UNIVERSIDADE ABERTA
www.uab.pt

Ministério da Educação e Ciência

p-Fólio

U.C. 21045

Estruturas de Dados e Algoritmos Avançados

8 de fevereiro de 2012

Exemplo de resolução

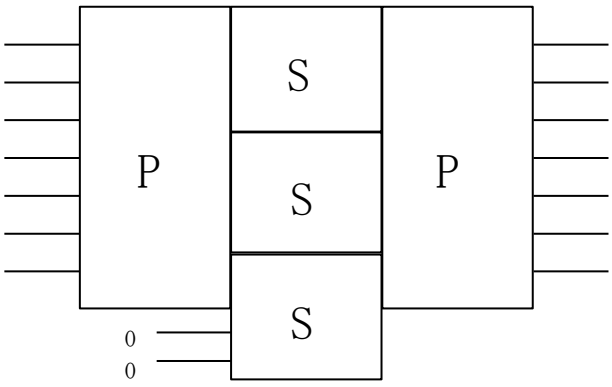
I [4,5 valores]

1.1. [1,5] Explique em que consiste o controlo da não-repudiação nos sistemas de segurança.

(Resposta: 5 linhas)

O controlo da não-repudiação é uma característica das assinaturas digitais que garante que o autor de um documento não possa negar que o assinou.

1.2. [3] Considere uma caixa P de 7 bits que opera com a chave "2604153" e uma caixa S de 3 bits que opera com a chave "51247630". 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 "1101110".

1101110 -(pbox)-> (00)1100111 -(sboxes)-> (11)0 100 011 -(pbox)-> **0010110**

(assume-se a convenção do livro adotado – bit menos significativo em cima, dígitos da chave referem-se aos bits de entrada; são possíveis outras interpretações)

II [3 valores]

2.1. [3] Aplique o algoritmo de Ziv-Lempel LZW para codificar a mensagem seguinte,

S="AABABCCBACBACBCCBABCABAA".

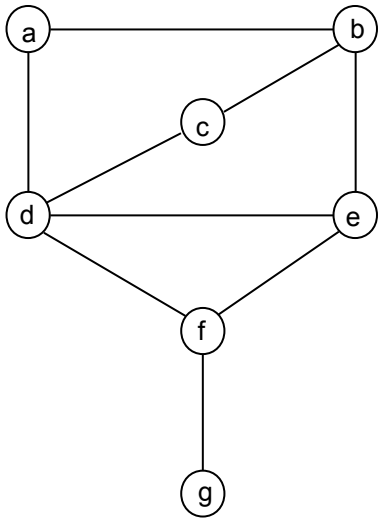
Calcule a taxa de compressão para a codificação obtida (suponha que cada caráter A,B,C requer 8 bits).

Input	Dicion.	Output
A	-	
A	AA	A
B	AB	A
A	BA	B
B	-	-
C	ABC	AB
C	CC	C
B	CB	C
A	-	-
C	BAC	BA
B	-	-
A	-	CB
C	AC	A
B	-	-
C	CBC	CB
C	-	-
B	CCB	CC
A	-	-
B	BAB	BA
C	BC	B
A	CA	C
B	-	-
A	ABA	AB
A	-	-
	-	AA

Taxa de compressão = (Tam. Input – Tam. Output)/Tam. Input = (24-16)/24=33,3%
(Outros valores possíveis, se o nº de bits da codificação de output for diferente do input, e se se considerarem marcadores de início e fim de mensagem).

III [4,5 valores]

3. Considere o grafo



3.1. [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 ativo/nº de iteração e os elementos da tabela a distância ao vértice inicial.

		1	2	3	4	5	6	7
	init	a	b	d	c	e	f	g
a	0							
b	∞	1						
c	∞	∞	2	2				
d	∞	1	1					
e	∞	∞	2	2	2			
f	∞	∞	∞	2	2	2		
g	∞	∞	∞	∞	∞	∞	3	

3.2. [1,5] Apresente uma *spanning tree* do grafo acima, que minimize o número de ligações entre nós.

Uma possibilidade entre muitas (o nº mínimo de ligações é 6):