POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

LOG2810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

H2023

SOLUTIONNAIRE

Exercice 1.

Dans le cadre d'un chiffrement RSA, on considère les valeurs $\boldsymbol{p} = 29$ qui est le 10ème nombre premier et $\boldsymbol{q} = 541$ qui est le 100ème nombre premier.

a) Calculez la base modulaire $\boldsymbol{n}$.

Réponse :

La base modulaire est le produit des deux nombres premiers p et q, c'est-à-dire :

$$\boldsymbol{n} = \boldsymbol{p} \cdot \boldsymbol{q} = 29 \cdot 541 = 15\,689.$$

Ainsi, la base modulaire $\boldsymbol{n}$ est $15\,689$.

b) Calculez l'indicatrice de Carmichael $\boldsymbol{i}$.

Réponse :

L'indicatrice de Carmichael est le plus petit commun multiple de $\boldsymbol{p} - 1$ et $\boldsymbol{q} - 1$.
Le PPCM est formé du produit de tous les facteurs premiers composant ces nombres et pour chaque facteur premier, on retient la puissance la plus élevée qui apparaît dans la décomposition de chacun de ces nombres.

$(\boldsymbol{p} - 1) = (29 - 1) = 28 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7$
$(\boldsymbol{q} - 1) = (541 - 1) = 540 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^3 \cdot 5$

Donc, $\boldsymbol{i} = PPCM(\boldsymbol{p} - 1, \boldsymbol{q} - 1) = PPCM(28, 540) = 2^2 \cdot 3^3 \cdot 5 \cdot 7 = 3\,780$

Ou bien, elle peut également être calculée à l'aide de la formule suivante :

$$\boldsymbol{i} = PPCM(\boldsymbol{p} - 1, \boldsymbol{q} - 1) = \frac{(\boldsymbol{p} - 1)(\boldsymbol{q} - 1)}{PGCD(\boldsymbol{p} - 1,\ \boldsymbol{q} - 1)}$$

où PGCD désigne le plus grand commun diviseur.

PGCD(28, 540) = PGCD(28, 8) = PGCD(4, 8) = PGCD(4, 4) = 4
Donc, $\boldsymbol{i} = PPCM(28, 540) = \frac{28 \cdot 540}{PGCD(28,540)} = \frac{15\,120}{4} = 3\,780.$

Ainsi, l'indicatrice de Carmichael $\boldsymbol{i}$ est 3 780.

c) En considérant que la clé de chiffrement est $\boldsymbol{e} = 113$, calculez la valeur de la clé privée $\boldsymbol{d}$.

Réponse :

On doit trouver l'inverse multiplicatif $\boldsymbol{d}$ tel que $\boldsymbol{e} \cdot \boldsymbol{d} \equiv 1(mod\ \boldsymbol{i})$.
$\boldsymbol{e} \cdot \boldsymbol{d} \equiv 1(mod\ \boldsymbol{i}) \Rightarrow 113 \cdot \boldsymbol{d} \equiv 1(mod\ 3\ 780)$.
On a donc l'équation $113\boldsymbol{d} + 3\ 780\boldsymbol{a} = 1$.
113 et 3780 sont relativement premiers.
Résolvons l'équation via l'algorithme d'Euclide étendu.

[113, 1, 0] [3780, 0, 1]
[113, 1, 0] [51, -33, 1]
[11, 67, -2] [51, -33, 1]
[11, 67, -2] [7, -301, 9]
[4, 368, -11] [7, -301, 9]
[4, 368, -11] [3, -669, 20]
[1, 1037, -31] [3, -669, 20]
[1, 1037, -31] [1, -2743, 82]
On peut donc prendre $\boldsymbol{d} = 1037$ comme clé privée.
On vérifiera aisément que $113 \cdot 1037 \equiv 1\ (mod\ 3780)$

d) Quel est le message $\boldsymbol{C}$ chiffré à partir du message $\boldsymbol{M} = 200$.
Note : Les calculs suivants vous sont fournis.

- $10^{113} \equiv 2\ 707 \pmod{15\ 689}$
- $2^{113} \equiv 12\ 354 \pmod{15\ 689}$
- $2\ 707^2 = 467 \cdot 15\ 689 + 1\ 086$
- $12\ 354 \cdot 1\ 086 = 855 \cdot 15\ 689 + 2\ 349$

Réponse :

$\boldsymbol{C} = \boldsymbol{M}^{\boldsymbol{e}} = 200^{113} = (2 \cdot 100)^{113} = 2^{113} \cdot 100^{113} = 2^{113} \cdot (10^{113})^2$
D'après l'énoncé $10^{113} \equiv 2\ 707 \pmod{15\ 689}$, alors $(10^{113})^2 \equiv 2\ 707^2 \pmod{15\ 689}$
Et, $2\ 707^2 = 467 \cdot 15\ 689 + 1\ 086$ alors $2\ 707^2 \equiv 1\ 086 \pmod{15\ 689}$
Donc, $(10^{113})^2 \equiv 1\ 086 \pmod{15\ 689}$
Ainsi, $2^{113} \cdot (10^{113})^2 \equiv 12\ 354 \cdot 1\ 086 \pmod{15\ 689} \equiv 2\ 349 \pmod{15\ 689}$
D'où $\boldsymbol{C} = 2\ 349$

Exercice 2.

