20 II

OS

23 II

TEOS

6248

27 II — 29 II

MR

1 III

TEMR

2.6.2 à 2.6.19

2.8.1

2.8.4 à 2.8.6

2.8.9

2.8.12

TE crypto

Thm

EULER

$$a^{\varphi(m)} \equiv 1 \mod m$$

$\varphi(m)$: nombre d'inversibles

$\mathbb{Z}_m^*$: l'ensemble des inversibles

$|\mathbb{Z}_m^*|$: nombre d'éléments d'un ensemble

$$\varphi(m) = |\mathbb{Z}_m^*|$$

$m = p^2$

$\varphi(m) = p(p-1) = 3 \cdot 2$

$m = 9 \quad = 3 \cdot 3$

Exemple :

$$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$pgdc(a, 9) = 1$

$$8 \cdot x \equiv 1 \mod 9$$

$$9 \mid (8x - 1) \Leftrightarrow 8x - 1 = k \cdot 9$$

$$\Leftrightarrow \quad 8 \cdot x + k \cdot 9 = 1$$

$$9 = 1 \cdot 9 + 0 \cdot 8$$

$$8 = 0 \cdot 9 + 1 \cdot 8$$

$$1 = 1 \cdot 9 - 1 \cdot 8 \qquad 1 = k \cdot 9 + x \cdot 8$$

$k = 1 \quad x = -1$

$$\Rightarrow \quad (-1) \cdot 8 \equiv 1 \mod 9$$

$$\Leftrightarrow \quad 8 \cdot 8 \equiv 1 \mod 9 \qquad 64 = 1 + 7 \cdot 9$$

$1^6 \mod 9 = 1$

$2^6 \mod 9 \;/\; 64 \mod 9 = 1$

$4^6 \mod 9 = 1$

$5^6 \mod 9 = 1$

$7^6 \mod 9 = 1$

$8^6 \mod 9 \;/\; (8 \cdot 8)^3 \mod 9 = (1)^3 \mod 9 = 1$

$\mathbb{Z}_{15} = \{0, \ldots, 14\}$

$\mathbb{Z}_{3 \cdot 5}$

$15 = 3 \cdot 5$

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

8 inversibles

$11^8 \bmod 15 = 1$

$(3-1)(5-1)$

Clef RSA : $(n ; e)$ $\quad n = p \cdot q$

p premier, q premier — 300 chiffres

$m \in \mathbb{Z}_n$

Chiffrer : $c = m^e \bmod n$

Pour déchiffrer $\quad d \cdot e \equiv 1 \mod (p-1)(q-1)$

d existe

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

Déchiffrer : $c^d \bmod n =$

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

Construction

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

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

$\Leftrightarrow e \cdot d + k\,\varphi(n) = 1$

$m^{1 - k \cdot \varphi(n)} \bmod n =$

$\Leftrightarrow e \cdot d = 1 - k \cdot \varphi(n)$

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

$m \cdot 1^{-k} \bmod n = m \bmod n$

$a^{b-c} = a^b \cdot a^{-c}$

$a^{-x \cdot y} = \left(a^y\right)^{-x}$

(n_{beo}, e_{beo})

$n_{beo} = p_{beo} \cdot q_{beo}$

$(p_{beo}, q_{beo}, d_{beo})$

$\varphi(n_{beo}) = (p_{beo}-1)(q_{beo}-1)$

$m \in \mathbb{Z}_{n_{beo}}$

$c = \boxed{m^e \bmod n_{beo}}$ chiffre $\longrightarrow$ $c^{d_{beo}} \bmod n_{beo} = m$

$p = 23$
$q = 31$

$e = 17$

$n = p \cdot q$

c) Clef publique : $(713 ; 17)$

$d \cdot e \equiv 1 \mod (p-1)(q-1)$

17

$(p-1)(q-1) = 22 \cdot 30 = 660$

$5 \cdot 660 + (-) \cdot 17 = 1$

2)

$660 = 1 \cdot 660 + 0 \cdot 17$

$17 = 0 \cdot 660 + 1 \cdot 17$

$14 = 1 \cdot 660 - 38 \cdot 17$ $\quad L_3 = L_1 - 38 \cdot L_2$

$3 = -1 \cdot 660 + 39 \cdot 17$ $\quad L_5 = L_3 - 4 \cdot L_4$

$2 = 5 \cdot 660 - 194 \cdot 17$

$1 = -6 \cdot 660 + 233 \cdot 17$

660	17
	38
14	

b) Clef privée $(23 ; 31 ; 233)$

$233 \cdot 17 \equiv 1 \mod 660$

d) $333^{17} \mod 713$

$17 \leftrightarrow 10001$

EXPO RAPIDE

333	1	1
~~374~~	2	0
~~128~~	4	0
~~608~~	8	0
225	16	1

$333^2 = 110889$

$r = 333 \cdot 225 \equiv 60 \mod 713$

Alice → Bob : 60

$C = 333^A \mod 713$

$A = 60$

$$\varphi(p^k) = (p-1)\,p^{k-1}$$

$$\boxed{\varphi(p \cdot q) = (p-1)(q-1)}$$

RSA

$$\varphi(p^k \cdot q^l) = (p-1)\,p^{k-1}\,(q-1)\,q^{l-1}$$