UGA-IUT2-Grenoble
Département Informatique

Année Universitaire 2022-2023

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

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

Exercice 1

1. Donnez les classes de congruence de $\mathbb{Z}/6\mathbb{Z}$.
2. Construisez les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$.
3. Donnez les diviseurs de zéro et les éléments inversibles.
4. Calculez dans $\mathbb{Z}/6\mathbb{Z}$ $\bar{4}\bar{4} \times \bar{7}\bar{7}$ puis $\bar{1}\bar{1}^3 + 2\bar{0}\bar{1}3$

Exercice 2 On veut déterminer l'inverse de 100 dans $\mathbb{Z}/143\mathbb{Z}$. Finissez de remplir le tableau d'Euclide Bézout ci-dessous.

a	b	r	q	u	v	i
		143		1	0	-1
	143	100		0	1	0
143	100	43	1			1
						2
						3

En déduire $pgcd(143, 100)$. En déduire un couple d'entiers relatifs (u, v) tel que $143u + 100v = pgcd(143, 100)$. En déduire l'inverse de 100 dans $\mathbb{Z}/143\mathbb{Z}$.

Exercice 3

- Déterminer le pgcd de 114 et 33. Déterminer un couple d'entiers relatifs (u, v) tel que $114u + 33v = pgcd(114, 33)$. Peut on calculer l'inverse de 33 dans $\mathbb{Z}/114\mathbb{Z}$? si oui calculer le.
- Déterminer le pgcd de 114 et 35. Déterminer un couple d'entiers relatifs (u, v) tel que $114u + 35v = pgcd(114, 35)$.Peut on calculer l'inverse de 35 dans $\mathbb{Z}/114\mathbb{Z}$? si oui calculer le.

2 Chiffrement Affine

Afin de coder un message on assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice 4 On se donne une fonction de codage affine f , par exemple : $f(x) = 9x+8$.
A une lettre du message :
• on lui associe un entier x entre 0 et 25 suivant le tableau de correspondance ci-dessus.
• on calcule $f(x) = 9x + 8$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26
• On traduit y par une lettre d'après le tableau de correspondance.
La fonction de codage est définie par la fonction f définie par : $f(x) = 9x + 8$

1. Coder la lettre W.
2. Le but de cette question est de déterminer la fonction de décodage.
   (a) Montrer que pour tous nombres entiers relatifs x et j, on a :
   $$9x \equiv j \ (mod\ 26) \Leftrightarrow x \equiv 3j \ (mod\ 26).$$
   (b) En déduire que la fonction f^{-1} de décodage est $f^{-1}(y) = 3y + 2$
   (c) Décoder la lettre L.

Exercice 5 La fonction de codage est définie par la fonction f telle que : $f(x) = 11x + 1$

1. Coder le mot : INFINI
2. Déterminer la fonction de déchiffrage f^{-1}.
3. Décoder le message XAZXZSBC

Exercice 6 On a reçu le message suivant : $JWPNWMRCFWMY$
On sait que le chiffrement est affine et que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.
Soit la fonction affine f définie par : $f(x) = ax + b$ où a et b sont des entiers naturels compris entre 0 et 25.

1. Démontrer que a et b vérifient le système suivant :$\begin{cases} 4a + b \equiv 4 \ (mod\ 26) \\ 9a + b \equiv 13 \ (mod\ 26) \end{cases}$
2. (a) Démontrer que $5a \equiv 9 \ (mod\ 26)$, puis que $a \equiv 7 \ (mod\ 26)$
   (b) En déduire que $b \equiv 2 \ (mod\ 26)$ et que f est définie par $f(x) = 7x + 2$

(c) Démontrer que pour tous relatifs x et z, on a :

$$7x \equiv z \ (mod\ 26) \Leftrightarrow x \equiv 15z \ (mod\ 26)$$

(d) En déduire que la fonction de décodage f^{-1} est $f^{-1}(y) = 15y + 22$

(e) Décoder le message.

