Chiffrement RSA

$$\boxed{\begin{aligned} p &= 47 \\ q &= 73 \end{aligned}}$$

CHIFFRER

DÉCHIFFRER

Clef privée (p, q, d)

Clef publique (n, e)

$\boxed{d \cdot e \equiv 1 \mod \phi(n)}$ $\quad pgdc(e; \underbrace{(p-1)(q-1)}_{\phi(n)}) = 1$

$e = 17$

$n = p \cdot q$ $\quad 3431$

clef publique : ✓

clef privée : · Vérifier que $\text{pgdc}(17; 46 \cdot 72) = 1$

· Calculer d : $\quad \underbrace{s \cdot 3312}_{\phi(n)} + t \cdot \underbrace{17}_{e} = 1$

$3312 \mod \phi(n) = 0$

$$1 \cdot 3312 + 0 \cdot 17 = 3312$$

$$0 \cdot 3312 + 1 \cdot 17 = 17$$

$$1 \cdot 3312 + (-194) \cdot 17 = 14$$

$$(-1) \cdot 3312 + 195 \cdot 17 = 3$$

$$\begin{array}{r|l} 14 & 3 \\ \hline 12 & 4 \\ \hline 2 & \end{array}$$

$$5 \cdot 3312 - 974 \cdot 17 = 2$$

0 mod 3312

$$-6 \cdot 3312 + \boxed{1169} \cdot 17 = 1$$

$$1169 \cdot 17 = 1 + 6 \cdot 3312$$

$$1169 \cdot e \equiv 1 \mod \phi(n)$$

$$\boxed{1169 = e^{-1} \mod \phi(n)}$$

$d = 1169$

Clef publique

$(3431 ; 17)$

Clef privée

$(47 ; 73 ; 1169)$

Soit $\boxed{m = 1234}$ inventé

$$C = m^e \mod n$$

$$C = 1234^{17} \mod 3431$$

$$17 = 16 + 1$$
$$= 16 + 0 + 0 + 0 + 1$$
$$2^4 \; 2^3 \; 2^2 \; 2^1 \; 2^0$$

$1234^1 \mod 3431 = 1234$ ✓

$1234^2 \mod 3431 = 2823$ ×

$1234^4 \mod 3431 = 2547$ ×

$1234^8 \mod 3431 = 2619$ ×

$1234^{16} \bmod 3431 = 592$ ✓

$1234^{17} = 1234^{16} \cdot 1234^{1}$

$\Rightarrow 1234^{17} \bmod 3431 = (1234 \cdot 592) \bmod 3431$

$= 3156$

On reçoit le chiffré : $\boxed{C = 454}$ inventé

$m = C^{d} \bmod n$

$454^{1169} \bmod \overset{n}{3431}$

$1169 = \underset{2^{10}}{1024} + 128 + 16 + 1$

$\underbrace{454^{1024} \cdot 454^{128} \cdot 454^{16} \cdot 454^{1}}_{\bmod 3431}$

$454^{1} \bmod 3431 = 454$

454^{2} 256

454^{4}	347
454^{8}	324
454^{16}	2046
454^{32}	296
454^{64}	1841
454^{128}	2884
454^{256}	712
454^{512}	2587
454^{1024}	2119

$$\underbrace{454 \cdot 2046}_{2514}$$

$$\underbrace{2514 \cdot 2884}_{673}$$

$$\underbrace{673 \cdot 2119}_{2222}$$

Le message est $\boxed{m = 2222}$

$n \in \mathbb{N}$ $\quad n \geq 2$ $\qquad 163$

n premier ?

1. Calculer $\sqrt{n}$

$$\boxed{n = a \cdot b}$$

$$\left.\begin{array}{l} a > \sqrt{n} \\ b > \sqrt{n} \end{array}\right\} \quad a \cdot b > \sqrt{n}\sqrt{n} = n$$

2. $12 < \sqrt{163} < 13$

3/5/7/11 ← À tester

$1+6+3 = 10 \Rightarrow 3 \nmid 163$

$5 \nmid 163$

$7 \cdot 20 = 140$ reste $23 \Rightarrow 7 \nmid 163$

$11 \cdot 14 = 154$ reste $9 \Rightarrow 11 \nmid 163$

$$\begin{array}{r|l} 163 & 11 \\ \cline{2-2} \underline{11} & 14 \\ 53 & \\ \underline{44} & \\ 9 & \end{array}$$

3. Conclure : 163 est premier

$\boxed{\text{Thm de Fermat:}}$

Soit p un premier et a un entier positif.

Si $p \nmid a$ alors

$$a^{p-1} \equiv 1 \mod p$$

Exemple : $p = 23 \quad a = 52$

$$52^{22} \underbrace{\mod 23}_{} = \left(52^{7}\right)^{3} \cdot 52 \mod 23$$

$$= 3^{3} \cdot 6 \mod 23$$

$$= 4 \cdot 6 \mod 23 = 24 \mod 23$$

$$= 1 \mod 23$$

$a \equiv 6 \mod n$

$$\underbrace{a \cdot c \mod n}_{\in \mathbb{Z}} = (a \mod n) \cdot (c \cdot \mod n)$$

Application : Inverse de $a \mod p$: $\quad \mathrm{pgdc}(a;p) = 1$

$$a^{p-1} \equiv 1 \mod p \Leftrightarrow a^{p-2} \cdot a \equiv 1 \mod p$$

$\Rightarrow$ L'inverse de a mod p est a^{p-2}

<u>Exemple</u> : Trouver l'inverse de 2 mod 11.

$$2^{10} \equiv 1 \bmod 11$$

$$\boxed{2^9} \cdot 2 \equiv 1 \bmod 11$$

$$2^9 = 2^8 \cdot 2 = (2^4)^2 \cdot 2$$

$16 \equiv 5 \bmod 11$

$$\begin{aligned} 2^9 \bmod 11 &= (2^4)^2 \cdot 2 \bmod 11 \\ &= 5^2 \cdot 2 \bmod 11 \\ &= 3 \cdot 2 \bmod 11 \\ &= 6 \bmod 11 \end{aligned}$$

$$\mathbb{Z}_5 = \{0; 1; 2; 3; 4\}$$

$\mathbb{Z}_p$ admet $p-1$ inversibles si p premier

Théorème d'Euler

Si n est un entier positif et que $\text{pgdc}(a; n) = 1$

alors $\boxed{a^{\phi(n)} \equiv 1 \mod n}$ pour $a \in \mathbb{Z}_n$

Exemple: $n = 15$

$\boxed{\phi(15) = (3-1)\cdot(5-1) = 8}$

$a = 7$

$a^8 \mod 15 = 1$

$7^8 \mod 15 = 1$ ✓

Thm RSA

$n = p \cdot q$

$e \cdot d \equiv 1 \mod \phi(n)$

$e \cdot d = 1 + k \cdot \phi(n)$

$m \in \mathbb{Z}_n$

$c = m^e \mod n$

$c^d \mod n = (m^e)^d \mod n$

$= m^{e \cdot d} \mod n$

$$= m^{1+k\cdot\phi(n)} \bmod n$$

$$= m \cdot m^{k\cdot\phi(n)} \bmod n$$

$$= m \cdot \left(m^{\phi(n)}\right)^{k} \bmod n$$

$$= m \cdot \left(\underbrace{m^{\phi(n)} \bmod n}_{=1 \text{ thm Euler}}\right)^{k} \bmod n$$

$$= m \bmod n$$