Especificação do Trabalho: Implementação de Esquema Criptográfico Simplificado

Introdução

O objetivo deste trabalho é implementar um esquema criptográfico simplificado utilizando funções básicas de geração de chave (GEN), criptografia (ENC) e descriptografia (DEC). A implementação deve ser feita na linguagem Python versão 3.10, e deve gerar resultados práticos que serão apresentados em slides e acompanhados de testes detalhados.

Definição das Funções

1. Função GEN(seed)

- Recebe um valor inicial (seed).
- Gera uma chave binária (lista de 0's e 1's) cujo comprimento é 4 vezes o tamanho da semente (|K| = 4 * len(seed)).

2. Função ENC(K, M)

- Recebe como entrada:
  - Uma chave K, lista binária com tamanho 4 * len(seed).
  - Uma mensagem M, também uma lista binária com tamanho 4 * len(seed).
- Retorna uma cifra C, lista binária de mesmo tamanho das entradas (4 * len(seed)).

3. Função DEC(K, C)

- Recebe a chave K e a cifra C.
- Retorna a mensagem original m.

Critérios de Avaliação

O trabalho será avaliado com base nos seguintes critérios de qualidade (até 5 pontos extras para os melhores trabalhos):

1. Tempo de execução

- Implementações com menor tempo de execução terão melhor avaliação.

2. Chaves equivalentes

- Idealmente, não deve haver duas chaves diferentes (K1 != K2) que produzam a mesma cifra para uma dada mensagem:
  - ENC(m, K1) = ENC(m, K2).
- Quanto menor o número de chaves equivalentes, melhor será a avaliação.

3. Teste de Difusão

- Avaliação da qualidade da cifra com base no efeito da alteração de um único bit da mensagem original.
- Avaliar quantos bits da cifra (C) são alterados quando apenas 1 bit da mensagem (M) é modificado.

4. Teste de Confusão

- Avaliação do impacto da alteração de um único bit na seed utilizada para gerar a chave.
- Quantificar quantos bits na cifra (C) se alteram ao manter a mensagem fixa e alterar um único bit da seed original.

Entregáveis

- Código-fonte Python 3.10 (.py) disponível via repositório Git.

- Slides de apresentação descrevendo o funcionamento das funções implementadas, resultados dos testes e conclusões (máximo de 4 slides).

- PDF detalhando a descrição do trabalho, código implementado e resultados dos testes realizados.