CIC0201 - Segurança Computacional – 2024/2

Disciplina: Segurança Computacional

Professora: Lorena Borges

Lista de Exercício 01

Ex1: Quebrando Shift Cipher

Elaborar o código para realizar a cifra por deslocamento (dica: validar para cifra de César onde k=3);
Elaborar o código que quebra a cifra por deslocamento, descodificando através de duas estratégias de ataques à cifra (CipherText-only):
por distribuição de frequência;
por ataque de força bruta;
O resultado será o texto descriptografado e o tamanho da chave de deslocamento k.
* Descrever a viabilidade das estratégias, comparar a complexidade e tempo de execução dos algoritmos.

** 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 a cifra por transposição (dica: pode escolher o método de permutação);
Elaborar o código que quebra a cifra por transposição, descodificando por análises ao texto cifrado (CipherText-only):
O resultado será o texto descriptografado
* Descrever a técnica de permutação utilizada no algoritmo para encriptar e estratégia de quebra da cifra.

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