Cryptographie chapitres 4 et 5

Série A

Exercice 1. (3 pts)

$\varphi(1'617) = \varphi(3 \cdot 7^2 \cdot 11) =$

$= 3 \cdot 7^2 \cdot 11 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{11}\right) =$

$= 3 \cdot 7^2 \cdot 11 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{10}{11} = \mathbf{840}$

Exercice 2. (4 pts)

Euler : $\text{PGCD}(11; 13) = 1 \Rightarrow 11^{\varphi(13)} \equiv 1 \bmod 13$

- $\varphi(13) = 12 \Rightarrow 11^{12} \equiv 1 \bmod 13$
- $11^{99} = 11^{8 \cdot 12 + 3} = (11^{12})^8 \cdot 11^3 \overset{\text{Euler}}{\equiv}$

$\equiv 1 \cdot 11^3 \equiv 1'331 \equiv \mathbf{5 \bmod 13}$

Série B

Exercice 1. (3 pts)

$\varphi(2'541) = \varphi(3 \cdot 7 \cdot 11^2) =$

$= 3 \cdot 7 \cdot 11^2 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \left(1 - \frac{1}{11}\right) =$

$= 3 \cdot 7 \cdot 11^2 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{10}{11} = \mathbf{1'320}$

Exercice 2. (4 pts)

Euler : $\text{PGCD}(11; 13) = 1 \Rightarrow 11^{\varphi(13)} \equiv 1 \bmod 13$

- $\varphi(13) = 12 \Rightarrow 11^{12} \equiv 1 \bmod 13$
- $11^{98} = 11^{8 \cdot 12 + 2} = (11^{12})^8 \cdot 11^2 \overset{\text{Euler}}{\equiv}$

$\equiv 1 \cdot 11^2 \equiv 121 \equiv \mathbf{4 \bmod 13}$

Exercice 3. (5 pts)

1) proposition vraie pour $n = 0$ car :

   $3^{0+3} \equiv 4^{0+2} \bmod 11$ vraie car $27 \equiv 16 \equiv 5 \bmod 11$

2) hypothèse de récurrence :

   $3^{n+3} \equiv 4^{4n+2} \bmod 11$ vraie pour n

3) conclusion :

   $3^{(n+1)+3} \equiv 4^{4(n+1)+2} \bmod 11$

4) raisonnement :

   $4^{4(n+1)+2} = 4^{4n+2+4} = 4^{4n+2} \cdot 4^4 \overset{\text{h.r.}}{\equiv} 3^{n+3} \cdot 256 \equiv 3^{n+3} \cdot 3 \equiv 3^{n+4} \bmod 11$ CQFD

Exercice 4. (3+5=8 pts)

Clé publique de Laurent $(91, 5)$: $n = 91$; $e = 5$

a) • HELLO en code ASCII : **07 04 11 11 14**

• Théorème RSA : $m^e \equiv c \bmod n$

• 07 : $7^5 \equiv c \bmod 91 \Rightarrow 7^5 \equiv 16'807 \equiv 63 \bmod 91$

• 04 : $4^5 \equiv c \bmod 91 \Rightarrow 4^5 \equiv 1'024 \equiv 23 \bmod 91$

• 11 : $11^5 \equiv c \bmod 91 \Rightarrow 11^5 \equiv 161'051 \equiv 72 \bmod 91$

• 14 : $14^5 \equiv c \bmod 91 \Rightarrow 14^5 \equiv 537'824 \equiv 14 \bmod 91$

• message crypté : **63 23 72 72 14**

b) • Théorème RSA : $c^d \equiv m \bmod n$ tel que $e \cdot d \equiv 1 \bmod \varphi(n)$

• $n = 91 = 7 \cdot 13 \Rightarrow \varphi(91) = \varphi(7) \cdot \varphi(13) = 6 \cdot 12 = 72$

• $5 \cdot d \equiv 1 \bmod 72 \overset{\text{inverse modulaire}}{\Rightarrow} d = 29$ ou

Algorithme d'Euclide étendu :

$72 = 14 \cdot 5 + 2 \quad \Rightarrow 2 = 72 - 14 \cdot 5$

$5 = 2 \cdot 2 + 1 \quad \Rightarrow 1 = 5 - 2 \cdot 2$

$\Rightarrow 1 = 29 \cdot 5 - 2 \cdot 72$

$\Rightarrow$ Clé secrète de Laurent $(7, 13, 29)$

• 41 : $41^{29} \equiv m \bmod 91$

$$29 = 2^4 + 2^3 + 2^2 + 2^0$$

n	$41^{2n} \bmod 91$
0	41
1	$41^2 = 1'681 \equiv 43$
2	$43^2 = 1'849 \equiv 29$
3	$29^2 = 841 \equiv 22$
4	$22^2 = 484 \equiv 29$

$$\Rightarrow 41^{29} \equiv 29 \cdot 22 \cdot 29 \cdot 41 \equiv 6 \bmod 91$$

• 00 : $0^{29} \equiv m \bmod 91 \Rightarrow 0^{29} \equiv 0 \bmod 91$

• message décrypté : **06 00 06** donne **GAG**