Trabalho 3 — Bruna Magna da Cruz, 11218813

① Calcular $[8^{-1}]_{3023}$

Como 3023 é primo, $\mathbb{Z}_{3023}$ é corpo e portanto 8^{-1} possui inverso.

Então,

MCD(3023, 8) $\quad 3023 = 377 \cdot 8 + 7 \quad \langle 7 = 3023 - 377 \cdot 8 \rangle$

MCD(8, 7) $\quad 8 = 7 \cdot 1 + 1$

MCD(7, 1) = 1

Queremos 1 como combinação linear de 3023 e 8: $1 = 3023s + 8t$

Temos que

$1 = 8 - 7 = 8 - (3023 - 377 \cdot 8) = 8 - 3023 + 377 \cdot 8 = -3023 + 378 \cdot 8$

$\Rightarrow 1 = (-1)3023 + 378 \cdot 8$. Logo, $t = 378$ e $s = -1$

Portanto, $[8^{-1}]_{3023} = [378]_{3023}$ // Note que: $[8]_{3023} \cdot [378]_{3023} = [3024]_{3023} = [1]_{3023}$

② $2^{74} + 3^{74} \Rightarrow (2^{74} + 3^{74}) \bmod 13$

$= [(2^{74} \bmod 13) + (3^{74} \bmod 13)] \bmod 13$

Como 13 é primo, podemos utilizar o Teorema de Fermat.

Temos que

$1 = 8 \cdot 7 = 8 - (3023 - 377 \cdot 8) = 8 - 3023 + 377 \cdot 8 = -3023 + 378 \cdot 8$

$\Rightarrow 1 = (-1)\,3023 + 378 \cdot 8$ Logo, $i = 378$ e $j = -1$

Portanto, $[8^{-1}]_{3023} = [378]_{3023}$ Note que $[8]_{3023} \cdot [378]_{3023} = [3024]_{3023} = [1]_{3023}$

(2) $2^{74} + 3^{74} \Rightarrow (2^{74} + 3^{74}) \bmod 13$

$= [(2^{74} \bmod 13) + (3^{74} \bmod 13)] \bmod 13$

Como 13 é primo, poderos aplicar o Teorema de Fermat

- $2^{74} \bmod 13$

Por Fermat, $2^{12} \bmod 13 = 1$

Como $74 = 12 \cdot 6 + 2$, $2^{74} \bmod 13 = 2^2 \bmod 13 = 4$

- $3^{74} \bmod 13$

Por Fermat, $3^{12} \bmod 13 = 1$

Como $74 = 12 \cdot 6 + 2$, $3^{74} \bmod 13 = 3^2 \bmod 13 = 9$

Logo, temos que

$[(2^{74} \bmod 13) + (3^{74} \bmod 13)] \bmod 13 = (4+9) \bmod 13 = 13 \bmod 13 = 0$

3)

```
            Terminal
Seja (a)^(e) (mod d)
Digite o valor de (a): 343
Digite o valor de (e): 343
Digite o valor de (d): 7387
O valor de (343)^(343) (mod 7387) é 6385
```

4)

```
p = 113
q = 281
e = 19
f = 28059
```

```
            Terminal
Digite a mensagem: 8813
Mensagem codificada: 27684
Mensagem decodifica: 8813
```

(5) Exercícios da Lista 4

6) Como n é um valor "fácil" de ser fatorado computacionalmente, podemos descobrir os primos p e q que o formam.

Fatorando, temos que: $n = 1241 = 17 \cdot 73$ e como, pelo Teorema da Fatoração Única (5.1), esta fatoração é única, $p = 17$ e $q = 73$

Seja $\phi = (17-1)(73-1) = 16 \cdot 72 = 1152$

Logo $f = [e^{-1}]_{1152} = [5^{-1}]_{1152} = [461]_{1152}$

Para descriptografar, mensagem $= c^{f} \pmod{n}$

$\Rightarrow$ mensagem $= 695^{461} \pmod{1241}$

Utilizando o código do exercício 3, mensagem = 444

7) Análogo ao 6.

