Crypto

RSA

$\mathbb{Z}_n = \{0; \dots; n-1\}$

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

$3 \cdot d \equiv 1 \mod 5$

$3 \cdot 2 = 6 \equiv 1 \mod 5$

m ← message

$m \in \mathbb{Z}_n$

c ← chiffre

$c \in \mathbb{Z}_n$

[def] p, q deux premiers ($\sim$ 1000 chiffres)

$n = p \cdot q$

$e = 17$ ou 65537

$2^{(2^2)} + 1$

Clef publique : $(n; e)$

Clef privée : $(p; q; d)$ ← inverse de e modulo $\varphi(n)$

$e \cdot d \equiv 1 \mod \underbrace{(p-1)(q-1)}_{\varphi(n)}$

$p = 5$

$q = 7$

$p - 1 = 4$

$q - 1 = 6$

$(p-1) \cdot (q-1) = 24$

$n = p \cdot q = 35$

$e = 17$

$17 \cdot d \equiv 1 \mod 24$ $\longrightarrow$ d

Euclide étendu

Chiffrer

Alice → Bob

(n, e) ← clef publique

$$E(m) = m^e \bmod n = c$$

Exponentiation modulaire

$$D(c) = c^d \bmod n$$

$$(m^e)^d \equiv m \bmod n$$

pgdc $2 > 6$

$$pgdc(2;6) = pgdc(6; 2 \bmod 6)$$

$pgdc(108; 68)$

$108 \bmod 68 = 40$

① $pgdc(68; 40)$

$68 \bmod 40 = 28$

② $pgdc(40; 28)$

③ $28/12$

④ $12/4$

⑤ $4/0$

TI 30

$3472 \bmod 1477 = 518$

$3472 \div 1477$

$3472 = 2 \cdot 1477 + 518$

$(3472; 1477) \rightarrow (1477; 518) \rightarrow (518; 441) \rightarrow (441; 77)$

$\rightarrow \ldots$

Euclide étendu a, b deux entiers positifs

$\exists\, s,t \in \mathbb{Z}$ tq. $a \cdot s + b \cdot t = pgdc(a;b)$

Exemple : $a=24$ $b=17$

$24 \cdot s + 17 \cdot t = 1$

$17 \cdot t = 1 - s \cdot 24$ $\quad 0 \bmod 24$

$\Rightarrow 17 \cdot t \equiv 1 \bmod 24$

t

L_1 $24 \cdot 1 + 17 \cdot 0 = 24$

L_2 $24 \cdot 0 + 17 \cdot 1 = 17$

L_3 $24 \cdot 1 + 17 \cdot (-1) = 7$

$7 - 2 \cdot 3 = 1$

L_4 $24 \cdot (-2) + 17 \cdot 3 = 3$

$24 \cdot 5 + 17(-7) = 1$

$24 - 1 \cdot 17 = 24 \bmod 17 = 7$

quotient, reste

$17 - 2 \cdot 7 = 3$

$L_4 \leftarrow L_2 - 2 \cdot L_3$

$17 \cdot (-7) = 1 - 24 \cdot 5$

$\downarrow$ mod 24

$17 \cdot 17 \equiv 1$

$p = 7$

$q = 13$

$n = 7 \cdot 13 = 91$

$e = 17$

Clef privée : $(7; 13; d)$

Clef publique : $(91; 17)$ ← e

$\varphi(n) = 6 \cdot 12 = 72$

Trouver d tq.

$e \cdot d = 17 \cdot d \equiv 1 \mod \varphi(n) = 72$

$72 \cdot 1 + 17 \cdot 0 = 72$

$72 \cdot 0 + 17 \cdot 1 = 17$

$72 \cdot 1 + 17(-4) = 4$

$72 \cdot (-4) + 17 \cdot 17 = 1$

$p = 13$ $\quad e = 17$

$q = 23$

$n = 13 \cdot 23 = 299$

$\varphi(n) = 12 \cdot 22 = 264$

$d \cdot e = d \cdot 17 \equiv 1 \mod 264$

Calcul de d

$264 \cdot 1 + 17 \cdot 0 = 264$

$r = 9 \quad q = 15$

$264 \cdot 0 + 17 \cdot 1 = 17$

$264 \cdot 1 + 17 \cdot (-15) = 9$

$-31 + 264 = 233$

$264 \cdot (-1) + 17 \cdot 16 = 8$

$264 \cdot 2 + 17 \cdot (-31) = 1$

$d \equiv -31 \mod 264$

$+264$

$d \equiv 233 \mod 264$

$\Rightarrow 17 \cdot (-31) = 1 - 264 \cdot 2$

$\Rightarrow 17 \cdot 233 \equiv 1 \mod 264$ $\quad \Rightarrow \boxed{d = 233}$

RSA: clef publique : $(299; 17)$ $\quad n = p \cdot q = 13 \cdot 23$

$(n; e)$

$\varphi(n) = (p-1)(q-1) = 264$

clef privée : $(13; 23; 233)$

chiffrer : $m \in \mathbb{Z}_{299} = \{0; 1; 2; \dots; 298\}$

$m = 54$

$c = 54^{17} \bmod 299$ $\quad \boxed{c = m^e \bmod n}$

$17 = 16 \cdot 1 + 8 \cdot 0 + 4 \cdot 0 + 2 \cdot 0 + 1 \cdot 1$

$17 = 16 + 1$

$c = 54^{16+1} \bmod 299$

$= 54^{16} \cdot 54^1 \bmod 299 = (54^{16} \bmod 299) \cdot (54^1 \bmod 299)$

$x = 16$ $\quad y = 54$

$x \cdot y \bmod 299$

$$54 \equiv 54 \mod 299$$

$$54^2 \equiv 225 \mod 299$$

$$54^4 \equiv 225^2 \equiv 94 \mod 299$$

$$54^8 \equiv 94^2 \equiv 165 \mod 299$$

$$54^{16} \equiv 165^2 \equiv 16 \mod 299$$

$$C = 16 \cdot 54 \mod 299 = \boxed{266} \mod 299$$

$$\boxed{C = 266}$$