TNC

exame de recurso

21. jun' 2019

Parte I

1. $x^2 \equiv 90 \pmod{101}$ admite soluções sse $\left(\frac{90}{101}\right) = 1$.

Temos

$$\left(\frac{90}{101}\right) = \left(\frac{2 \times 3^2 \times 5}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3^2}{101}\right)\left(\frac{5}{101}\right)$$

$$= (-1) \times 1 \times \left(\frac{5}{101}\right) = -\left(\frac{5}{101}\right)$$

$101 \equiv -3 \pmod 8$
$\Rightarrow \left(\frac{2}{101}\right) = -1$

$\left(\frac{a^2}{p}\right) = 1$
a primo com p
(p primo ímpar)

Pela LRQ,

$$\left(\frac{5}{101}\right) = (-1)^{\frac{5-1}{2} \times \frac{101-1}{2}} \left(\frac{101}{5}\right)$$

$$= \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$101 \equiv 1 \pmod 5$

Logo, $\left(\frac{90}{101}\right) = -1$ e $x^2 \equiv 90 \pmod{101}$

não admite soluções.

2. $m = 727$

$b = 3$

$3^{60} \equiv 297 \pmod{727}$ $\quad 3^{360} \equiv 350 \pmod{727}$

? $3^{\frac{m-1}{2}} \equiv \left(\frac{3}{m}\right) \pmod m$?

$$3^{\frac{m-1}{2}} = 3^{\frac{726}{2}} = 3^{363} = (3^{60})^6 \times 3^3 \equiv 350 \times 3^3 \pmod{727}$$
$$\equiv 9450 \pmod{727}$$
$$\equiv -1 \pmod{727}$$

$$\left(\frac{3}{727}\right) \underset{\substack{\text{LRQ} \\ \text{mdc}(3,727)=1 \\ 3 \nmid 727}}{=} (-1)^{\frac{3-1}{2}\times\frac{727-1}{2}} \left(\frac{727}{3}\right) = (-1)^{363} \left(\frac{727}{3}\right) = -\left(\frac{1}{3}\right) =$$

$727 \equiv 1 \pmod 3$

$$= -\left(\frac{1^2}{3}\right) = -1$$

$\left(\frac{a^2}{p}\right)=1$

3.

Teste de Miller-Rabin: Sejam n ímpar e b tal que $\text{mdc}(b,n)=1$ e $1<b<n$. Sejam $s, t \in \mathbb{N}$, com t ímpar, tais que $n-1 = 2^s \cdot t$.

Se $b^t \equiv 1 \pmod n$ ou $b^{2^j t} \equiv -1 \pmod n$, para algum j t.q. $0 \leq j \leq s-1$, dizemos que n passa o teste para a base b.

Se n é composto, a probabilidade de n passar o teste de Miller para k bases é $< \frac{1}{4^k}$

$n = 57$

$n-1 = 56 = 2^3 \times 7 \qquad s=3,\ t=7$

Temos

$2 \equiv 2 \pmod{57}$

$2^2 \equiv 4 \pmod{57}$

$2^3 \equiv 8 \pmod{57}$

$2^4 \equiv 16 \pmod{57}$

$2^7 \equiv 8 \times 16 \pmod{57}$

$\equiv 14 \pmod{57}$

Assim, $2^t \not\equiv 1 \pmod{57}$ e $2^t \not\equiv -1 \pmod{57}$

É-nos dado que

$$2^{14} \not\equiv -1 \pmod{57} \text{ e } \quad 2^{28} \not\equiv -1 \pmod{57}$$

Assim,

$$2^{2 \cdot t} \not\equiv -1 \pmod{57}$$

e

$$2^{2^2 \times t} \not\equiv -1 \pmod{57}.$$

Assim, vimos que

$$2^{t} \not\equiv 1 \pmod{57} \text{ e que } \quad 2^{2^j \times t} \not\equiv -1 \pmod{57}$$

para todo j t.q. $0 \leq j \leq s-1$.

