

## TD6 - Système RSA - *Corrigé*

### Exercice 1 :

1.  $\varphi(n) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1)$ . Donc,  $\varphi(2773) = \varphi(47) \times \varphi(59) = 46 \times 58 = 2668$ .
2. On sait que  $ed \equiv 1 [\varphi(n)]$ . Autrement dit,  $51d \equiv 1 [2668]$ . On résout Bezout pour  $2668u + 51v = 1$  et on obtient  $(16, -837)$ . Comme  $-837 \equiv 1831 [2668]$ , on a finalement  $51 \times 1831 \equiv 1 [2668]$  et donc  $d = 1831$ .
3. On cherche donc à calculer  $1322^{51} \equiv c [2773]$ . En binaire, on a  $51 \equiv 110011_2$  :
  - Bit 4 :  $C=1322$   $C=C^*C [n]$  :  $C= 694$   $e4=1$  :  $C=C^*M [n]$  :  $C= 2378$
  - Bit 3 :  $C=2378$   $C=C^*C [n]$  :  $C= 737$
  - Bit 2 :  $C=737$   $C=C^*C [n]$  :  $C= 2434$
  - Bit 1 :  $C=2434$   $C=C^*C [n]$  :  $C= 1228$   $e1=1$  :  $C=C^*M [n]$  :  $C= 1211$
  - Bit 0 :  $C=1211$   $C=C^*C [n]$  :  $C= 2377$   $e0=1$  :  $C=C^*M [n]$  :  $C= 585$
 Finalement on obtient  $c = 585$

4. On cherche donc à calculer  $357^{1831} \equiv m [2773]$ . En binaire, on a  $1831 \equiv 11100100111_2$ 
  - Bit 9 :  $C=357$   $C=C^*C [n]$  :  $C= 2664$   $e9=1$  :  $C=C^*M [n]$  :  $C= 2682$
  - Bit 8 :  $C=2682$   $C=C^*C [n]$  :  $C= 2735$   $e8=1$  :  $C=C^*M [n]$  :  $C= 299$
  - Bit 7 :  $C=299$   $C=C^*C [n]$  :  $C= 665$
  - Bit 6 :  $C=665$   $C=C^*C [n]$  :  $C= 1318$
  - Bit 5 :  $C=1318$   $C=C^*C [n]$  :  $C= 1226$   $e5=1$  :  $C=C^*M [n]$  :  $C= 2321$
  - Bit 4 :  $C=2321$   $C=C^*C [n]$  :  $C= 1875$
  - Bit 3 :  $C=1875$   $C=C^*C [n]$  :  $C= 2234$
  - Bit 2 :  $C=2234$   $C=C^*C [n]$  :  $C= 2129$   $e2=1$  :  $C=C^*M [n]$  :  $C= 251$
  - Bit 1 :  $C=251$   $C=C^*C [n]$  :  $C= 1995$   $e1=1$  :  $C=C^*M [n]$  :  $C= 2327$
  - Bit 0 :  $C=2327$   $C=C^*C [n]$  :  $C= 2033$   $e0=1$  :  $C=C^*M [n]$  :  $C= 2028$
 Finalement on obtient  $m = 2028$

### Exercice 2 :

1. Parmi les couples... :
  - (a)  $(3087, 323)$  :  $3087 = 3^2 \times 343$ , donc  $n$  n'est pas composé uniquement de 2 nombres premiers, la clé n'est pas une clé RSA valide.
  - (b)  $(3243, 475)$  :  $3243 = 3 \times 23 \times 47$ , donc  $n$  n'est pas composé uniquement de 2 nombres premiers, la clé n'est pas une clé RSA valide.
  - (c)  $(3953, 625)$  :  $3953 = 59 \times 67$ . Donc  $\varphi(3953) = 58 \times 66 = 3828$ . De plus  $PGCD(3828, 625) = 1$ . Donc c'est une clé publique correct.
  - (d)  $(3599, 435)$  :  $3599 = 59 \times 61$ . Donc  $\varphi(3599) = 58 \times 60 = 3480$ . Par contre,  $PGCD(3480, 435) = 435$ . Comme  $\varphi(n)$  et  $e$  ne sont pas premier entre eux, la clé n'est pas une clé RSA valide.
2. Donc on travaille uniquement sur la troisième clé. Par Bezout, on trouve à l'équation  $3828u + 625v = 1$  la solution  $(-8, 49)$ . Donc  $d = 49$ .
3. On cherche à calculer  $234^{625} \equiv c [3953]$ . On a  $625 = 1001110001_2$ 
  - Bit 8 :  $C=234$   $C=C^*C [n]$  :  $C= 3367$
  - Bit 7 :  $C=3367$   $C=C^*C [n]$  :  $C= 3438$

- Bit 6 :  $C=3438 \ C=C^*C \ [n] : C= 374 \ e6=1 : C=C^*M \ [n] : C= 550$
- Bit 5 :  $C=550 \ C=C^*C \ [n] : C= 2072 \ e5=1 : C=C^*M \ [n] : C= 2582$
- Bit 4 :  $C=2582 \ C=C^*C \ [n] : C= 1966 \ e4=1 : C=C^*M \ [n] : C= 1496$
- Bit 3 :  $C=1496 \ C=C^*C \ [n] : C= 618$
- Bit 2 :  $C=618 \ C=C^*C \ [n] : C= 2436$
- Bit 1 :  $C=2436 \ C=C^*C \ [n] : C= 643$
- Bit 0 :  $C=643 \ C=C^*C \ [n] : C= 2337 \ e0=1 : C=C^*M \ [n] : C= 1344$

