

1. (valor 2.5 pontos)

Ache a mensagem para o texto cifrado KMYGKMDP com o algoritmo RSA, tendo a mensagem agrupada em blocos de 2 e usando a tabela dada no cabeçalho. Use $p = 17$, $q = 89$ e $d = 3$.

Mesmo procedimento feito em aula para encriptação é feito também para a decriptação.

R: ACROACIA

$$N = p \cdot q = 17 \cdot 89 = 1513$$

$$KM \rightarrow 11 \cdot 27 + 13 = 310$$

$$YG \rightarrow 25 \cdot 27 + 7 = 682$$

$$KM \rightarrow 11 \cdot 27 + 13 = 310$$

$$DP \rightarrow 4 \cdot 27 + 16 = 124$$

$$RSA(310, 3) \rightarrow 310^3 \pmod{1513} = 30$$

$$RSA(682, 3) \rightarrow 682^3 \pmod{1513} = 501$$

$$RSA(310, 3) \rightarrow 310^3 \pmod{1513} = 30$$

$$RSA(124, 3) \rightarrow 124^3 \pmod{1513} = 244$$

$$30 = 1 \cdot 27 + 3 = "AC"$$

$$501 = 18 \cdot 27 + 15 = "RO"$$

$$30 = 1 \cdot 27 + 3 = "AC"$$

$$244 = 9 \cdot 27 + 1 = "IA"$$

$$\begin{array}{r} 30 \longdiv{27} \\ 3 \quad \quad \quad 1 \\ \hline \end{array} \rightarrow A$$

$$\rightarrow C$$

$$\begin{array}{r} 501 \longdiv{27} \\ 15 \quad \quad \quad 18 \\ \hline \end{array} \rightarrow R$$

$$\rightarrow O$$

$$\begin{aligned} I &= 0 \\ A &= 1 \\ B &= 2 \\ C &= 3 \\ D &= 4 \\ E &= 5 \\ F &= 6 \\ G &= 7 \\ H &= 8 \\ I &= 9 \\ J &= 10 \\ K &= 11 \\ L &= 12 \\ M &= 13 \end{aligned}$$

$$\begin{aligned} N &= 14 \\ O &= 15 \\ P &= 16 \\ Q &= 17 \\ R &= 18 \\ S &= 19 \\ T &= 20 \\ U &= 21 \\ V &= 22 \\ W &= 23 \\ X &= 24 \\ Y &= 25 \\ Z &= 26 \end{aligned}$$

H → 8

2. (valor 2.5 pontos)

Considere a construção de Merkle-Damgard, com a função $f(x, y) = x^2 + y^2 \pmod{27}$.

Usando $y_0 = E$ responda:

5

- (a) Calcule $H(\text{JAVA})$. R: 'W'
- (b) Calcule uma colisão para a palavra JAVA. R. _JAVA_
- (c) Ache $x \in \mathcal{M}$ tal que $H(x) = Q$. R. $x = 'S'$

OBS: Agrupe em blocos de 1.

a) $H(\text{JAVA}) = f(x, y) =$

$$\begin{aligned} &= 10^2 + 5^2 \pmod{27} = 17 \neq Q \\ &= 1^2 + 17^2 \pmod{27} = 20 = T \\ &= 2^2 + 20^2 \pmod{27} = 20 = T \\ &= 1^2 + 20^2 \pmod{27} = 23 = \boxed{W} \end{aligned}$$

$$\begin{aligned} 484 + 400 &= 884 \boxed{27} \\ 1 + 400 &= 401 \boxed{27} \end{aligned}$$

b) $H(_\text{JAVA}_) = f(x, y) =$

$$\begin{aligned} &= 0^2 + 5^2 \pmod{27} = 25 = Y \\ &= 10^2 + 25^2 \pmod{27} = 23 = W \\ &= 1^2 + 23^2 \pmod{27} = 17 = Q \\ &= 2^2 + 17^2 \pmod{27} = 17 = Q \\ &= 1^2 + 17^2 \pmod{27} = 20 = T \\ &= 0^2 + 20^2 \pmod{27} = 22 = \boxed{V} \end{aligned}$$

$$484 + 289$$

Não cheguei no resultado do professor.
minha colisão deu o mesmo resultado de W.

c.)

3. (valor 2.5 pontos)

Encripte a palavra PYTHON com o algoritmo RSA, tendo a mensagem agrupada em blocos de 2 e usando a tabela dada no cabeçalho. Use $p = 17$, $q = 67$ e $e = 5$.

R: JDQD?Y

$$PY \rightarrow 16 \times 27 + 25 = 457$$

$$TH \rightarrow 20 \times 27 + 8 = 548$$

$$ON \rightarrow 15 \times 27 + 14 = 419$$

$$N = p * Q = 17 * 67 = 1139$$

$$RSA(457, 5) \rightarrow 457^5 \pmod{1139} = 274$$

$$RSA(548, 5) \rightarrow 548^5 \pmod{1139} = 463$$

$$RSA(419, 5) \rightarrow 419^5 \pmod{1139} = 1132$$

$$274 = (274 / 27 = 10 \text{ com } \text{mod } 4) \quad \begin{array}{r} \boxed{1} \\ \times 27 + \boxed{4} = JD \end{array} \quad \begin{array}{r} 274 \mid 27 \\ \hline 10 \\ \boxed{4} \end{array} \rightarrow J$$

$$463 = 17 \cdot 27 + 4 = QD$$

$$1132 = 41 \cdot 27 + 25 = ?Y$$

4. (valor 2.5 pontos)

Responda com clareza as questões abaixo

- (a) O algoritmo de hash do exercício 2 é seguro contra a segunda pré-imagem? R: Não, pelo exercício b).
- (b) O algoritmo de encriptação baseado no RSA usando p e q pequenos é seguro? R: Não, pois, é fácil achar a decomposição em fatores primos de N.