Portanto, 57 não passa o teste de Miller-Rabin para a base 2.

4. $n = 161 = pq$ com p, q primos distintos.

(a) $\sqrt{n} \approx 12{,}688$

$s = 13$

$s^2 - n = 13^2 - 161 = 8$ (não é um quadrado perfeito)

$s = 14$

$s^2 - n = 14^2 - 161 = 196 - 161 = 35$ (não é um quadrado perfeito)

$s = 15$

$s^2 - n = 15^2 - 161 = 225 - 161 = 64 = 8^2$

$t = \sqrt{s^2 - n} = 8$

$n = (15-8)(15+8) = 7 \times 23$

(b) $n = 161$

$(p-1)$ - Pollard $\quad mdc(63, n) = 7$

$\mathbb{Z}_{161}$

$b = 2$

$mdc(b-1, n) = 1$

$b^2 = 4$

$mdc(4-1, n) = 1$

$b^{3 \times 2} = 4^3 = 64$

$mdc(64-1, n) = mdc(63, n) = 7$

dado no enunciado

Logo, 7 é um divisor não trivial de n.

(c) $n = 143$

ρ - Pollard

$\mathbb{Z}_{143}$

$a = f(f(x_0)) = 26$

$b = f(x_0) = 5$

$mdc(26-5, n) =$
$= mdc(21, n) = 1$

dado

$a \equiv f(f(a)) \pmod{143}$
$\equiv 15 \pmod{143}$

$b \equiv f(b) \pmod{143}$
$\equiv 26 \pmod{143}$

$mdc(26-15, n) =$
$= mdc(11, n) = 11 \neq 1$

Assim, $11 \mid 143$

Temos que $143 = 11 \times 13$

5. Suponhamos que $n = pq$ e que conhecemos p e q. Sabemos que $\varphi(n) = (p-1)(q-1)$

Reciprocamente, suponhamos que conhecemos n e $\varphi(n)$. Pretendemos determinar p e q.

Temos

$$\varphi(n) = (p-1)(q-1) \Leftrightarrow$$

$$\Leftrightarrow \varphi(n) = pq - p - q + 1$$

$$\Leftrightarrow p+q = n - \varphi(n) + 1 \quad (1)$$

Além disso,

$$(p-q)^2 = (p+q)^2 - 4pq.$$

Suponhamos, sem perda de generalidade, que $p > q$. Então,

$$p - q = \sqrt{(p+q)^2 - 4pq}$$

$$= \sqrt{(n - \varphi(n) + 1)^2 - 4n} \quad (2)$$

Assim, conhecendo n e $\varphi(n)$, podemos determinar, por (1) e (2), $p+q$ e $p-q$. De seguida, calculamos p e q através de:

$$p = \frac{1}{2}\left((p+q) + (p-q)\right)$$

e

$$q = \frac{1}{2}\left((p+q) - (p-q)\right).$$

6. Admitamos que n é um pseudoprimo fraco de base 2. Então, n é composto e

$$2^{n-1} \equiv 1 \pmod{n}.$$

Como $2^{n-1} \equiv 1 \pmod{n}$, temos que $n \mid (2^{n-1} - 1)$, ou seja,

$$2^{n-1} - 1 = nk,$$

para algum k. Note-se que, sendo $2^{n-1} - 1$ ímpar, k também é ímpar.

Seja $N = 2^n - 1$. Temos que

$$N - 1 = 2^n - 1 - 1 = 2^n - 2 = 2 \cdot (2^{n-1} - 1)$$
$$= 2 \times \underbrace{(nk)}_{\text{ímpar}},$$

donde

$$N - 1 = 2^s \times t, \text{ com } s = 1 \text{ e } t = nk.$$

Mais,

$$2^t = 2^{nk} = (2^n)^k$$
$$\equiv 1 \pmod{N}.$$

$$2^n = (2^n - 1) + 1$$
$$= N + 1 \equiv 1 \pmod{N}$$

Como $2^t \equiv 1 \pmod{N}$, podemos afirmar que N passa o teste de Miller para a base 2.

