# AED3

Segunda prova - 06 de junho de 2017

23,5
25 pontos

NOME: Gabriel Luciano Gomes

1) Considere o seguinte alfabeto usado em um sistema de criptografia: (5 pontos)

| 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 | _ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 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 |

O símbolo _ equivale ao espaço em branco.

x mod 87

a) Cifre a mensagem A RA ARRANHA A ARANHA usando a cifra de Vigenère e a chave BOLA.

A_RA_ARRANHA_A_ARANHA
BOLABOLABOLABOLABOLA

CHAVE → BOLA
1 14 11 0

0 26 17 0 26 0 17 17 0 13 7 0 26 0 26 0 17 0 13 7 0
1 14 11 0 1 14 11 0 1 14 11 0 1 14 11 0 1 14 11 0 1
1 13 1 0 0 0 1 17 1 0 13 0 0 14 10 0 13 14 24 7 1

BNBAAOBRBASAAOKASOYHB

2,5

b) Cifre a mensagem A RA ARRANHA A ARANHA usando a cifra de colunas e a chave BOLA.

2 4 3 1

| B | O | L | A |
|---|---|---|---|
| A | _ | R | A |
| _ | A | R | R |
| A | N | H | A |
| _ | A | _ | A |
| R | A | N | H |
| A | | | |
| | | | |
| | | | |

ARAAHA_A_RARRH_N_ANAA

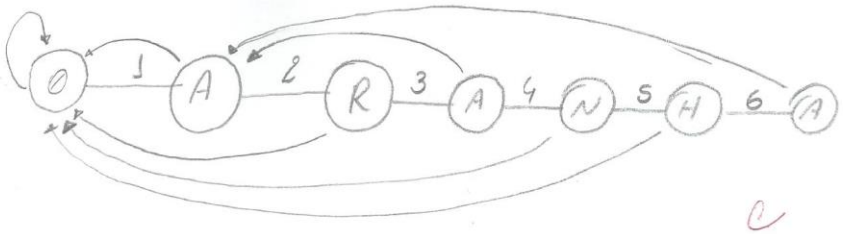
2,5

2) Explique, com base na criptografia, como funciona a assinatura digital. (5 pont

O documento passa por uma função hash, que gera uma mensagem. Essa mensagem é criptografada com uma chave privada e então concatenada ao documento. A pessoa que recebe o documento passa o documento por uma mesma hash para recolhimento da mensagem que contém a assinatura e então à descriptografa com uma chave pública, ao mesmo tempo que também é descriptografada com uma chave privada da recebedora. Caso os duas assinaturas sejam iguais, a assinatura é legítima e a operação/transação é realizada

4,0

3) Crie um diagrama de estados para a *string* ARANHA para reconhecimento de padrões por KMP. Mostre a sequência de estados percorrida para o reconhecimento dessa *string* no texto A RA ARRANHA A ARANHA. (5 pontos)




5,0

| | A | | R | A | | A | R | R | A | N | H | A | | A | | A | R | A | N | H | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Estados | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 2 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

Usando o algoritmo de Boyer-Moore, faça o reconhecimento de todas as ocorrências do padrão ARANHA no texto A RA ARRANHA A ARANHA. A cada passo, indique o deslocamento por caráter ruim (D.C.R.) e o deslocamento por sufixo bom (D.S.B.) calculados. Considere os espaços entre as palavras como caracteres normais. (5 pontos)

| A | | R | A | | A | R | R | A | N | H | A | | A | | A | R | A | N | H | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

ARANHA

ARANHA

ARANHA

ARANHA

ARANHA

| D.C.R. | D.S.B. |
|---|---|
| 5 | 3 |
| 3 | 1 |
| 5 | 3 |
| 2 | 1 |
| | |
| | |
| | |
| | |
| | |
| | |

4.5

5) Calcule a distância de edição entre os padrões ARANHA e BARANGA. (5 pontos)

| | | A | R | A | N | H | A |
|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| B | 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| A | 2 | 1 | 2 | 2 | 3 | 4 | 5 |
| R | 3 | 2 | 1 | 2 | 3 | 4 | 5 |
| A | 4 | 3 | 2 | 1 | 2 | 3 | 4 |
| N | 5 | 4 | 3 | 2 | 1 | 2 | 3 |
| G | 6 | 5 | 4 | 3 | 2 | 2 | 3 |
| A | 7 | 6 | 5 | 4 | 3 | 3 | 2 |

2 distância de edição

5.0