Partie I

1. Propriété fondamentale

$n = p\,q$ est le produit de deux nombres premiers p et q distincts.

On pose $m = (p-1)(q-1)$ et on note c un nombre premier avec m. On note x un entier naturel.

a. Démontrer qu'il existe des entiers d et k tels que : $c\,d = k\,m + 1$ (c'est à dire $c\,d \equiv 1$ modulo m)

b. **Cas où x est non divisible par p.**

Démontrer que $x^{p-1} \equiv 1$ modulo p

En déduire que $x^{k\,m} \equiv 1$ modulo p puis que $x^{c\,d} \equiv x$ modulo p.

Cas où x est divisible par p.

Démontrer que $x^{c\,d} \equiv x$ modulo p.

c. Démontrer de façon analogue que pour tout x entier naturel, $x^{c\,d} \equiv x$ modulo q

d. En déduire que pour tout entier naturel x, $x^{c\,d} \equiv x$ modulo n

$n = p\,q$ (n étant un entier naturel, p et q étant premiers)

sa connaissance permet de trouver les entiers m, c, et d de la partie 1

les messages à crypter sont des entiers x compris entre 0 et $n-1$.

Cryptage : x est crypté par $C(x)$ congru x^c modulo n.

Les données n et a sont nécessaires pour crypter et le couple $(n\,;\,c)$ est la clé publique, connue de tous.

Décryptage : y est décrypté par $D(y)$ congru y^d modulo n.

Les données n et b sont nécessaires pour décrypter et d est la clé privée, connu seulement de la personne qui reçoit le message.

On peut vérifier que $D(C(x))$ congru $(x^c)^d$ congru $x^{c\,d}$ congru x modulo n; on retrouve donc la valeur x après cryptage, puis décryptage.

Partie II

1. Axel souhaite recevoir en message crypté l'âge de Cynthia. Il choisit $p = 3$ et $q = 11$

a. Calculer n et m, puis déterminer le plus petit entier qu'il peut choisir pour c.

b. Déterminer alors le plus petit entier qu'il peut choisir pour d

c. Axel envoie sa clé publique (33 ; 3) à Cynthia. Cette dernière crypte son âge et lui envoie le nombre 29. Retrouver l'âge de Cynthia.

2. En retour, Cynthia souhaite qu'Axel lui envoie en message crypté son numéro de téléphone. Les numéros sont cryptés deux par deux

a. justifier que n doit être supérieur ou égal à 100

b. Montrer que la clé publique la plus petite possible que Cynthia peut envoyer est alors (106 ; 3).

c. Crypter alors avec cette clé le numéro de téléphone d'Axel : 06 13 87 11 45.

CORRECTION

Partie I

1. *a.* c est un nombre premier avec m donc d'après le théorème de Bézout, il existe deux nombres entiers relatifs u et v tels que $c\,u + m\,v = 1$ donc $c\,u = -m\,v + 1$

en posant $d = u$ et $-v = k$; il existe des entiers d et k tels que : $c\,d = k\,m + 1$

b. **Cas où x est non divisible par p.**

p est un nombre premier et x est non divisible par p donc x est premier avec p donc d'après le petit théorème de Fermat, $x^{p-1} \equiv 1$ modulo p

$x^{p-1} \equiv 1$ modulo p donc $(x^{p-1})^{q-1} \equiv 1^{q-1}$ modulo p

soit $x^m \equiv 1$ modulo p donc $(x^m)^k \equiv 1^k$ modulo p soit $x^{k\,m} \equiv 1$ modulo p

$x^{c\,d} = x^{k\,m+1} = x^{k\,m} \times x$ or $x^{k\,m} \equiv 1$ modulo p donc $x^{c\,d} \equiv x$ modulo p.

c. **si x est divisible par q,** alors $x \equiv 0$ modulo q donc $x^{c\,d} \equiv 0$ modulo q donc $x^{c\,d} \equiv x$ modulo q.

si x est non divisible par q, alors q est un nombre premier et x est non divisible par q donc x est premier avec q donc d'après le petit théorème de Fermat, $x^{q-1} \equiv 1$ modulo q

$x^{q-1} \equiv 1$ modulo q donc $(x^{q-1})^{p-1} \equiv 1^{p-1}$ modulo q

soit $x^m \equiv 1$ modulo q donc $(x^m)^k \equiv 1^k$ modulo q soit $x^{k\,m} \equiv 1$ modulo q

$x^{c\,d} = x^{k\,m+1} = x^{k\,m} \times x$ or $x^{k\,m} \equiv 1$ modulo q donc $x^{c\,d} \equiv x$ modulo q.

