R3.09 Cryptographie et sécurité
TD 2 : Arithmétique et chiffrements asymmétrique

17 décembre 2024

1 Un peu d'arithmétique : Euclide Bézout, calcul du pgcd et de l'inverse

Définition 1

Soient $n \in \mathbb{N}, n > 1, (a, b) \in \mathbb{Z}^2$. a et b sont congrus modulo n. $a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z}, a = b + kn$

$x \in \mathbb{Z}/n\mathbb{Z}$ est inversible **si et seulement si** il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \times y = \overline{1}$

$x \in \mathbb{Z}/n\mathbb{Z}$ est un diviseur de zéro **si et seulement si** $x \neq \overline{0} \wedge \exists y \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}, xy = \overline{0}$

Exercice 1. 1. Donnez les classes de congruence de $\mathbb{Z}/6\mathbb{Z}$.

Réponse

$\oplus$	0	1	2	3	4	5
0	0	0	0	0	0	0
1		1	2	3	4	5
2			4	0	2	4
3				3	0	3
4					4	2
5						1

Les diviseurs de zéro sont $\overline{2}, \overline{3}, \overline{4}$ car $\overline{2} \times \overline{3} = \overline{0}$ et $\overline{4} \times \overline{3} = \overline{0}$.
Les éléments inversibles sont $\overline{1}$ et $\overline{5}$ car $\overline{1} \times \overline{1} = \overline{1}$ et $\overline{5} \times \overline{5} = \overline{1}$.
$\overline{44} \times \overline{77} = \overline{2} \times \overline{5} = \overline{4}$

$$\begin{aligned}\overline{11}^3 + \overline{2013} =& \overline{-1}^3 + \overline{3} \\ =& \overline{-1} + \overline{3} \\ =& \overline{2}\end{aligned}$$

Théorème 1: Bachet-Bézout

Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$.
$\text{pgcd}(a, b) = 1 \iff \exists (u, v) \in \mathbb{Z}, au + bv = 1$

$$u_i = u_{i-2} - u_{i-1}q_i$$
$$v_i = v_{i-2} - v_{i-1}q_i$$

$$\text{pgcd}(a, b) = \text{pgcd}(b, a \pmod b)$$

$\text{pgcd}(143, 100) = 1$ donc $\overline{100}$ est inversible dans $\mathbb{Z}/143\mathbb{Z}$.
$143 \times 7 + 100(-10) = 1$
Dans $\mathbb{Z}/143\mathbb{Z}$, l'équation devient $\overline{0} \times \overline{7} + \overline{100}(\overline{-10}) = \overline{1}$

Exercice 2.

a	b	r	q		u	v	i
		114			1	0	-1
	114	33			0	1	0
114	33	15	3		1	-3	1
33	15	3	2		-2	7	2
15	3	0	5				3

$\text{pgcd}(114, 33) = 3$
$\overline{33}$ est un diviseur de zéro dans $\mathbb{Z}/114\mathbb{Z}$.

a	b	r	q		u	v	i
		114			1	0	-1
	114	35			0	1	0
114	35	9	3		1	-3	1
35	9	6	3		-3	10	2
9	6	3	1		4	-13	3
6	3	0	2				4

$\text{pgcd}(114, 35) = 1$

$114 \times 4 + 35 \times (-13) = 1$ dans $\mathbb{Z}/114\mathbb{Z}$, l'équation devient

$$\overline{0} \times \overline{4} + \overline{35} \times (\overline{-13}) = \overline{0} + \overline{1} = \overline{1}$$

Exercice 3. 1. Coder la lettre W.

Réponse : L

chiffre associé à W est 22, donc $x = 22$

$$\begin{aligned} f(22) &= 9 \times 22 + 8 \equiv 9 \times (-4) + 8 \pmod{26} \\ &\equiv -36 + 8 \pmod{26} \equiv -10 + 8 \pmod{26} \\ &\equiv -2 \pmod{26} \equiv 24 \pmod{26} \end{aligned}$$

et 24 est associé à la lettre Y.