Fatorando $n = 1247$, temos que $1247 = 29 \cdot 43$, logo $p = 29$ e $q = 43$

Seja $\phi = (29-1) \cdot (43-1) = 28 \cdot 42 = 1176$

Logo, $f = [e^{-1}]_{1176} = [17^{-1}]_{1176} = [761]_{1176}$

$\Rightarrow$ mensagem: $695^{461} \pmod{1241}$

Utilizando o código do exercício 3, mensagem: 444

7) Análogo ao 6.

Fatorando $n = 1247$, temos que $1247 = 29 \cdot 43$, logo $p = 29$ e $q = 43$

Seu $\phi = (29-1)\cdot(43-1) = 28 \cdot 42 = 1176$

Logo, $f = [e^{-1}]_{1176} = [17^{-1}]_{1176} = [761]_{1176}$

Portanto mensagem: $c^f \pmod{n} = 430^{761} \pmod{1247} = 645$, pois queremos assinar a mensagem 460 ou seja, aplicar a função com os valores setados.

8)

Seu $n = pq$ e $\phi = (p-1)(q-1)$, temos $\phi = pq - p - q + 1 = n - p - q + 1$

Logo, $\phi = n - p - q + 1 \Rightarrow p = n + q - \phi + 1$ e como $n = pq \Rightarrow n = q(n - q - \phi + 1) = q(n-\phi) + q - q^2$

Substituindo

$1741441 = (1741441 - 1734232)q + q - q^2$

$2760q - q^2 - 1741441 = 0 \Rightarrow q = 1783$ ou $q = 977$

Como é análogo para p, podemos dizer $p = 1783$ e $q = 977$.

⑥ 11) Utilizando o Teste de Miller-Rabin

• $d = 645$

644	2
322	2
161	

Logo, $645 = 2^2 \cdot 161 + 1$

Escrevendo a sequência $b^{2^i \cdot q} \pmod d$: $i = 0, \dots, k$ temos: $b^{161} \pmod d$, $b^{322} \pmod d$, $b^{644} \pmod d$

Com $b = 2$ e $i = k = 2$, temos $2^{644} \pmod{645} = 1$. Vamos então analisar as duas propriedades do Teste de Miller-Rabin:

$2^{161} \pmod{645}$ $\quad$ $2^{322} \pmod{645}$ $\quad$ $2^{644} \pmod{645}$

257 $\quad$ 259 $\quad$ 1

Como a sequência não começa por 1 nem vale $d-1 = 644$ antes do primeiro 1, $d = 645$ é composto

• Além disso, como $2^{644} \pmod{645} = 1$, 645 é pseudoprimo em relação à base 2

Com $b = 3$ e $i = k = 2$, temos $3^{644} \pmod{645} = 36$, então é simplesmente composto em relação à base 3.

· Além disso, como $2^{644} \pmod{645} = 1$, 645 é pseudoprimo em relação à base 2

Com $b=3$ e $i=k=2$, temos $3^{644} \pmod{645} = 36$, então é simplesmente composto em relação à base 3.

· d = 613

612 | 2 Logo $613 = 2^2 \cdot 153 + 1$

306 | 2

153

A sequência será $b^{153} \pmod d$, $b^{306} \pmod d$, $b^{612} \pmod d$

Com $b=2$, e $i=k=2$, temos $2^{612} \pmod{613} = 1$ Vamos analisar o Teste de Miller-Rabin

$2^{153} \pmod{613}$ $2^{306} \pmod{613}$ $2^{612} \pmod{613}$

578 612 1

Como TMR pois a sequência vale 613-1 antes do primeiro 1, d = 613 é fortemente pseudo primo com respeito a base 2

Com $b=3$ e $i=k=2$, temos $3^{612} \pmod{613} = 1$ Por Miller-Rabin

$3^{153} \pmod{613} = 612$ $3^{306} \pmod{613} = 1$ $3^{612} \pmod{613} = 1$

Como TMR vale, d = 613 é fortemente pseudoprimo com respeito à base 3.