Além disso, sendo n composto, n admite um divisor não trivial d. Assim, $2^d - 1 \mid 2^n - 1$, donde N é composto.

Portanto, N é um pseudoprimo forte de base 2.

Parte II

7. $p = 37$

Elgamal chave pública $(p, 2, 28)$

$r = 2$ r.p. de p $\qquad$ $\text{ord}_{37} 2 = \varphi(37) = 36$

Assim, $\mathbb{Z}_p^* = \langle r \rangle$

$b \equiv r^a \pmod p$ $\qquad$ $b = 28$

$\text{ind}_2 b = a \Rightarrow a = \text{ind}_2 28 = 34$

criptograma: $(21, 8)$

$\gamma = 21$
$\delta = 8$

mensagem original: $(\gamma^a)^{-1} \delta \pmod p$

$(\gamma^a)^{-1} = (21^{34})^{-1}$

$21 \equiv -16 \pmod{37} \Rightarrow (21^a)^{-1} \equiv ((-16)^a)^{-1} \pmod{37}$

$\Rightarrow (21^{34})^{-1} \cdot 8 \equiv ((-16)^{34})^{-1} \cdot 8 \pmod{37}$

$$((-16)^{34})^{-1} \times 8 \equiv ((-1)^{34} \times (16^{34}))^{-1} \times 8 \pmod{37}$$
$$\equiv (2^{4\times 34})^{-1} \times 8 \pmod{37}$$
$$\equiv ((2^{34})^4)^{-1} \times 2^3 \pmod{37}$$

$$2^{34} \equiv 28 \pmod{37}$$
$$\equiv -9 \pmod{37} \Rightarrow (2^{34})^4 \equiv (-9)^4 \pmod{37}$$
$$\Rightarrow (2^{34})^4 \equiv 3^8 \pmod{37}$$
$$\Rightarrow (2^{34})^4 \equiv 81 \times 81 \pmod{37}$$
$$\Rightarrow (2^{34})^4 \equiv 7 \times 7 \pmod{37}$$
$$\Rightarrow (2^{34})^4 \equiv 12 \pmod{37}$$

Assim

$$(\gamma^a)^{-1}\delta \equiv (12)^{-1} \times 2^3 \pmod{37}$$
$$\equiv 3^{-1} \times (2^2)^{-1} \times (2^2) \times 2 \pmod{37}$$
$$\equiv 3^{-1} \times 2 \pmod{37}$$
$$\equiv 13 \pmod{37}$$

$3^{-1} = 25$ em $\mathbb{Z}_{37}$

$25 \times 2 = 50 \equiv 13 \pmod{37}$

Assim, a mensagem original é 13

8.

$$(n, e) = (55, 3)$$

$n = 5 \times 11$

$\varphi(n) = 4 \times 10 = 40$

$3^4 \equiv 1 \pmod{40} \Rightarrow 3 \times 3^3 \equiv 1 \pmod{40}$

$\Rightarrow$ O inverso de 3 em $\mathbb{Z}_{40}$ é $3^3 = 27$

Assim, $d = 27$

cripto $= 8$

decifração: $\quad$ cripto$^{d} \pmod{n}$

$$8^{27} \equiv (2^3)^{27} \pmod{55}$$

$$\equiv 2^{81} \pmod{55}$$

Pelo Teo. Euler, sabemos que $\quad 2^{\varphi(55)} \equiv 1 \pmod{55}$

Assim, $\quad 2^{40} \equiv 1 \pmod{55}$

Portanto,

$$8^{27} \equiv 2^{40} \times 2^{40} \times 2 \pmod{55}$$

$$\equiv 2 \pmod{55}$$

e a mensagem decifrada é 2.