2. Le but de cette question est de déterminer la fonction de chiffrement.

(a)

$$\begin{aligned} 9x \equiv j \pmod{26} &\iff 3 \times 9x \equiv 3j \pmod{26} \\ \iff 27x \equiv 3j \pmod{26} &\iff x \equiv 3j \pmod{26} \end{aligned}$$

(b)

$$\begin{aligned} \forall x \in \mathbb{Z}/26\mathbb{Z}, y = 9x + 8 &\iff 3y = 3 \times 9x + 2 \times 3 \pmod{26} \\ &\iff 3y = 27x + 24 \pmod{26} \iff 3y = x + 24 \pmod{26} \\ &\iff x = 3y - 24 \iff x = 3y + 2 \end{aligned}$$

On obtient $f^{-1}(y) = 3y + 2$

(c) Le chiffre associé de L est 11, donc $y = 11$ $f^{-1}(11) = 3 \times 11 + 2 = 35 \equiv 9 \pmod{26}$ 9 est associé à J. La lettre L ets décodé en lettre J

Exercice 4. 1. Chiffrer le mot : INFINI

Réponse

lettre	$f(x) = 8x + 1 \pmod{26}$	lettre codée
I	$11 \times 8 + 1 \pmod{26} \equiv 11$	L
N	$11 \times 13 + 1 \pmod{26} \equiv 14$	O
F	$11 \times 5 + 1 \pmod{26} \equiv 4$	E

INFINI => LOELOL

2. $f(x) = 11x + 1$, on cherche l'inverse de 11 dans $\mathbb{Z}/26\mathbb{Z}$ grâce à la méthode Euclide-Bézout

a	b	r	q		u	v	i
		26			1	0	-1
	26	11			0	1	0
26	11	4	2		1	-2	1
11	4	3	2		-2	5	2
4	3	1	1		3	-7	3
3	1	0	3				4

On obtient $26 \times 3 + 11 \times (-7) = 1$, $-7 \equiv 19 \pmod{26}$ Donc 19 est l'inverse de 11 dans $\mathbb{Z}/26\mathbb{Z}$

Dans

$$\begin{aligned} \mathbb{Z}/26\mathbb{Z}, y = 11x + 1 &\iff 19y = 19 \times 11x + 19 \pmod{26} \\ &\iff 19y = x + 19 \pmod{26} \iff x = 19y - 19 \pmod{26} \\ &\iff x = 19y + 7 \pmod{26} \end{aligned}$$

On obtient $f^{-1}(y) = 19y + 7 \pmod{26}$

3. Déchiffrer XAZXZSBC.

Réponse

lettre	code	$x = f^{-1}(y) = 19y + 7$	lettre déchiffrée
X	23	8	C
A	0	7	H
Z	25	14	O
S	18	11	L
B	1	0	A
C	2	19	T

Exercice 5.

Exercice 6. 1. La lettre E est associée au nombre 4 et l'image de E par f est E, ça veut dire $f(4) = 4$, soit $a \times 4 + b \equiv 4 \pmod{26}$ Les lettres J et N sont associées aux nombres 9 et 13, et l'image de J est Nn ça veut

dire $f(9) = 13$, soit $a \times 9 + b \equiv 13 \pmod{26}$ Donc on obtient le système $\begin{cases} 4a + b \equiv 4 \pmod{26} \\ 9a + b \equiv 13 \pmod{26} \end{cases}$

2. (a) Nous avons $\begin{cases} 4a + b \equiv 4 \pmod{26} \\ 9a + b \equiv 13 \pmod{26} \end{cases} \Rightarrow (9a + b) - (4a + b) \equiv 13 - 4 \pmod{26} \Rightarrow 5a \equiv 9 \pmod{26}$ Pour résoudre cette équation on cherche l'inverse de 5 dans $\mathbb{Z}/26\mathbb{Z}$:

a	b	r	q		u	v	i
		26			1	0	-1
	26	5			0	1	0
26	5	1	5		1	-5	1
5	1	0	5				2

... Nous obtenons $5a \equiv 9 \pmod{26} \iff 21 \times 5a \equiv 21 \times 9 \pmod{26} \iff a \equiv 7 \pmod{26}$ posons $a = 7$ dans l'équation $4a + b \equiv 4 \pmod{26}$ Nous obtenons $28 + b \equiv 4 \pmod{26} \iff 6 \equiv 4 - 28 \pmod{26} \iff 6 \equiv 2 \pmod{26}$ Finalement $f(x) = ax + b = 7x + 2$

