Théorie des nombres et crypto – TE n° 744B

Problème 1 (4 points)

Calculer les nombres entier a et b tels que

$$9945\,a + 3003\,b = \text{pgcd}(9945, 3003)$$

Donner également le pgcd(9945, 3003).

Posons $x = 9945$ et $y = 3003$

	$\cdot x$	$\cdot y$	
9945	1	0	$9945 = 3 \cdot 3003 + 936$
3003	0	1	$3003 = 3 \cdot 936 + 195$
936	1	−3	$936 = 4 \cdot 195 + 156$
195	−3	10	$195 = 1 \cdot 156 + 39$
156	13	−43	$156 = 4 \cdot 39$
39	−16	53	

Donc $a = -16$, $b = 53$

et pgcd $= 39$

Problème 2 (6 points)

Calculer les expressions suivantes.

a) $2022 \cdot 2021 \cdot 2020 \pmod{2019}$

b) $208^{13} \pmod{215}$

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

a) $3 \cdot 2 \cdot 1 \equiv 6 \pmod{2019}$

b) $208^{13} \equiv (-7)^{13} \equiv (-7)^6 \cdot (-7)^6 \cdot (-7)$

$\equiv 117649 \cdot 117649 \cdot (-7)$

$\equiv 44 \cdot 44 \cdot (-7)$

$\equiv -13552 \equiv 209$

$\equiv 208$

c) $1024^{1024} \equiv \left(2^{10}\right)^{1024} \equiv \left((2^5)^2\right)^{1024}$

$\equiv 32^{2048} \equiv 0 \pmod{32}$

Problème 3 (3 points)

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

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

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

Les deux derniers chiffres sont 07

ou :

$7^0 \equiv 1$

$7^1 \equiv 7$

$7^2 \equiv 49$

$7^3 \equiv 43$

$7^4 \equiv 01$

} mod 100

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

$729 \equiv 1 \pmod 4$

TABLE 1 – Annuaire des clés publiques **RSA**

	n	e
Alice	1739	35
Bob	133	5

Problème 4 (4 points)

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

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

$35 = 1 + 2 + 32$

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

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

$16^8 \equiv 1423249 \equiv 747 \pmod{1739}$

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

$16^{32} \equiv 2337841 \equiv 625 \pmod{1739}$

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

$S = 192$

Problème 5 (6 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 : $35d + 1656k = 1$

	· 1656	· 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 $(1739, 899)$

① b) Pour déchiffrer S, on calcule

$M = S^d \pmod{n}$

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

Problème 6 (8points)

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 : $5d + 108k = 1$

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

$d \equiv -43 \equiv 65 \pmod{108}$ 4

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

$123^2 \equiv 15129 \equiv 100$

$123^4 \equiv 10000 \equiv 25$

$123^8 \equiv 625 \equiv 93 \pmod{133}$

$123^{16} \equiv 8649 \equiv 4$

$123^{32} \equiv 16$

$123^{64} \equiv 256 \equiv 123$

$M \equiv 123 \cdot 123 \equiv 100 \pmod{133}$ 4