Lista de exercícios 1
Criptografia clássica
Segurança da Informação

1. Escreva uma definição formal dos algoritmos de Geração de Chave, Encriptação e Decriptação para a cifra de Vigenère.

2. Descreva um método para atacar uma cifra de substituição.

3. Qual é o tamanho do espaço de chaves em cifras de substituição assumindo 26 letras?

4. Quais são as 5 letras mais comuns em português? E em inglês?

5. Escreva um código em C que recebe um arquivo em texto codificação ASCII e computa as frequências de caracteres únicos e de pares de caracteres (2-grams).

6. Decripte: VMF QTP FOH MJJ XSFCS SIMTNFZXF YIS EIYUIK HWPQ MJJ QSLV TGJKGF

7. Quantas chaves são necessárias para 2 pessoas se comunicarem usam criptografia de chave secreta?

8. Quantas chaves são necessárias para N pessoas se comunicarem usam criptografia simétrica?

9. O que é uma cifra? O que é um código?

10. Descreva a cifra de substituição mono-alfabética.

11. Escreva um código em C para encriptar/decriptar usando uma cifra de substituição mono-alfabética.

12. Descreva uma cifra de permutação.

13. Escreva um código em C para encriptar/decriptar usando uma cifra de permutação.

14. Em que situações a codificação Base64 é útil?

15. Qual é o ganho de usar a codificação em Base64 em comparação a usar ASCII para representar números em Hexadecimal?

16. O que é busca de força-bruta?

17. Escreva um código em C para fazer busca exaustiva para encontrar a chave de textos cifrados por uma cifra de permutação.

18. Escreva um código em C para fazer busca exaustiva para encontrar a chave de textos cifrados por uma cifra mono-alfabética.