(b) $7x \equiv z \pmod{26} \iff 15 \times 7x \equiv 15 \times z \pmod{26} \iff x \equiv 15z \pmod{26}$

(c) On cherche $f^{-1}(y)$

$$\forall y \in \mathbb{Z}/26\mathbb{Z}, y = 7x + 2 \iff y \equiv 7x + 2 \pmod{26}$$
$$\iff 15y \equiv 15 \times 7x + 15 \times 2 \pmod{26} \iff 15y \equiv x + 4 \pmod{26} \iff$$

Donc on obtient $f^{-1}(y) = 15y + 22$

(d)

Définition 2: Nombres inversibles

Les nombres inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les nombres premiers avec n

Exemple 1

Soit $n = 6$, les nombres inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont $\{1, 5\}$

2 Echange de clés Diffie-Hellman

Exercice 7. — Soit $p = 17$, prouvez que $g = 3$ est un génrateur de $(\mathbb{Z}/17\mathbb{Z})^\times$.
$(\mathbb{Z}/17\mathbb{Z})^\times = \{1, 2, \ldots, 16\}, \varphi(17) = 16$.
$< 3 >= (\mathbb{Z}/17\mathbb{Z})^\times$, $< 3 >$ est générateur de $(\mathbb{Z}/17\mathbb{Z})^\times$.

— Soit $p = 17$ et $g = 3$ les clés partagées entre Alice et Bob. Alice choisit $a = 7$, et Bob choisit $b = 4$. Completer le protocole de Diffie-Hellman pour partager une clé secrète.
  — $a = 7$
  — $g^a = 3^7 \pmod{17} \equiv 11 \pmod{17}$
  — envoie 11 à Bob
  — $13^7 \pmod{17} \equiv (-4)^7 \pmod{17} \equiv ((-4)^2)^3 \times (-4) \pmod{17} \equiv 4 \pmod{17}$

3 Rappel arithmétique : Théorème d'Euler

Exercice 8.
1. $77 = 7 \times 11$
2. $\varphi(77) = (7-1)(11-1) = 6 \times 10 = 60$
3. $\text{pgcd}(77, 9) = 1$, d'après le théorème de Fermat amélioré : $9^{60} \equiv 1 \pmod{77}$
4. $125 = 2 \times 60 + 5$
5. $9^{125} = 9^{2\times 60+5} = (9^{60})^2 \times 9^5 \equiv 1^2 \times 9^5 \pmod{77} \equiv 9^5 \pmod{77} \equiv (9^2)^2 \times 9 \pmod{77} \equiv 4^2 \times 9 \pmod{77} \equiv 67 \pmod{77}$

Exercice 9.
1. (a) $291 = 3 \times 97$
   (b) $\varphi(291) = (3-1)(97-1) = 2 \times 96 = 192$
   (c) $100^{\varphi(291)} = 100^{192} \equiv 1 \pmod{291}$
   (d) $193 = 192 + 1$
   (e) $100^{192+1} \pmod{291} \equiv 100^{192} \times 100^1 \pmod{291} \equiv 1 \times 100^1 \pmod{291} \equiv 100 \pmod{291}$
2. (a) $119 = 7 \times 17$
   (b) $\varphi(119) = (7-1)(17-1) = 6 \times 16 = 96$
   (c) $11^{\varphi(119)} = 11^{96} \equiv 1 \pmod{119}$
   (d) $300 = 3 \times 96 + 12$
   (e) $11^{3\times 96+12} \pmod{119} \equiv (11^{96})^3 \times 11^{12} \pmod{119} \equiv 1^3 \times 11^{12} \pmod{119} \equiv$

