04,02,20

Clé privée

p, q , $p \neq q$ premiers

$n = p \cdot q$

e tel que $pgcd(e, \varphi(n))$

Calculer d tel que

$$ed \equiv 1 \pmod{\varphi(n)}$$

d est la gâche secrète

d, n

Clé publique

n , e

Chiffrement $0 \leq m < n$: $c \equiv m^e \pmod{n}$

Déchiffrement $c^d \equiv (m^e)^d \equiv m^{ed} = m \pmod{n}$

La fonction $f(p,q) = pq$, où p et q sont deux grands nombre premiers, est une fonction à sens unique.
Il est en effet impossible de factoriser p et q en un temps réaliste

2.9.1 Chiffrer et déchiffrer le message $m = 8$ à l'aide du système RSA, avec $p = 7$, $q = 11$ et $e = 17$.

clé privée	$n = 77$
clé publique	$n = 77$ $\quad e = 17$

$n = p \cdot q = 77$ $\qquad \varphi(77) = 10 \cdot 6 = 60$ $\qquad$ et $\qquad$ $\text{pgcd}(60, 17) = 1$

Chiffrement $\qquad m = 8, \qquad c \equiv 8^{17} \equiv 8^{16} \cdot 8 \equiv 36 \cdot 8 \equiv 57 \pmod{77}$

$8^2 \equiv 64 \pmod{77}$

$8^4 \equiv 64^2 \equiv 15 \pmod{77}$

$8^8 \equiv 15^2 \equiv 71 \pmod{77}$

$8^{16} \equiv 71^2 \equiv 36 \pmod{77}$

Calculer d tel que $\qquad ed \equiv 1 \pmod{\varphi(n)}$

$17d \equiv 1 \pmod{60} \qquad \Leftrightarrow \qquad 17d + 60k = 1$

$17d + 60k = 1$

$17d \equiv 1 \pmod{60}$

Ligne	reste	$\cdot 60$	$\cdot 17$	Commentaires	q	Calcul de q	
1	60	1	0				
2	17	0	1	$9 = 60 - 3 \cdot 17$	3	$60 \div 17$	$60 = 3 \cdot 17 + 9$
3	9	1	-3	$8 = 17 - 1 \cdot 9$	1	$17 \div 9$	$17 = 1 \cdot 9 + 8$
4	8	-1	4	$1 = 9 - 1 \cdot 8$	1	$9 \div 8$	$9 = 1 \cdot 8 + 1$
5	1	2	-7				

$17 \cdot (-7) + 2 \cdot 60 = -119 + 120 = 1$

Donc $d = -7 \equiv 53 \pmod{60}$

$d = 53$ de la secrète

Déchiffrement :

$$C^d = 57^{53}$$

$53 = 32 + 16 + 4 + 1$

$$57^2 \equiv 15 \pmod{77}$$

$$57^4 \equiv 71 \pmod{77}$$

$$57^8 \equiv 36 \pmod{77}$$

$$57^{16} \equiv 64 \pmod{77}$$

$$57^{32} \equiv 15 \pmod{77}$$

$$57^{53} \equiv 15 \cdot 64 \cdot 71 \cdot 57 \equiv 8 \pmod{77}$$

2.9.2 Connaissant la clef publique (n, e) d'un individu, déterminer la clé privée d dans les cas suivants :

a) ~~$n = 1073, e = 115$;~~ impossible

b) $n = 1073, e = 115$; OK

c) $n = 111, e = 31$;

d) $n = 117, e = 17$;

e) $n = 105, e = 13$;

f) $n = 10001, e = 187$.

a) $n = 1073 = 29 \cdot 37$; $\varphi(n) = 28 \cdot 36 = 1008$

$\text{pgcd}(e, \varphi(n)) = \text{pgcd}(117, 1008) = 9$

b) $n = 1073 = 29, 37$; $\varphi(1073) = 1008$

$\text{pgcd}(115, 1008) = 1$

Calculer : $115 \cdot d \equiv 1 \pmod{1008}$

$115\, d + k \cdot 1008 = 1$

Ligne	reste	$\cdot 1008$	$\cdot 115$	Commentaires	q	calcul de q
1	1008	1	0			
2	115	0	1	$88 = 1008 - 8 \cdot 115$	8	$1008 \div 115$
3	88	1	-8	$27 = 1 \cdot 115 - 1 \cdot 88$	1	$115 \div 88$
4	27	-1	9	$7 = 88 - 3 \cdot 27$	3	$88 \div 27$
5	7	4	-35	$6 = 27 - 3 \cdot 7$	3	$27 \div 7$
6	6	-13	114	$1 = 1 \cdot 7 - 1 \cdot 6$	1	$7 \div 6$
7	1	17	-149			

On a $115(-149) + 17 \cdot 1008 = 1$

$115 \cdot 859 \equiv 1 \pmod{1008}$

$d = 859$

2.9.2 Connaissant la clef publique (n, e) d'un individu, déterminer la clé privée d dans les cas suivants :

a) ~~$n = 1073, e = 117;$~~ impossible

b) $n = 1073, e = 115$;

c) $n = 111, e = 31$;

d) $n = 117, e = 17$;

e) $n = 105, e = 13$;

f) $n = 10001, e = 187.$

a) $n = 1073 = 29 \cdot 37$; $\varphi(n) = 28 \cdot 36 = 1008$

$\text{pgcd}(e, \varphi(n)) = \text{pgcd}(117, 1008) = 9$

b) $n = 1073 = 29, 37$; $\varphi(1073) = 1008$

$\text{pgcd}(115, 1008)$ $\quad d = 859$