Soluções

Unidade Curricular: 21045 – Estruturas de Dados e Algoritmos Avançados
Prova: Época de recurso, ano letivo de 2013/14, data de 2014/07/24

Grupo I [6 valores]

1.1 [2]

Os algoritmos de cifra têm como objetivo ocultar o conteúdo da mensagem enquanto as assinaturas digitais pretendem garantir a autoria das mensagens assim como a sua não repudiação e integridade.

1.2.1 [2]

```
Tabela da caixa P        Tabela da caixa S
bits entrada 6245 1037   palavra entrada 0123 4567 89AB CDEF
bits saída   0123 4567   palavra saída   62F7 AB10 D9CE 5348

Caixa P
bits      7654 3210
entrada X 0001 0111
saída   Y 0011 0110

Caixas S
bits      7654 3210
entrada Y 0011 0110
saída   Z 0111 0001
```

1.2.2 [2]

Partindo das tabelas das caixas P e S, trocando a entrada pela saída (troca de linhas) obtém-se a correspondência entrada/saída das caixas inversas,

```
caixa P-1                caixa S-1
bits entrada 0123 4567   palavra entrada 62F7 AB10 D9CE 5348
bits saída   6245 1037   palavra saída   0123 4567 89AB CDEF
```

reordenando as colunas de modo a obter a forma padrão convencionada para as chaves,

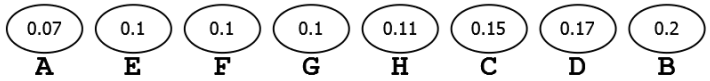
```
Tabela da caixa P-1      Tabela da caixa S-1
bits entrada 5416 2307   palavra entrada 0123 4567 89AB CDEF
bits saída   0123 4567   palavra saída   761D EC03 F945 A8B2

Caixas S-1
bits      7654 3210
entrada Z 1010 1001
saída   Y 0100 1001
```

```
Caixa P-1
bits      7654 3210
entrada Y 0100 1001
saída   X 0110 1000
```

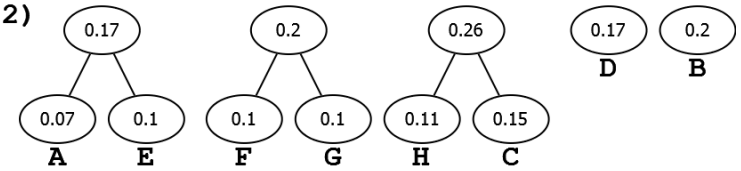
Grupo II [8 valores]

2.1 [3]

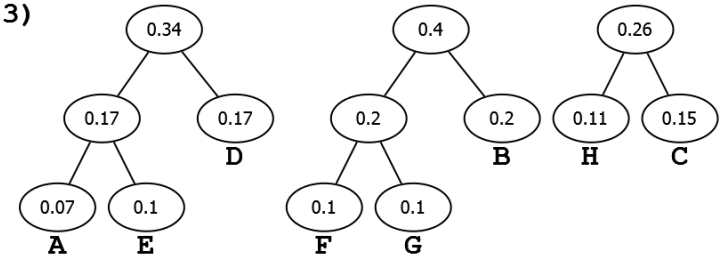
1)



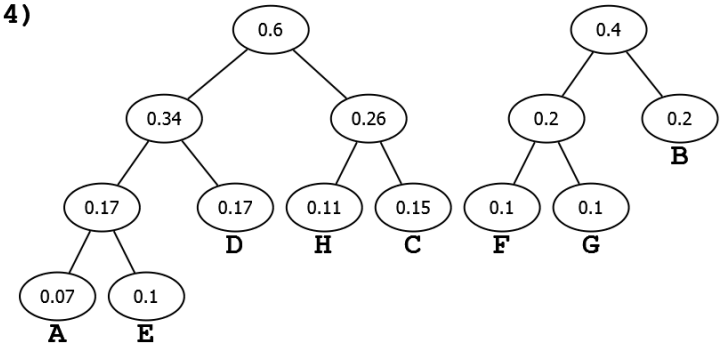
2)



