UNIVERSIDADE PORTUCALENSE
INFANTE D. HENRIQUE

Algoritmia Aplicada

Departamento de Inovação, Ciência e Tecnologia

Laboratório 3

Processamento de Cadeias de Caracteres

NOTA:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	□
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

1. Escreva um algoritmo para codificar um texto (TEXTO) pelo método *Cifra de Vigenere* (chave: CHAVE). Codifique o texto "CARACTER", considerando que a chave é igual ao texto.

2. Escreva um algoritmo para descodificar uma mensagem (CODIGO) que foi codificada pelo método *Cifra de Vigenere* (chave: CHAVE). Descodifique a mensagem "FBJBEMM", considerando que a chave é "ABD".

3. Escreva um algoritmo para codificar um texto (TEXTO) por um *Método de Permutação*, em que grupos sucessivos de N caracteres são rearranjados do seguinte modo: cada caracter avança uma posição, cabendo ao último caracter a primeira posição (organização circular). Admita que o texto é completado por tantos espaços quantos os necessários para perfazer o último grupo de N caracteres. Codifique o texto "GOSTO DISTO", considerando N= 3.

Admita que um cripto-analista conhecia o texto codificado e sabia qual o método utilizado para o efeito, exceptuando o valor de N. Quantas tentativas diferentes teria de ensaiar para descobrir o texto original?

4. Escreva um algoritmo para codificar um texto (TEXTO) por um *Método de Permutação*, em que grupos sucessivos de N caracteres são rearranjados do seguinte modo: cada caracter avança M (M < N) posições (organização circular). Admita que o texto é completado por tantos espaços quantos os necessários para perfazer o último grupo de N caracteres. Codifique o texto "GOSTO DISTO", considerando N = 4 e M = 2.

Admita que um cripto-analista conhecia o texto codificado e sabia qual o método utilizado para o efeito, exceptuando os valores de N e M. Quantas tentativas diferentes teria de ensaiar para descobrir o texto original?

5. Escreva um algoritmo para recuperar um texto comprimido pelo *Método dos Comprimentos de Séries*. Admita que o texto original apenas contém letras e o caracter <espaço>.

6. Crie a árvore de codificação usada pelo algoritmo de *Huffman*, para encriptar a frase "POUCAS FRASES COM UMA PALAVRA". Para o efeito, considere que os ramos esquerdos originam os 0´s e os ramos direitos originam os 1´s, e que os caracteres estão pela ordem, <espaço> , C, E, F, M, O, P, R, S, U, V, L, A
Usando a árvore criada, descodifique a mensagem "10110010110100 000110111001001101111".

7.

a) Crie a árvore de *Huffman* para encriptar a frase "ESTRUTURA AUTO ORGANIZATIVA", dispondo os caracteres pela ordem <espaço>, E, S, T, O, G, N, I, Z, V, R, U, A.

b) Escreva um algoritmo que receba uma árvore de *Huffman* criada com apontadores e uma cadeia de 0´s e 1´s, e devolva o texto descodificado correspondente (considere que os ramos esquerdos originam os 0´s e os ramos direitos originam os 1´s).

8. Escreva um algoritmo que receba uma árvore de *Huffman* criada com apontadores e devolva um vector, indexado por caracteres, contendo as *strings* de codificação dos vários caracteres (considere que os ramos esquerdos originam os 0´s e os ramos direitos originam os 1´s).

9. Uma cadeia de caracteres contém um texto encriptado pelo método de *Vigenere* e a respectiva chave de codificação, estando os caracteres desta chave distribuídos ao longo da cadeia, de D em D caracteres, sendo o último caracter um "S". Escreva um algoritmo que receba uma cadeia, CADEIA, e D, e devolva a chave e o texto original.

10. Considerando o texto, "ZABBCCCDDDDEEEEEFFFFFFZZZZ", comprima-o, utilizando o método *codificação segundo comprimentos de séries*. Utilize, para o efeito, apenas os 26 caracteres do alfabeto "ABC…XYZ", e considere que o caracter Z é também usado para indicar que se segue um par do tipo (contador, caracter).

11. Considerando o texto, "EXAME", encripte-o pelo método *cifra de Vernam*, usando a chave "EXAME". Quantas tentativas diferentes teria de ensaiar um cripto-analista para tentar decifrar o código? Admitindo que as ensaiava todas, será que descobria o texto original? Justifique.

12. Enuncie duas propriedades fundamentais do método de encriptação "*RSA*".

13. Um alfabeto usa apenas sete caracteres (A,B,C,D,E,F,G). Em média, um texto escrito com esse alfabeto tem as seguintes frequências de ocorrência de cada uma das letras (em percentagem): A-30, B-30, C-20, D-8, E-5, F-4, G-3 (note-se que a soma destas percentagens é obviamente 100%).

a) Desenhe a *árvore de Huffman* correspondente a estas frequências, representando as letras verticalmente e por ordem alfabética.

b) Admitindo que os ramos esquerdos (ascendentes) valem 1 e que os direitos (descendentes) valem 0, descodifique o código 0 0 0 1 1 1 1 0 0 0 1.

c) Admita que tem um texto de exactamente 100 caracteres daquele alfabeto. Qual a economia que esperaria encontrar com este método de compressão, face ao texto original escrito com um código compacto de 3 bits por caracter.

14. Considerando o texto, "FÉRIAS", encripte-o pelo método *cifra de Vigenere*, usando a chave "JA". Admitindo que um cripto-analista conhecia o comprimento da chave, mas não o seu conteúdo, quantas tentativas diferentes teria de ensaiar para tentar descobrir o texto original? Justifique.