UNIVERSIDADE ABERTA
www.uab.pt

Ministério da Ciência, Tecnologia e Ensino Superior

U.C. 21045

Estruturas de Dados e Algoritmos Avançados

14 de Fevereiro de 2013

INSTRUÇÕES

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

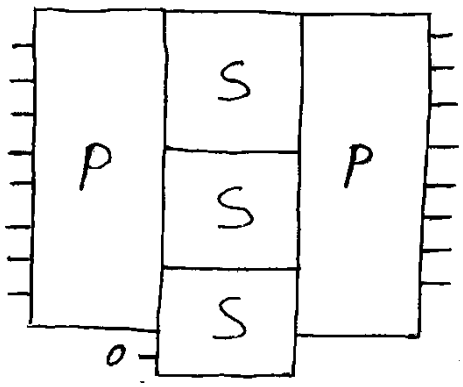
- Leia estas instruções na totalidade antes de iniciar a resolução do teste.
- O teste é constituído por três grupos de questões, tem 3 páginas e termina com a palavra FIM.
- O cabeçalho deve ser preenchido de modo legível antes do início da resolução.
- O teste é SEM CONSULTA. Todos os elementos necessários 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 correcção do teste terá em conta critérios de proficiência e compreensibilidade do código ou pseudo-código.
- 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 respectivas questões.
- O tempo de realização do teste é de 120 minutos, mais 30 minutos de tolerância.

I [6 valores]

1.1. [1.5] Diga o que entende por criptoanálise (cryptanalysis) e por criptografia (criptography).

1.2. [1.5] Comente a frase "O criptógrafo deve assumir sempre que o criptoanalista consegue cifrar quantidades arbitrárias de texto simples à sua escolha".

1.3. [3] Considere uma caixa P de 8 bits que opera com a chave "32476501 " e uma caixa S de 3 bits que opera com a chave "73210645". Considere a associação destas caixas em cascata de modo a formar um dispositivo que implementa uma cifra de produto, conforme a figura seguinte,



Determine a palavra binária à saída do dispositivo se à entrada for colocada a palavra binária "1101 0011".

II [6 valores]

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

Símbolo	A	B	C	D	E	F
Prob.	0,20	0,12	0,25	0,02	0,1	0.31

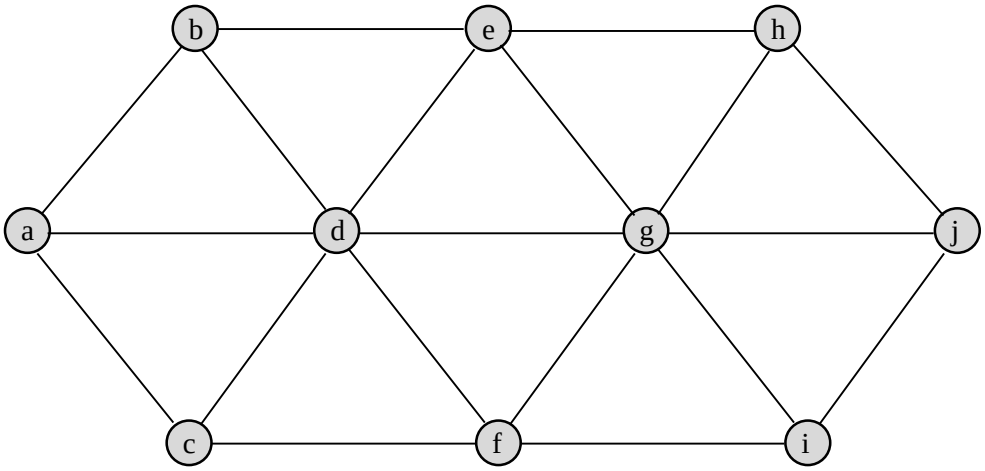
2.2. [3] Aplique o algoritmo de Ziv-lempel LZW para codificar a mensagem seguinte,

S="DDCDACDDDCDAADCDAADCBADBBDDADADBC"

Para o efeito indique as palavras iniciais do dicionário e depois construa uma tabela com as seguintes colunas: entrada, palavra procurada no dicionário, saída e nova palavra do dicionário. Entradas não usadas da tabela devem ser deixadas em branco.

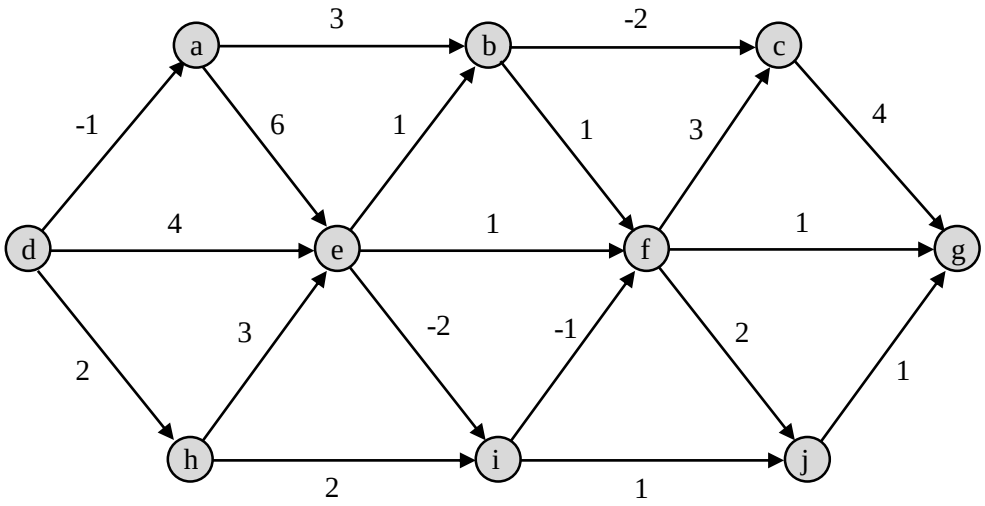
III [8 valores]

3. Considere o grafo seguinte,



3.1. [3] Aplique o algoritmo de pesquisa em largura (breadth first search) para efectuar o varrimento do grafo (graph traversal), tomando para vértice inicial o vértice b. Indique justificando a sequência em que os vértices do grafo são visitados.

4. Considere o grafo seguinte,



4.1. [1] Converta o grafo para a representação por tabela de adjacências.

4.2. [3] Aplique o algoritmo de Ford com início no vértice d. Construa uma tabela onde as linhas representam os vértices do grafo, as colunas o nº de iteração e os elementos da tabela a distância ao vértice inicial.

4.3. [1] Indique a distância mais curta e o respectivo caminho entre o vértice d e o vértice g. Justifique.

FIM