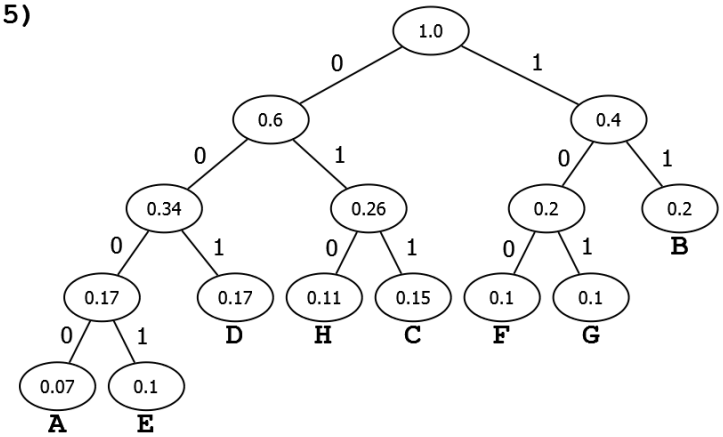
3)



4)



5)



Símbolo	Codificação de Huffman
A	0000
E	0001
D	001
H	010
C	011
F	100
G	101
B	11

2.2 [3]

Codificação LZW			
Entrada	Saída	Tabela	
		Índice	Palavra
D	—	1	A
A	4	2	B
DA	1	3	C
B	6	4	D
A	2	5	E
C	1	6	DA
DA	3	7	AD
D	6	8	DAB
BA	4	9	BA
CD	9	10	AC
E	11	11	CD
EE	5	12	DAD
BAC	16	13	DB
E	14	14	BAC
A	5	15	CDE
A	1	16	EE
B	1	17	EEB
CD	2	18	BACE
D	11	19	EA
DB	4	20	AA
CD	13	21	AB
AB	11	22	BC
BA	21	23	CDD
B	9	24	DD
BAB	2	25	DBC
AC	28	26	CDA
—	10	27	ABB
	—	28	BAB
		29	BB
		30	BABA

Nota: Na coluna da entrada, ocorre mudança de linha quando o próximo símbolo (1º da linha seguinte) completa uma palavra nova do dicionário.

2.3 [2]

Mensagem= C,CCCC,CA,B,CCA,AB,CCAAC,AABCCA,AAAAC,AB (as vírgulas separam a contribuição de cada tripla)

Descodificação LZ77		
Buffer Procura 7←0	Look-ahead buffer (Saída)	Triplas (Entrada)
	C	(0,0,C)
C	CCCC	(0,3,C)
CCCCC	CA	(2,1,A)
CCCCCCA	B	(0,0,B)
CCCCCCAB	CCA	(4,2,A)
CCCABCCA	AB	(0,1,B)
CABCCAAB	CCAAC	(4,4,C)
AABCCAAC	AABCCA	(7,5,A)
ACAABCCA	AAAAC	(0,4,C)
CCAAAAAC	AB	(2,1,B)

Grupo III [6 valores]

3.1 [2]

Exemplo de pseudocódigo (com ou sem especificação vértice inicial):

```
DepthFirstSearch(v0)
   para todos os vertices v
      num(v)=0;
   i=1;
   DFS(v0);
   enquanto existe vertice v com num(v)=0
      DFS(v)
end

DFS(v)
   num(v)=i;
   i=i+1;
   para todos os vertices u adjacentes a v
      Se num(u)=0
         DFS(u);
end
```

Ordem de visita: b, a, c, d, f, e, h, g, i, j.

4.1 [0,5]

Grafo simples, orientado (digrafo), ponderado.

4.2 [0,5]

Matriz de Adjacências										
	a	b	c	d	e	f	g	h	i	j
a	0	1	1	1	0	0	0	0	0	0
b	0	0	0	0	1	0	0	0	0	0
c	0	1	0	0	0	1	0	0	0	0
d	0	0	0	0	1	0	1	0	0	0
e	0	0	0	0	0	0	0	1	0	0
f	0	0	0	1	1	0	1	0	1	0
g	0	0	0	0	1	0	0	1	0	0
h	0	0	0	0	0	0	0	0	0	1
i	0	0	0	0	0	0	1	1	0	1
j	0	0	0	0	0	0	0	0	0	0

4.2 [3]

Ordem das arestas: ab, ac, ad, be, cb, cf, de, dg, eh, fd, fe, fg, fi, ge, gh, hj, ig, ih, ij

Algoritmo de Ford					
Vértice	**Iteração**				
	0	1		2	3
a	0				
b	∞	2	0		
c	∞	1			
d	∞	1			
e	∞	3	-1		
f	∞	2			
g	∞	4	3		
h	∞	4		0	
i	∞	3			
j	∞	5	4	1	

A distância mais curta entre o vértice `a` e o vértice `j` é 1. O caminho é a, c, f, e, h, j.

FIM