Dans tous les cas : $x^{c\,d} \equiv x$ modulo q.

d. p et q divisent $x^{c\,d} - x$, p et q sont deux entiers naturels premiers donc premiers entre eux donc, d'après le théorème de Gauss, $p\,q$ divise $x^{c\,d} - x$.

Pour tout entier naturel x, $x^{c\,d} \equiv x$ modulo n

Partie II

1. Axel souhaite recevoir en message crypté l'âge de Cynthia. Il choisit $p = 3$ et $q = 11$

a. Calculer n et m, puis déterminer le plus petit entier qu'il peut choisir pour c.

$n = p\,q = 3 \times 11 = 33$

$m = (p - 1)(q - 1) = 2 \times 10 = 20 = 2^2 \times 5$

c est un nombre premier avec m donc le plus petit entier possible pour c est 3.

b. Il faut résoudre : $c\,u + m\,v = 1$ avec $c = 3$ et $m = 20$

soit $3u + 20v = 1$, une solution est $u = 7$ et $v = -1$

$\begin{cases} 3u + 20v = 1 \\ 3 \times 7 + 20 \times (-1) = 1 \end{cases}$ donc par différence terme à terme : $3(u - 7) + 20(v + 1) = 0$ soit $3(u - 7) = -20(v + 1)$

3 et 20 sont premiers entre eux et 20 divise $3(u - 7)$ donc d'après le théorème de Gauss, 20 divise $u - 7$ donc il existe un entier relatif k tel que $u - 7 = 20k$ donc $u = 20k + 7$

$d = u$ donc $d = 20k + 7$, le plus petit entier naturel qu'il peut choisir pour d est 7.

c. Le couple $(n ; c)$ est la clé publique donc $n = 33$ et $c = 3$

Décryptage : y est décrypté par $D(y)$ congru y^d modulo n.

$D(y) \equiv 29^7$ modulo 33

$29 \equiv -4$ modulo 33

$29^2 \equiv 16$ modulo 33

$29^3 \equiv -64$ modulo 33 donc $29^3 \equiv 2$ modulo 33

$29^6 \equiv 2^2$ modulo 33

$29^7 \equiv 4 \times 29$ modulo $33 \Leftrightarrow 29^7 \equiv 4 \times (-4)$ modulo $33 \Leftrightarrow 29^7 \equiv 17$ modulo 33

29 est décrypté par 17. Cynthia *a* 17 ans.

2. *a.* Justifier que n doit être supérieur ou égal à 100

Le nombre x à crypter est au maximum égal à 99 or $0 \leq x \leq n - 1$ donc $n \geq 100$.

b. La plus petite valeur possible de c est 3 d'après la question 1. *a*.

$n = p\,q$ est le produit de deux nombres premiers p et q distincts.

Le plus petit nombre premier possible est $p = 2$, or $n = p\,q$ et $n \geq 100$ donc $2q \geq 100$ donc $q \geq 50$

Le plus petit nombre premier supérieur à 50 est 53 donc $q = 53$ et $n = 2 \times 53 = 106$

La clé publique la plus petite possible que Cynthia peut envoyer est alors (106 ; 3).

c.

x	06	13	87	11	45
x^3	216	2197	658503	1331	91125
quotient de x^3 par 106	2	20	6212	12	859
reste de x^3 par 106	4	77	31	59	71

Le numéro de téléphone d'Axel : 06 13 87 11 45 est codé par 04 77 31 59 71.