CIC0201 - Segurança Computacional – 2025/1

Disciplina: Segurança Computacional

Professora: Lorena Borges

Lista de Exercícios 01

Ex1: Quebrando Shift Cipher

- Elaborar os códigos para realizar a cifra por deslocamento e a respectiva decifração (dica: validar para cifra de César onde k=3);
- Elaborar os códigos que quebram a cifra por deslocamento, através de duas estratégias de ataques à cifra (CipherText-only):
    - por ataque de força bruta;
    - por distribuição de frequência;

* Descrever a viabilidade das estratégias, comparar a complexidade dos algoritmos e tempo de execução, onde cada técnica seria melhor aplicada etc.

** Utilizar a distribuição de frequência da língua portuguesa: https://www.dcc.fc.up.pt/~rvr/naulas/tabelasPT/

Ex2: Quebrando Cifra por Transposição

- Elaborar o código para realizar uma cifra por transposição (dica: pode escolher o método de permutação);
- Elaborar os códigos que quebram a cifra por transposição, através de duas estratégias de ataques à cifra (CipherText-only):
    - por ataque de força bruta;
    - por distribuição de frequência;

* Descrever a cifra por transposição escolhida no algoritmo para encriptar e a viabilidade das estratégias, comparar a complexidade dos algoritmos e tempo de execução, onde cada técnica seria melhor aplicada etc.

** Utilizar a distribuição de frequência da língua portuguesa: https://www.dcc.fc.up.pt/~rvr/naulas/tabelasPT/

As entregas deverão conter:

Códigos (C/C++, Java ou Python): para cada exercício, função de criptografia com a chave k, função de descriptografia, códigos de quebra da cifra e resultados dos textos das tentativas de quebra.

Análises: relatório em .pdf consolidando uma rápida contextualização teórica sobre as cifras e técnicas utilizadas, inspeção/explicação dos códigos, saídas dos testes realizados, comparativos e análises no contexto de segurança computacional.