La génération de séquence de nombres aléatoires est essentielle pour les algorithmes aléatoires, les simulations et de nombreux autres usages en informatique. La méthode la plus couramment utilisée pour générer des nombres pseudos-aléatoires est celle du générateur congruentiel linéaire qui est définie récursivement comme suit :

$$x_{n+1} = (a\ x_n + c)(mod\ m)$$

Où $\boldsymbol{m}$ est le module, $\boldsymbol{a}$ le multiplicateur, $\boldsymbol{c}$ l'incrément et le terme initial $\boldsymbol{x_0}$ appelé la graine (*seed* en anglais) avec des conditions telles que $2 \leq a < m$, $0 \leq c < m$ et $0 \leq x_0 < m$.

Quelle est la séquence de nombres pseudo-aléatoires générée à l'aide du générateur congruentiel linéaire $x_{n+1} = (4\,x_n + 1)(mod\ 7)$ avec une graine $x_0 = 3$?

Réponse :

On calcule les termes de cette séquence en utilisant successivement la fonction récursive du générateur congruentiel linéaire, en partant de la graine $x_0 = 3$ pour obtenir x_1.

On obtient donc,

$x_1 = (4\,x_0 + 1)(mod\ 7) = (4 \cdot 3 + 1)(mod\ 7) = 13(mod\ 7) = 6$
$x_2 = (4\,x_1 + 1)(mod\ 7) = (4 \cdot 6 + 1)(mod\ 7) = 25(mod\ 7) = 4$
$x_3 = (4\,x_2 + 1)(mod\ 7) = (4 \cdot 4 + 1)(mod\ 7) = 17(mod\ 7) = 3$

Puisque $x_3 = x_0$ et que chaque terme ne dépend que du terme précédent, on constate que la séquence

3, 6, 4, 3, 6, 4 …

continue à se répéter indéfiniment.

Exercice 3.

Calculez [(101^{493} mod 13) · (101^{508} mod 13)] (mod 13).

Note : Le calcul suivant vous est fourni.

- 1 001 = 12 · 83 + 5

Réponse :

Soit m un entier positif et a et b des entiers,
Par la définition de la congruence, on sait que

a ≡ (a mod m) (mod m)
b ≡ (b mod m) (mod m)

Par conséquent, a · b ≡ [(a mod m) · (b mod m)] (mod m).
Ainsi, 101^{493} · 101^{508} = 101^{1001} ≡ [(101^{493} mod 13) · (101^{508} mod 13)] (mod 13).
Donc, calculer [(101^{493} mod 13) · (101^{508} mod 13)] (mod 13) revient à calculer 101^{1001} (mod 13).
101 ≡ 10 (mod 13), alors 101^{1001} ≡ 10^{1001} (mod 13).
13 est un nombre premier et 13 ne divise pas 10.
Par le petit théorème de Fermat, on sait que 10^{12} ≡ 1 (mod 13).
Et donc, 10^{1001} = (10^{12})^{83} · 10^5 ≡ 1^{83} · 10^5 (mod 13) ≡ 1 · 10^5 (mod 13) ≡ 10^5 (mod 13).

Puisque 10^5 = 10 (10^2)^2.
Et 10^2 = 100 ≡ 9 (mod 13).
Donc 10^5 = 10 (10^2)^2 ≡ 10 · 9^2 (mod 13) ≡ 10 · 81 (mod 13) ≡ 10 · 3 (mod 13) ≡ 30 (mod 13)
≡ 4 (mod 13).

D'où [(101^{493} mod 13) · (101^{508} mod 13)] (mod 13) = $101^{1001}\ (\mathrm{mod}\ 13)$ ≡ 4 (mod 13)

Exercice 4.
Trouvez l'entier a qui laisse un reste de 1 et de 2 lorsqu'il est divisé par 27 et 88, respectivement.

Réponse :
Nous cherchons un entier a qui satisfait les conditions suivantes :

$$a \equiv 1 \ (mod\ 27)$$
$$a \equiv 2 \ (mod\ 88)$$

Elles peuvent être réécrites comme suit :

$$a = 27s + 1$$
$$a = 88t + 2$$

On obtient donc : $27s + 1 = 88t + 2$.
En réécrivant, on a $27s - 88t = 1$.
Il suffit donc de résoudre l'équation $27s' + 88t' = 1$.
27 et 88 sont relativement premiers.
Résolvons l'équation via l'algorithme d'Euclide étendu.

