UNIVERSIDADE ABERTA
www.uab.pt

Ministério da Educação e Ciência

U.C. 21045

Estruturas de Dados e Algoritmos Avançados

29 de janeiro de 2014

INSTRUÇÕES

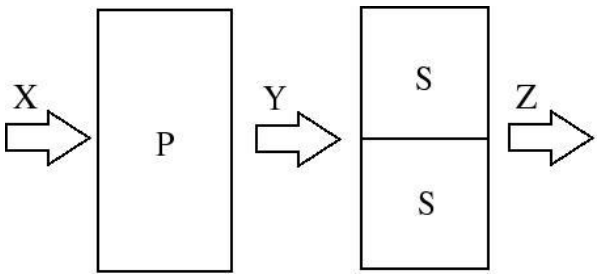
Para a resolução do teste, leia as seguintes informações e instruções, antes de responder

- Leia estas instruções na totalidade antes de iniciar a resolução do teste.
- O enunciado do teste é constituído por três grupos de questões, tem **3** páginas e termina com a palavra FIM.
- O teste deve ser resolvido na sua totalidade em folhas de respostas, ficando o aluno com o enunciado.
- O teste é SEM CONSULTA. Todos os elementos necessários à resolução são fornecidos no enunciado.
- Utilize esferográfica azul ou preta para responder às questões. Respostas a lápis não serão consideradas.
- Nas respostas, tenha a preocupação de utilizar uma letra legível por outra pessoa.
- A correção do teste terá em conta critérios de proficiência e compreensibilidade do código ou pseudocódigo.
- Se o seu exemplar não estiver completo ou nele se verificar qualquer outra deficiência, por favor dirija-se ao professor vigilante.
- O não cumprimento das instruções implica a anulação das respetivas questões.
- O tempo de realização do teste é de 120 minutos, mais 30 minutos de tolerância.

I [6 valores]

1.1. [2] Comente e justifique o segundo princípio criptográfico: É necessário um método que anule ataques por reenvio de mensagens genuínas.

1.2. Considere uma caixa P de 8 bits que opera com a chave "43521076" e uma caixa S de 4 bits que opera com a chave "E9862D4F70CB13A5" (hexadecimal). Considere a associação destas caixas em cascata de modo a formar um dispositivo que implementa uma cifra de produto, conforme a figura seguinte,



1.2.1 [2] Determine as palavras binárias Y e Z se à entrada for colocada a palavra binária X="1010 0111".

1.2.2 [2] As funções P^{-1} (inversa da caixa P) e S^{-1} (inversa da caixa S) podem ser obtidas por caixas P e S com chaves apropriadas, denominadas chaves inversas. Determine as chaves inversas que permitem respetivamente implementar a função inversa da caixa P e da caixa S. Determine as palavras binárias Y e X se à saída se tem Z="1100 0101".

II [8 valores]

2.1. [3] Construa uma codificação de Huffmann para o alfabeto da tabela abaixo. Apresente a construção da árvore de Huffmann passo a passo e a codificação final para cada símbolo.

Símbolo	A	B	C	D	E	F	G	H
Probabilidade	0.05	0,10	0,05	0,15	0,25	0,1	0.18	0.12

Notas: (i) Na união de dois símbolos/árvores, a posição da união é a da esquerda; (ii) Na união de dois símbolos/árvores quando existe mais do que uma possibilidade, são escolhidos os dois símbolos/árvores mais à esquerda.

2.2. [3] Aplique o algoritmo de Ziv-Lempel LZ77 para codificar a mensagem seguinte,

S="AABCDDDBCDABBABBABACDADABACDCDBACDEEEBACE"

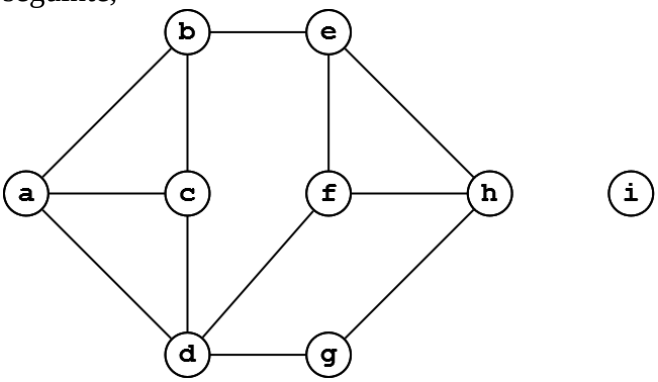
Utilize $\ell 1$=8 (dimensão do buffer de procura, indexado de 0 a 7, da direita para a esquerda) e $\ell 2$=8 (dimensão do look-ahead buffer). Calcule a taxa de compressão para a codificação obtida (suponha que cada caracter A,B,C,D,E requer 8 bits).

2.3. [2] Aplique o algoritmo de Ziv-Lempel LZ77 para descodificar a mensagem seguinte, para a qual foi utilizado $\ell 1=8$ (dimensão do buffer de procura, indexado de 0 a 7, da direita para a esquerda).

(0,0,B) (0,0,C) (1,1,A) (0,0,C) (2,2,C) (5,3,A) (4,4,C) (1,5,A) (0,4,B) (0,1,C)

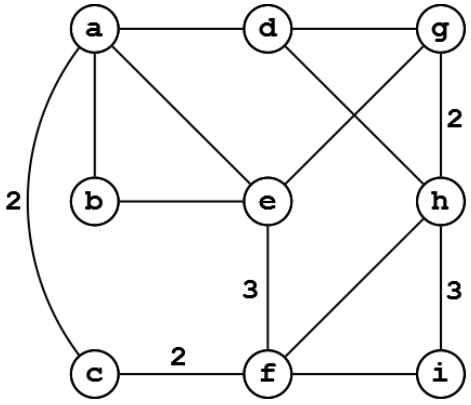
III [6 valores]

3. Considere o grafo seguinte,



3.1. [2] Descreva o algoritmo de pesquisa em profundidade (depth first search) em pseudocódigo e aplique-o para efetuar o varrimento do grafo (graph traversal) tomando para vértice inicial o vértice `f`. Considere os vértices adjacentes ordenados alfabeticamente.

4. Considere o grafo da figura seguinte, com arestas de peso unitário por defeito,



4.1. [0.5] Classifique o grafo. Justifique.

4.2. [0.5] Converta o grafo para a representação por tabela de adjacências. Considere os vértices adjacentes ordenados alfabeticamente.

4.3. [3] Aplique o algoritmo de Dijkstra com início no vértice a. Construa uma tabela onde as linhas representam os vértices do grafo, as colunas o vértice activo/nº de iteração e os elementos da tabela a distância ao vértice inicial. Indique a distância mais curta e o respetivo caminho entre o vértice `a` e o vértice `i`.

FIM