Donc finalement  $c = 1344$

4. 12 bits, donc le message maximale (en nombre) est  $2^{12} - 1 = 4095$ . Donc il faut choisir  $p$  et  $q$  tel que  $p \times q = n > 4095$ . On prend par exemple  $n = 59 \times 71 = 4189$ . Comme  $\varphi(4189) = 4060 = 2^2 \times 5 \times 7 \times 29$ , on choisit un  $e$  premier avec  $\varphi(n)$ , par exemple  $e = 31$ . On obtient la clé publique  $(4189, 31)$ .

### Exercice 3 :

Soient  $(e, d) \in \mathbb{N}^2$  avec  $ed \equiv 1 \ [\varphi(n)/2]$ . Il existe donc un  $k \in \mathbb{Z}$  avec  $ed - 1 = k \frac{\varphi(n)}{2} = k \frac{(p-1)(q-1)}{2}$ . Soit  $x \in \mathbb{N}$  avec  $0 \leq x < n$ .

- Si  $\text{pgcd}(x, p) = 1$ , alors selon le petit théorème de Fermat on a  $x^{p-1} \equiv 1 \ [p]$ . Comme  $(q-1)$  est pair,  $k \frac{(q-1)}{2}$  est un entier et on déduit  $x^{ed-1} = x^{(p-1)(q-1)k/2} = (x^{p-1})^{(q-1)k/2} \equiv 1^{(q-1)k/2} \ [p] \equiv 1 \ [p]$ . On en déduit que  $x^{ed} \equiv x \ [p]$
- Si  $p|x$ , alors  $x \equiv 0 \ [p]$ , donc  $x^{ed} \equiv 0 \ [p]$  et  $x^{ed} \equiv x \ [p]$

Donc, dans les deux cas la propriété  $x^{ed} \equiv x \ [p]$  est vérifiée pour  $p$ . Raisonnement symétrique pour  $q$ . Comme  $p \neq q$  et que  $n = p \times q$ , il en résulte que  $x^{ed} \equiv x \ [n]$ .

### Exercice 4 :

Quel raisonnement pour pouvoir décrypter un message? J'ai à ma disposition la clé publique  $(n, e) = (899, 11)$  et le message crypté  $c = 468$ .

- Pour décrypter ce message  $c$  et récupérer la message initial  $m$ , j'utilise la formule  $c^d \equiv m \ [n]$ . Donc il faut que je calcule la clé privée  $(n, d)$ .
- Pour calculer  $d$ , j'utilise la formule  $ed \equiv 1 \ [\varphi(n)]$ . Donc il faut que je calcule  $\varphi(n)$ .
- Pour calculer  $\varphi(n)$ , j'utilise la formule  $\varphi(n) = (p-1)(q-1)$  avec  $n = pq$ . Donc il faut que je calcule la décomposition en facteur premier de  $n$ . *C'est justement cette étape qui est dur dans le monde réel et rend le "casse" de RSA impossible.*

En pratique numériquement maintenant : On  $n = 899 = 29 \times 31$ . Donc  $\varphi(899) = 28 \times 30 = 840$ . On cherche donc à résoudre  $11d \equiv 1 \ [840]$ . Avec Euclide étendu, on trouve  $3 \times 840 - 229 \times 11 = 1$ . Finalement, on a donc  $d \equiv -229 \ [840] \equiv 611 \ [840]$ .

Il faut maintenant calculer  $468^{611} \equiv 13 \ [899]$ . On utilise pour cela l'algorithme utilisant la représentation binaire de la puissance avec  $611 \equiv 1001100011_2$ .

- Bit 8 :  $C=468 \ C=C^*C \ [n] : C= 567$
- Bit 7 :  $C=567 \ C=C^*C \ [n] : C= 546$
- Bit 6 :  $C=546 \ C=C^*C \ [n] : C= 547 \ e6=1 : C=C^*M \ [n] : C= 680$
- Bit 5 :  $C=680 \ C=C^*C \ [n] : C= 314 \ e5=1 : C=C^*M \ [n] : C= 415$
- Bit 4 :  $C=415 \ C=C^*C \ [n] : C= 516$
- Bit 3 :  $C=516 \ C=C^*C \ [n] : C= 152$
- Bit 2 :  $C=152 \ C=C^*C \ [n] : C= 629$
- Bit 1 :  $C=629 \ C=C^*C \ [n] : C= 81 \ e1=1 : C=C^*M \ [n] : C= 150$
- Bit 0 :  $C=150 \ C=C^*C \ [n] : C= 25 \ e0=1 : C=C^*M \ [n] : C= 13$

On obtient finalement que  $m = 13$ .

### Exercice 5 :

$e_A$  et  $e_B$  sont premiers entre eux donc en appliquant l'algorithme d'Euclide étendu, Eve peut déterminer  $1 = se_A + te_B$ . Puis, elle peut calculer  $c_A^s \times c_B^t = (m^{e_A})^s \times (m^{e_B})^t = m^{se_A + te_B} \equiv m \ [n]$ .