teste 29/maio/2019

1.

$n = 943$

$\sqrt{n} \approx 30,708$

$s = 31$

$s^2 - n = 31^2 - 943 = 961 - 943 = 18$ (não é quadrado perfeito)

$s \leftarrow s+1$

$s = 32$

$s^2 - n = 32^2 - 943 = 1024 - 943 = 81 = 9^2$

$t = \sqrt{s^2 - n} = 9$

$a = s - t = 32 - 9 = 23$

$b = s + t = 32 + 9 = 41$

$n = ab = 23 * 41$

23 e 41 são divisores não triviais de n

2. $n = 143$

ρ - Pollard

$x_0 = 2$

$f(x) = x^2 + 1$ $\quad \mathbb{Z}_n$

$a = f(f(x_0)) \pmod n$
$\equiv f(5) \pmod n$
$\equiv 26 \pmod n$

$b = f(x_0) \pmod n$
$\equiv 5 \pmod n$

$m.d.c.(a-b, n) = mdc(21, 143) = 1$

$$a \equiv f(f(a)) \pmod{143}$$
$$\equiv f(f(26)) \pmod{143}$$
$$\equiv ((26^2+1)^2+1) \pmod{143}$$
$$\equiv 15 \pmod{143}$$

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

$\operatorname{mdc}(26-15, 143) = \operatorname{mdc}(11, 143) = 11 \neq 1$

Logo, 11 é um fator não trivial de 143.

3. $p = 17$

$\operatorname{ind}_3 2 = 14$ módulo 17

(a) $17 \nmid (3^8 - 1) \iff 3^8 \not\equiv 1 \pmod{17}$

Sabemos que $3^{16} \equiv 1 \pmod{17}$, pelo T. Euler.

Assim,
$$(3^8)^2 \equiv 1 \pmod{17}.$$

Como 17 é primo, não existem raízes quadradas não triviais de 1 módulo 17. Logo,

$$3^8 \equiv \pm 1 \pmod{17}.$$

Portanto, $3^8 \equiv -1 \pmod{17}$.

Além disso, $\operatorname{ord}_{17} 3 \mid \varphi(17) = 16$. Logo, $\operatorname{ord}_{17} 3 \in \{1, 2, 4, 8, 16\}$. Vimos já que $\operatorname{ord}_{17} 3 \neq 8$. Além disso,

$3^1 \equiv 3 \pmod{17}$

$3^2 \equiv 9 \pmod{17}$

$$\begin{aligned} 3^4 = 3^2 \times 3^2 &\equiv 9 \times 9 \pmod{17} \\ &\equiv 81 \pmod{17} \\ &\equiv 13 \pmod{17} \end{aligned}$$

Assim, $\text{ord}_{17} 3 \notin \{1,2,4\}$.

Temos

$$\left.\begin{array}{l} \text{ord}_{17} 3 \in \{1,2,4,8,16\} \\ \text{ord}_{17} 3 \neq 8 \\ \text{ord}_{17} 3 \notin \{1,2,4\} \end{array}\right\} \Rightarrow \text{ord}_{17} 3 = 16$$

Assim, 3 é r.p. de 17.

b) $9^x \equiv 2 \pmod{17}$

$$\begin{aligned} &\Rightarrow \text{ind}_3 (9^x) \equiv \text{ind}_3 2 \pmod{16} \\ &\Rightarrow \text{ind}_3 9 \quad x \equiv \text{ind}_3 2 \pmod{16} \\ &\Rightarrow 2x \equiv 14 \pmod{16} \\ &\Rightarrow x \equiv 7 \pmod{8} \\ &\Rightarrow x \equiv 7 \pmod{16} \text{ ou } \\ &\qquad x \equiv 15 \pmod{16} \end{aligned}$$

soluções: x t.q. $x \equiv 7 \pmod{16}$
ou $x \equiv 15 \pmod{16}$

c) <u>Elgamal</u> chave pública : $(p,3,2)$

$(\gamma, \delta) = (2,5)$

$$b \equiv r^a \pmod{p} \Rightarrow \operatorname{ind}_r b = a$$

$$a = \operatorname{ind}_3 2 = 14$$

$$(r^a)^{-1} \cdot b \equiv (2^{14})^{-1} \times 5 \pmod{17}$$

$$\equiv 13^{-1} \times 5 \pmod{17}$$

$$\equiv 4 \times 5 \pmod{17}$$

$$\equiv 3 \pmod{17}$$

$$2^2 \equiv 4 \pmod{17}$$

$$2^4 \equiv 16 \pmod{17}$$

$$\equiv -1 \pmod{17}$$

$$2^{12} \equiv (2^4)^3 \pmod{17}$$

$$\equiv -1 \pmod{17}$$

$$2^{14} = 2^2 \times 2^{12} \equiv 4 \times (-1) \pmod{17}$$

$$\equiv 13 \pmod{17}$$

mensagem original: 3

4. $$\left(\frac{68}{129}\right) = \left(\frac{68}{3}\right) \cdot \left(\frac{68}{43}\right) = \left(\frac{2^2 \times 17}{3}\right)\left(\frac{2^2 \times 17}{43}\right) =$$

$129 = 3 \times 43$

$3, 43$ primos

$$= \underbrace{\left(\frac{2^2}{3}\right)}_{1}\left(\frac{17}{3}\right)\underbrace{\left(\frac{2^2}{43}\right)}_{1}\left(\frac{17}{43}\right) = \left(\frac{17}{3}\right)\left(\frac{17}{43}\right) =$$

$$= \underbrace{\left(\frac{2}{3}\right)}_{=-1} \cdot (-1)^{\frac{17-1}{2} \times \frac{43-1}{2}} \left(\frac{43}{17}\right) = -1 \times (-1)^{8 \times 21} \cdot \left(\frac{43}{17}\right) =$$

$$= -1 \times 1 \times \left(\frac{9}{17}\right) = -1 \times 1 \times \underbrace{\left(\frac{3^2}{17}\right)}_{=1}$$

$$= -1.$$

5. p, q primos

$n = pq$.

$\varphi(n)$ pode ser escrita como $\varphi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$.

De facto, $\varphi(n) = (p-1)(q-1)$

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

$\varphi(n)$: nº de nºs primos relativos com n inferiores a n

Logo, o nº de nºs não primos relativos com n inferiores a n é

$$n - n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right).$$

Logo, a probabilidade de x não ser primo com n é

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

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

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

$$= \frac{1}{p} + \frac{1}{q} - \frac{1}{pq}.$$

6. p primo ímpar

Pelo critério de Euler, se a é tal que $mdc(a,p)=1$,

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

Logo, para a t.q. $1 \leq a \leq p-1$, $mdc(a,p)=1$.

Portanto, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, para qualquer a, $1 \leq a \leq p-1$.

Assim, p passa o teste de primalidade probabilístico Solovay - Strassen