Exercice 10. $a = 9$, $b = 85$
— $\varphi(n) = \varphi(85) = \varphi(5 \times 17) = (5-1)(17-1) = 4 \times 16 = 64$
— l'inverse de $e = 5$ dans $\mathbb{Z}/\varphi(n)\mathbb{Z} = \mathbb{Z}/64\mathbb{Z}$

a	b	r	q		u	v	i
		64			1	0	-1
	64	5			0	1	0
64	5	4	12		1	-12	1
5	4	1	1		-1	13	2
4	1	0	4				3

Nous obtenus l'inverse de 5 dans $\mathbb{Z}/64\mathbb{Z}$ est $d = 13$

— $\text{pgcd}(9, 85) = 1$ d'après le théorème d'Euler, $9^{64} \equiv 1 \pmod{85}$
$a^{e \times d} = (a^e)^d = 9^{5 \times 13} \equiv 9^{65} \pmod{85} \equiv 9^{64} \times 9 \equiv 9 \pmod{85}$

4 Chiffrement RSA

Exercice 11 (*Justification de la méthode*)**.**

Exercice 12 (*Chiffrement/Déchiffrement RSA*)**.** On considère la clé publique RSA (319, 11), c'est-à-dire pour $n = 319$ et $e = 11$.

1. Quel est le chiffrement avec cette clé du message $M = 100$?

Réponse

$c = 100^{11} \pmod{319} = (10^{11})^2 \pmod{319} \equiv 263^2 \pmod{319} \equiv 265 \pmod{319}$

2. Calculer d la clé privée correspondant à la clé publique e.

Réponse

$\varphi(319) = 10 \times 28 = 280$
On calcule l'inverse de $e = 11$ dans $\mathbb{Z}/280\mathbb{Z}$:

a	b	r	q		u	v	i
		280			1	0	-1
	280	11			0	1	0
280	11	5	25		1	-25	1
11	5	1	2		-2	51	2
5	1	0	5				3

Donc $d = 51$

3. Déchiffrer le message $C = 133$.

Réponse

$M = C^d \pmod{n} = 133^{51} \pmod{319} \equiv (133^{25})^2 \times 133 \pmod{319} \equiv 133^3 \pmod{319} \equiv 12 \pmod{319}$

4. Le message chiffré 625 peut-il résulter d'un chiffrement avec la clé publique ? Même question avec la clé privée.

Réponse

Non pour les deux car les messages à chiffrer doivent être plus petits que $n = 319$.

Exercice 13 (*Cryptographie RSA et authentification*)**.**

Exercice 14 (*Connaître p et q c'est connaitre $\varphi(n)$*)**.**

Exercice 15 (*Attaque RSA par module commun*)**.**

5 Arithmétique : Générateur et problème du logarithme discret

Exercice 16 (**Notion de générateur**)**.** On se place dans $\mathbb{Z}/7\mathbb{Z}$

- Donner les éléments inversibles.
  $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}, \varphi(7) = 6$
- — $< 2 >= \{1, 2, 4\}$, $2^0 \equiv 1 \pmod 7$, $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$ On s'arrête quand on obtient l'élément 1. $< 3 >= \{1, 2, 3, 4, 5, 6\} = (\mathbb{Z}/7\mathbb{Z})^\times$ l'ordre de $< 3 >$ est 6
  - Donc $< 3 >$ est un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$.
- On se place maintenant dans $\mathbb{Z}/9\mathbb{Z}$.
  - $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}, \varphi(9) = \varphi(3^2) = (3-1) \times 3^{2-1} = 2 \times 2 = 6.$
  - $< 4 >= \{1, 4, 7\}$, ordre de $< 4 >$ est 3.
    $< 7 >= \{1, 4, 7\}$, ordre de $< 7 >$ est 3.
    $< 2 >= \{1, 2, 4, 5, 7, 8\}$, ordre de $< 7 >$ est 4.

  - $< 2 >$ est un générateur de $(\mathbb{Z}/9\mathbb{Z})^\times$.