CIC0201 - Segurança Computacional – 2024/2

Profa. Lorena Borges

Trabalho de Implementação 1 – S-DES

Este trabalho explora o S-DES (Simplified DES) que representa uma versão simplificada do DES usada para fins educacionais. O S-DES é projetado para ajudar a entender os conceitos básicos de cifragem de blocos, utilizando chaves menores e um processo menos complexo.

O S-DES utiliza uma **chave de 10 bits** e trabalha com **blocos de dados de 8 bits**, além de realizar apenas duas rodadas da rede de Feistel.

Segue a descrição dos passos do S-DES:

1. **Geração de Chaves Subjacentes**

O S-DES utiliza uma chave principal de 10 bits, da qual duas subchaves (K1 e K2) são derivadas através de permutações e deslocamentos:

Passos de Geração de Chaves:

- Permutação P10: Reorganiza os bits da chave.
- Deslocamento Circular: Divide a chave em duas metades e aplica um deslocamento circular.
- Permutação P8: Seleciona e permuta 8 dos 10 bits para formar K1.
- Deslocamento Circular Duplo: Aplica um deslocamento circular duplo nas metades.
- Permutação P8: Novamente seleciona e permuta 8 bits para formar K2.

2. **Permutação Inicial (IP):**

   Antes de iniciar as rodadas de Feistel, o S-DES aplica uma permutação inicial aos bits do bloco de dados.

3. **Divisão em Metades:**

   O bloco de dados de 8 bits é dividido em duas metades de 4 bits, denominadas L (esquerda) e R (direita).

4. **Rodadas de Feistel:**

   O S-DES executa duas rodadas principais de Feistel. Em cada rodada:

   - Função F: Uma função não-linear é aplicada à metade direita (R) combinada com a subchave da rodada (K1 na primeira rodada e K2 na segunda rodada). Esta função inclui expansão/permutação, S-Boxes (substituições) e uma permutação P4.
   - XOR: O resultado da função F é então combinado com a metade esquerda (L) usando a operação XOR.
   - Troca: As metades L e R são trocadas no final da primeira rodada.

5. **Permutação Final (IP^{-1}):**

   Após as rodadas de Feistel, uma permutação final é aplicada para obter o bloco cifrado.

TRABALHO:

Crie um software que possa encriptar e decriptar usando S-DES.
Parâmetros e Dados:
Chave de 10 bits: 1010000010
Bloco de dados de 8 bits: 11010111

Observações:

1. Não é permitida a utilização de bibliotecas públicas, como OpenSSL, para primitivas criptográficas de cifração e decifração assimétrica, e geração de chaves.
2. A avaliação será mediante a verificação das funcionalidades e inspeção do código.
3. Implementação preferencialmente individual, podendo ser em dupla. Linguagens preferenciais C, C++, Java e Python.

O que deve ser entregue: o código fonte e seu executável, descritivo (4 pg max) do S-DES e da resolução em etapas das funções intermediárias para o texto em claro e chaves fornecidas.

Data de Entrega: 20/12/2024. Instruções de entrega serão divulgadas oportunamente.

Material para consulta (postado na plataforma Aprender3):

G-SDES