

Théorie des nombres et crypto – TE n° 744A

Problème 1 (4 points)

Calculer les nombres entiers x et y tels que

$$9945x + 3003y = \text{pgcd}(9945, 3003)$$

Donner également le $\text{pgcd}(9945, 3003)$.

Posons $a = 9945$ et $b = 3003$

	$\cdot a$	$\cdot b$	
9945	1	0	
3003	0	1	$9945 = 3 \cdot 3003 + 936$
936	1	-3	$3003 = 3 \cdot 936 + 195$
195	-3	10	$936 = 4 \cdot 195 + 156$
156	13	-43	$195 = 1 \cdot 156 + 39$
39	-16	53	$156 = 4 \cdot 39$

Donc $x = -16$, $y = 53$ et $\text{pgcd}(9945, 3003) = 39$

Problème 2 (6 points)

Calculer les expressions suivantes.

a) $2019 \cdot 2020 \cdot 2021 \pmod{2018}$

b) $209^{13} \pmod{215}$

c) $1024^{1024} \pmod{32}$

$$a) \quad 1 \cdot 2 \cdot 3 \equiv 6 \pmod{2018}$$

$$\begin{aligned} b) \quad 209^{13} &\equiv (-6)^{13} \equiv (-6)^7 \cdot (-6)^6 \\ &\equiv -279936 \cdot 46656 \\ &\equiv -6 \cdot 1 \equiv -6 \equiv 209 \pmod{215} \end{aligned}$$

$$\begin{aligned} c) \quad 1024^{1024} &\equiv (2^{10})^{1024} \equiv ((2^5)^2)^{1024} \\ &\equiv 32^{2048} \equiv 0 \pmod{32} \end{aligned}$$

Problème 3 (3 points)

Quels sont les deux derniers chiffres de $7^{9^{9^9}}$?

$$(7^9) \equiv 7 \pmod{100}$$

$$\text{donc } \left((7^9)^9 \right)^9 \equiv 7 \pmod{10}$$

Les deux derniers chiffres sont 07

ou :

$7^0 \equiv 1$		} mod 100
$7^1 \equiv 7$		
$7^2 \equiv 49$		
$7^3 \equiv 43$		
$7^4 \equiv 01$		

$$\left((7^9)^9 \right)^9 = 7^{729} \equiv 7 \pmod{100}$$

$$729 \equiv 1 \pmod{4}$$

TABLE 1 – Annuaire des clés publiques RSA

	n	e
<i>Alice</i>	1739	35
<i>Bob</i>	133	5

Problème 4 (4 points)

Envoyer à *Alice* le message $M = 16$ crypté à l'aide du système RSA.

$$C \equiv 16^{35} \pmod{1739}$$

$$35 = 1 + 2 + 32$$

$$16^2 \equiv 256 \pmod{1739}$$

$$16^4 \equiv 65'536 \equiv 1193 \pmod{1739}$$

$$16^8 \equiv 142'3249 \equiv 747 \pmod{1739}$$

$$16^{16} \equiv 558'009 \equiv 1529 \pmod{1739}$$

$$16^{32} \equiv 233'7841 \equiv 625 \pmod{1739}$$

$$C \equiv 16 \cdot 256 \cdot 625 \equiv 2560000 \equiv 192 \pmod{1739}$$

$$S = 192$$

6
Problème 5 (# points)

- a) Calculez la clé privée d'Alice.
b) Alice a reçu le message $S = 876$ crypté à l'aide du système RSA. Écrire le calcul qui permet à Alice de déchiffrer S .

④ 2) $1739 = 37 \cdot 47$, $\varphi(n) = 36 \cdot 46 = 1656$
Calculons d : $35d + 1656k = 1$

	$\cdot 1656$	$\cdot 35$	
1656	1	0	
35	0	1	$1656 = 47 \cdot 35 + 11$
11	1	-47	$35 = 3 \cdot 11 + 2$
2	-3	142	$11 = 5 \cdot 2 + 1$
1	16	-757	

donc $35 \cdot (-757) \equiv 1 \pmod{1656}$
et $d \equiv -757 \equiv 899 \pmod{1656}$
La clé privée est $(1739, 899)$

④ b) Pour déchiffrer S , on calcule
$$M = S^d \pmod{n}$$

donc $M = 876^{899} \pmod{1739}$

Problème 6 (8 points)

Vous interceptez le message $S = 123$ crypté à l'aide du système RSA que *Bob* a reçu. Déchiffrez-le!

clé publique de Bob : $(133, 5)$
 $133 = 19 \cdot 7$, $\varphi(133) = 18 \cdot 6 = 108$
Calculons d : $5d + 108v = 1$

	$\cdot 108$	$\cdot 5$	
108	1	0	
5	0	1	$108 = 21 \cdot 5 + 3$
3	1	-21	$5 = 1 \cdot 3 + 2$
2	-1	22	$3 = 1 \cdot 2 + 1$
1	2	-43	

donc $5 \cdot (-43) \equiv 1 \pmod{108}$
 $d \equiv -43 \equiv 65 \pmod{108}$

Déchiffrons le message : $M = 123^{65} \pmod{133}$

123^2	$\equiv 15129$	$\equiv 100$	
123^4	$\equiv 18000$	$\equiv 25$	
123^8	$\equiv 625$	$\equiv 93$	$\pmod{133}$
123^{16}	$\equiv 8549$	$\equiv 4$	
123^{32}	$\equiv 16$	\equiv	
123^{64}	$\equiv 256$	$\equiv 123$	

$\Pi \equiv 123 \cdot 123 \equiv 100 \pmod{133}$