (01011011, 00011001), 10110110), 11111010)

1º bloco -> rotação de 1 bit a esquerda

2º bloco -> rotação de 2 bits a esquerda

3º bloco -> rotação de 3 bits a esquerda

4º bloco -> rotação de 4 bits a esquerda