**Trabalho de Implementação 1 - S-DES**

**Disciplina**: CIC0201 - Segurança Computacional – 2024/2

**Professora**: Lorena Borges

**Alunos**: Pedro Henrique Souza dos Santos e Fabio Lucas Parra

**GitHub:** [**https://github.com/flbparra/simplified\_des\_sec\_2024**](https://github.com/flbparra/simplified_des_sec_2024)

**Descrição do Projeto**

Este documento apresenta a implementação do algoritmo **S-DES (Simplified DES)** em Python, organizado em fases claras conforme especificado:

* Gerar Chave
* Permutação Inicial do Bloco de Dados
* Entrar nas Rodadas de Feistel
* Modular Operador Principal
* Visualização de Resultado

**Estrutura e Implementação**

1. **Gerar Chaves**

**Objetivo:** Gerar as chaves subjacentes K1 e K2 a partir da chave principal de 10 bits fornecida.

* Realiza permutação de bits de acordo com uma tabela especificada. Interface gráfica do usuário

  Descrição gerada automaticamente
* Realiza deslocamento circular à esquerda.

Texto

Descrição gerada automaticamente

* Gera as chaves K1 e K2 a partir de uma chave de 10 bits.  
  Interface gráfica do usuário, Texto

  Descrição gerada automaticamente
* Permutação P10

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

* Deslocamento circular e geração de K1

Texto

Descrição gerada automaticamente

* Deslocamento circular duplo e geração de K2  
  Texto

  Descrição gerada automaticamente

**Chave fornecida**

Fundo preto com letras brancas

Descrição gerada automaticamente

1. **Permutação Inicial do Bloco de Dados**

**Objetivo:** Aplicar a permutação inicial (IP) no bloco de dados de 8 bits.

* **Permutação Inicial**

**Uma imagem contendo Texto

Descrição gerada automaticamente**

* **Bloco de dados fornecido**

**Texto

Descrição gerada automaticamente**

1. **Entrar nas Rodadas de Feistel**

**Objetivo**: Realizar as duas rodadas de Feistel utilizando as chaves K1 e K2 geradas.

* Realiza a operação XOR entre dois conjuntos de bits.

Texto

Descrição gerada automaticamente

* Executa uma rodada de Feistel.

Expansão/Permutação = (E/P)

Texto

Descrição gerada automaticamente

* S-Boxes

Texto

Descrição gerada automaticamente

* Executando as rodadas de Feistel

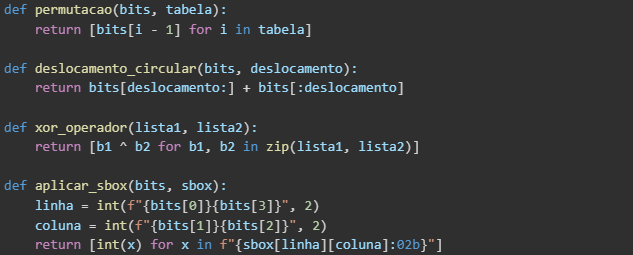
Texto

Descrição gerada automaticamente

1. **Modular Operador Principal**

**Objetivo**: Modularizar as operações principais (permutar, XOR, S-Box) para facilitar a reutilização do código e manter a clareza.

**Observação:** Todas as funções implementadas anteriormente já modularizam essas operações (permutar, XOR, sbox).



1. **Visualização de Resultados**

**Objetivo**: Mostrar os resultados das etapas executadas:

**Implementação final**:

* Chaves geradas



* Saida após a permutação inicial



* Saídas após as rodadas de Feistel

Texto

Descrição gerada automaticamente

* Permutação final (FP)

Texto

Descrição gerada automaticamente

**Resultado:**

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente