teste 27/maio/2019

1. $n = 2^4 \times 3 + 1 = 49$

$n - 1 = 2^4 \times 3$

$s = 4$
$t = 3$

base $b = 2$

n passa o teste de Miller para a base 2 se

$$b^t \equiv 1 \pmod{n}$$

ou

$$b^{2^j \times t} \equiv -1 \pmod{n}, \text{ para algum } j \text{ tal que } 0 \leq j \leq s-1 = 3$$

Temos que

$$2^3 \equiv 8 \pmod{n} \not\equiv \pm 1 \pmod{n}$$

$$2^{2\times 3} = (2^3)^2 \equiv 8^2 \pmod{49}$$
$$\equiv 15 \pmod{49}$$
$$\not\equiv -1 \pmod{49}$$

$$2^{2^2\times 3} = (2^{2\times 3})^2 \equiv 15^2 \pmod{49}$$
$$\equiv 225 \pmod{49}$$
$$\equiv 29 \pmod{49}$$
$$\not\equiv -1 \pmod{49}$$

$$2^{2^3\times 3} = (2^{2^2\times 3})^2 \equiv 29^2 \pmod{49}$$
$$\equiv 841 \pmod{49}$$
$$\equiv 8 \pmod{49}$$
$$\not\equiv -1 \pmod{49}.$$

Logo, 49 não passa o teste de Miller para a base 2

2. $(p-1)$ - Pollard

factorizar $n = 77$

$\mathbb{Z}_{77}$

$b = \mathbb{Z}_{77}\,(2)$

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

$b = 2$
$mdc\,(1, 77) = 1$

$2^2 = 4$
$mdc\,(3, 77) = 1$

$2^3 = 8$
$mdc\,(7, 77) = 7$ $\longrightarrow$ 7 é um fator não trivial de n

$77 : 7 = 11$

$n = 7 \times 77$

3. RSA

$(n, e) = (55, 3)$ $\qquad e \in \mathbb{Z}^*_{\varphi(n)}$

$\varphi(n) = \varphi(5 \times 11) = \varphi(5)\,\varphi(11) = 4 \times 10 = 40$

$d = e^{-1}$ em $\mathbb{Z}^*_{\varphi(n)}$

$3^4 \equiv 1 \pmod{40} \Leftrightarrow 3 \times 3^3 \equiv 1 \pmod{40}$
$\Leftrightarrow d = 3^3 \pmod{40} \Leftrightarrow d = 27$

cripto = 8

$$\text{mensagem} \equiv \text{cripto}^{d} \pmod{55}$$

$$\equiv 8^{27} \pmod{55}$$

$$8^2 = 64 \equiv 9 \pmod{55}$$

$$8^3 \equiv 8 \times 9 \pmod{55}$$

$$\equiv 72 \pmod{55}$$

$$\equiv 17 \pmod{55}$$

$$8^4 \equiv 9 \times 9 \pmod{55}$$

$$\equiv 26 \pmod{55}$$

$$8^7 \equiv 17 \times 26 \pmod{55}$$

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

$$8^{21} \equiv 8^7 \times 8^7 \times 8^7 \pmod{55}$$

$$\equiv 8 \pmod{55}$$

$$8^{27} \equiv 8^{21} \times 8^3 \times 8^3 \pmod{55}$$

$$\equiv 8 \times 8^3 \times 8^3 \pmod{55}$$

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

mensagem : 2

4. $p = 19$

$r = 2$ raiz primitiva de p

chave El Gamal

escolher a tal que $1 \leq a \leq p-1$

calcular $b \equiv r^a \pmod p$

$a = 9$

$r^3 \equiv 8 \pmod{19}$

$r^4 \equiv -3 \pmod{19}$

$$r^8 = r^4 . r^4 \equiv (-3)(-3) \pmod{19}$$
$$\equiv 9 \pmod{19}$$

$$r^9 = r . r^8 \equiv 2 \times 9 \pmod{19}$$
$$\equiv 18 \pmod{19} \qquad \underline{b = 18}$$

chave pública $(19, 2, 18) = (p, r, b)$

chave privada $9 = a$

cifrar mens $= 5$

escolher K t.q. $1 \leq K \leq p-2 = 17$

por ex: $K = 3$

$\gamma = r^3 \pmod p$

$\delta =$ mens $. \, b^3 \pmod p$

$\gamma = r^3 \pmod{p}$
$\equiv 8 \pmod{19}$

$\delta = 5 \times 18^3 \pmod{19}$

$\equiv 5 \times (-1)^3 \pmod{19}$

$\equiv -5 \pmod{19}$

$\equiv 14 \pmod{19}$

criptograma:
$(\gamma, \delta) = (8, 14)$

5. símbolo de Jacobi $\left(\frac{83}{235}\right)$ $235 = 5 \times 47$

mdc $(83, 235) = 1$

$$\left(\frac{83}{235}\right) = \left(\frac{83}{5}\right) \times \left(\frac{83}{47}\right)$$

$$\left(\frac{83}{5}\right) = \left(\frac{3}{5}\right) \underset{\text{LRQ}}{\underset{\downarrow}{=}} (-1)^{\frac{3-1}{2} \times \frac{5-1}{2}} \left(\frac{5}{3}\right) = \left(\frac{5}{3}\right) \underset{5 \equiv 2 \pmod 3}{\underset{|}{=}} \left(\frac{2}{3}\right) \underset{3 \equiv 3 \pmod 8}{\underset{\downarrow}{=}} -1$$

$$\left(\frac{83}{47}\right) \underset{83 \equiv 36 \pmod{47}}{\underset{\downarrow}{=}} \left(\frac{36}{47}\right) = \left(\frac{6^2}{47}\right) \underset{\left(\frac{a^2}{n}\right) = 1}{\underset{\downarrow}{=}} 1$$

Assim, $\left(\frac{83}{235}\right) = -1 \times 1 = -1.$

6. p primo ímpar

$\Rightarrow p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$

Pelo Critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

CASO 1: $p \equiv 1 \pmod 4$

Então, $p-1 = 4k$, para algum $k \in \mathbb{N}$. Nesse caso,

$$\frac{p-1}{2} = \frac{4k}{2} = 2k$$

e

$$(-1)^{\frac{p-1}{2}} = 1$$

CASO 2: $p \equiv 3 \pmod 4$

Então, $p-3 = 4k$, para algum $k \in \mathbb{N}$, pelo que $p-1 = 4k+2$. Nesse caso,

$$\frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$$

e

$$(-1)^{\frac{p-1}{2}} = -1.$$

No CASO 1, $\left(\frac{-1}{p}\right) \equiv 1 \pmod p$, pelo que $\left(\frac{-1}{p}\right) = 1$.

No CASO 2, $\left(\frac{-1}{p}\right) \equiv -1 \pmod p$, donde $\left(\frac{-1}{p}\right) = -1$.

7. Sabemos que $\# \mathbb{Z}_n^* = \varphi(n)$ e que qualquer conjunto de $\varphi(n)$ elementos invertíveis em $\mathbb{Z}_n$ e incongruentes entre si é um s.r.r.

Consideremos $S = \{r^1, r^2, \dots, r^{\varphi(n)}\}$.

Suponhamos que existem $i, j \in \{1, \dots, \varphi(n)\}$ tais que $r^i \equiv r^j \pmod{n}$. Sabemos que

$$r^i \equiv r^j \ (\text{mod } n) \Leftrightarrow i \equiv j \ (\text{mod } \text{ord}_n r) \Leftrightarrow$$

$$\Leftrightarrow i \equiv j \ (\text{mod } \varphi(n)) \underset{1 \leq i,j \leq \varphi(n)}{\Leftrightarrow} i = j. \text{ Assim,}$$

$r^i \not\equiv r^j \pmod{n}$, para $i, j \in \{1, \dots, \varphi(n)\}$ tais que $i \neq j$.

Logo, $\# S = \varphi(n)$ e S é formado por elementos incongruentes (módulo n) entre si. Portanto, S é um s.r.r. módulo n.