[27, 1, 0] [88, 0, 1]
[27, 1, 0] [7, -3, 1]
[6, 10, -3] [7, -3, 1]
[6, 10, -3] [1, -13, 4]
[1, 75, -23] [1, -13, 4]

On peut prendre $s' = -13$ et $t' = 4$, soit $s = -13$ et $t = -4$.
On en déduit que $a = -350$ est l'entier qui laisse un reste de 1 et de 2 lorsqu'il est divisé par 27 et 88, respectivement.

Exercice 5.
Résolvez dans $\mathbb{Z}$ l'équation suivante :

$$720a + 27b = 36$$

Réponse :
PGCD(720, 27) = PGCD(18, 27) = PGCD(18, 9) = PGCD(9, 9) = 9
9 divise 36, alors l'équation $720a + 27b = 36$ possède des solutions.
Si on divise le tout par 9, on obtient $80a + 3b = 4$.
Il suffit donc de résoudre $80a' + 3b' = 1$, puis multiplier les résultats obtenus par 4 pour trouver a et b.
Utilisons l'algorithme d'Euclide étendu pour trouver a' et b'.

[80, 1, 0] [3, 0, 1]
[2, 1, -26] [3, 0, 1]
[2, 1, -26] [1, -1, 27]
[1, 2, -53] [1, -1, 27]

On peut prendre $a' = -1$ et $b' = 27$ comme une des solutions de $80a' + 3b' = 1$.
On en déduit que $a = -4$ et $b = 108$ constituent une solution particulière de l'équation $80a + 3b = 4$ et par conséquent, solution particulière de l'équation $720a + 27b = 36$.
Les solutions recherchées sont donc de la forme $a = -4 - 3k$ et $b = 108 + 80k$, avec k entier.

Exercice 6.
Montrez que 7 divise $2222^{5555} + 5555^{2222}$. Présentez toutes les étapes de votre réponse.
Note : Les calculs suivants vous sont fournis.

- $5555 = 6 \cdot 925 + 5$
- $2222 = 7 \cdot 317 + 3$
- $2222 = 6 \cdot 370 + 2$
- $5555 = 7 \cdot 793 + 4$

Réponse :
7 est un nombre premier et 7 ne divise pas 2222.
En appliquant le petit théorème de Fermat, $2222^6 \equiv 1 \pmod 7$.
Or, $5555 = 6 \cdot 925 + 5$, donc $2222^{5555} \equiv 1^{925} \cdot 2222^5 \pmod 7$.
Ainsi, $2222^{5555} \equiv 2222^5 \pmod 7$.
Or, $2222 = 7 \cdot 317 + 3$, donc $2222 \equiv 3 \pmod 7$.
Donc, $2222^5 \equiv 3^5 \pmod 7$, soit $2222^5 \equiv 5 \pmod 7$.
D'où $2222^{5555} \equiv 5 \pmod 7$.

Similairement, 7 est un nombre premier et 7 ne divise pas 5555.
En appliquant le petit théorème de Fermat, $5555^6 \equiv 1 \pmod 7$.
Or, $2222 = 6 \cdot 370 + 2$, donc $5555^{2222} \equiv 1^{370} \cdot 5555^2 \pmod 7$.
Ainsi, $5555^{2222} \equiv 5555^2 \pmod 7$.
Or, $5555 = 7 \cdot 793 + 4$, donc $5555 \equiv 4 \pmod 7$.
Donc, $5555^2 \equiv 4^2 \pmod 7$, soit $5555^2 \equiv 2 \pmod 7$.
D'où $5555^{2222} \equiv 2 \pmod 7$.

Enfin, nous obtenons
$2222^{5555} \equiv 5 \pmod 7$ et $5555^{2222} \equiv 2 \pmod 7$,
Alors $(2222^{5555} + 5555^{2222}) \equiv (5+2) \pmod 7$.
Soit $(2222^{5555} + 5555^{2222}) \equiv 0 \pmod 7$.
D'où 7 divise $2222^{5555} + 5555^{2222}$.
CQFD

Exercice 7.
Soit m un nombre premier et a un entier naturel. Montrez que :

$$(a + 1)^m - a^m - 1 \text{ est divisible par } m$$

Réponse :
m étant premier, d'après le petit théorème de Fermat, on a :

(I) $a^m \equiv a \pmod m$
(II) $(a + 1)^m \equiv (a + 1) \pmod m$

En soustrayant **(I)** de **(II)**, on obtient successivement :
$(a + 1)^m - a^m \equiv [(a + 1) - a] \pmod m$
$(a + 1)^m - a^m \equiv 1 \pmod m$
$(a + 1)^m - a^m - 1 \equiv 0 \pmod m$

D'où $(a + 1)^m - a^m - 1$ est divisible par m.
CQFD