• $d = 1105$

1104	2	Logo, $1105 = 2^4 \cdot 69 + 1$
552	2	Fazendo $b=2$ e $i=k=4$, $2^{1104} \pmod{1105} = 1$ Por Miller-Rabin,
276	2	$2^{69} \text{ M } 1105$ $2^{138} \text{ M } 1105$ $2^{276} \text{ M } 1105$ $2^{552} \text{ M } 1105$ $2^{1104} \text{ M } 1105$
138	2	967 259 781 1 1
69		Como TMR não vale, $d = 1105$ é pseudoprimo em relação a base 2.

Com $b=3$ e $i=k=4$ $3^{1104} \pmod{1105} = 1$ Vamos analisar por Miller-Rabin,

$3^{69} \text{ M } 1105$ $3^{138} \text{ M } 1105$ $3^{276} \text{ M } 1105$ $3^{552} \text{ M } 1105$ $3^{1104} \text{ M } 1105$

1093 144 846 781 1

Logo como TMR não vale, $d = 1105$ é pseudoprimo em relação a base 3.

Portanto 1105 é composto por Miller-Rabin

• $d = 121$

120	2	Logo, $121 = 2^3 \cdot 15 + 1$
60	2	Fazendo $b=2$ e $i=k=3$, $2^{120} \pmod{121} = 56$. Logo, $d = 121$ é composto.
30	2	Analogamente, $b=3$ e $i=k=3$, $3^{120} \pmod{121} = 1$. Analisando por Miller-Rabin
15		$3^{15} \text{ M } 121$ $3^{30} \text{ M } 121$ $3^{60} \text{ M } 121$ $3^{120} \text{ M } 121$
		1 1 1 1

Como TMR vale $d = 121$ é fortemente pseudoprimo em relação a base 3 (mas é

• d: 121

120 | 2 Logo $121 = 2^3 \cdot 15 + 1$

60 | 2 Fazendo b=2 e i=k=3, $2^{120} \pmod{121} = 56$ logo, d: 121 é composto.

30 | 2 Analogamente b=3 e i=k=3, $3^{120} \pmod{121} = 1$ Analisando por Miller-Rabin

15 | $3^{15} \pmod{121}$ $3^{30} \pmod{121}$ $3^{60} \pmod{121}$ $3^{120} \pmod{121}$

1 1 1 1

Como TMR vale, d: 121 é fortemente pseudoprimo em relação a base 3 (mas é composto pela base 2).

• d: 223

222 | 2 Logo, $223 = 2 \cdot 111 + 1$

111 | Fazendo b: 2 e i=k=1, $2^{222} \pmod{223} = 1$ Analisando Miller-Rabin,

$2^{111} \pmod{223}$ $2^{222} \pmod{223}$

1 1

Por TMR vale, d: 223 é fortemente pseudoprimo em relação a base 2

Com b=3 e i=k=1, $3^{222} \pmod{223} = 1$. Analisando por Miller-Rabin,

$3^{111} \pmod{223}$ $3^{222} \pmod{223}$

222 1

Como TMR vale, d: 223 é fortemente pseudoprimo em relação a base 3 [illegible]

S T Q Q S S D

__/__/__

· $d = 703$

702	2
351	

Logo, $703 = 2 \cdot 351 + 1$

Fazendo $b = 2$ e $i = k = 1$, $2^{702} \pmod{703} = 628$, logo é certamente composto

Para $b = 3$ e $i = k = 1$, $3^{702} \pmod{703} = 1$. Analisando Miller-Rabin,

$3^{351} \quad M\ 703 \qquad 3^{702} \quad M\ 703$

$702 \qquad\qquad 1$

Como tmb vale $d = 703$ é fortemente pseudoprimo em relação a base 3 (mas é composto pela base 2).