Exercice 7 Le chiffrement de Hill a été publié en 1929. C'est un chiffre polygraphique, c'est à dire qu'on ne chiffre pas les lettres les unes après le autres, mais par "paquets". On présente ici un exemple "bigraphique", c'est à dire que les lettres sont regroupées deux à deux.

- **Etape 1** On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant toujours le même tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient des couples d'entiers $(x_1; x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

- **Etape 2** Chaque couple $(x_1; x_2)$ est transformé en $(y_1; y_2)$ tel que :

$$\begin{cases} y_1 \equiv 11x_1 + 3x_2 \ (mod\ 26) \quad avec\ 0 \leq y_1 \leq 25\ et\ 0 \leq y_2 \leq 25. \\ y_2 \equiv 7x_1 + 4x_2 \ (mod\ 26) \end{cases}$$

- **Etape 3** Chaque couple $(y_1; y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres

Exemple

	étape 1		étape 2		étape 3	
TE	$\rightarrow$	$(19, 4)$	$\rightarrow$	$(13, 19)$	$\rightarrow$	NT
mot en clair						mot codé

1. Coder le mot ST.
2. Coder PALACE et RAPACE. Que constatez-vous ?
3. On veut maintenant déterminer la procédure de décodage :
   (a) Calculer l'inverse de 23 dans $\mathbb{Z}/26\mathbb{Z}$.
   (b) Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système $(S1)$, vérifie les équations du système $(S2)$ défini par : $\begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \ (mod\ 26) \\ 23x_2 \equiv 19y_1 + 11y_2 \ (mod\ 26) \end{cases}$
   (c) Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système $(S2)$, vérifie les équations du système $(S3)$ défini par : $\begin{cases} x_1 \equiv 16y_1 + y_2 \ (mod\ 26) \\ x_2 \equiv 11y_1 + 5y_2 \ (mod\ 26) \end{cases}$

(d) Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système $(S3)$, vérifie les équations du système $(S1)$.

(e) Ecrire Les étapes du déchiffrement sur le même mode que les étapes du chiffrement.

(f) Décoder le mot : PFXXKNU

Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, on supprimera la lettre dont le code est W.

3 Rappel arithmétique : Théorème d'Euler

Rappelons tout d'abord les règles de calcul sur les puissances que vous connaissez déjà :

$$a^n \times a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}$$

Exercice 8 On souhaite calculer 9^{125} $(mod\ 77)$ à la main.
1. Trouvez les diviseurs premiers de 77 et donnez la décomposition de 77.
2. Calculez $\varphi(77)$
3. Enoncez le théorème de Euler pour les variables $a = 9$ et $n = 77$ puis
4. Effectuez la division euclidienne de 125 par $\varphi(n)$
5. et en déduire le calcul de 9^{125} $(mod\ 77)$.

Exercice 9 En utilisant la même technique qu'à l'exercice précédent calculez :
•100^{193} $(mod\ 291)$ •11^{300} $(mod\ 119)$ •190^{3205} $(mod\ 187)$

Exercice 10 Considérons l'entier $a = 9$ et $n = 85$

- retrouvez $\varphi(n)$ et calculez l'inverse de $e = 5$ dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. On notera cet inverse d
- Calculez $a^{(e\times d)}$ et $(a^e)^d$ dans $\mathbb{Z}/n\mathbb{Z}$. Que pensez vous de ces résultats.

4 Chiffrement RSA

Exercice 11 *(Justification de la méthode)*

1. Dans le protocole RSA, expliquez pourquoi l'inverse d de e dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$ existe toujours et comment le calculer.

2. Montrer que x^d $(mod\ n)$ permet de retrouver m.

Dans les deux exercices qui suivent, on pourra utiliser les résultats numériques suivants:
• $319 \equiv 11 \times 29$; $10^{11} \equiv 263(mod\ 319)$; $263^2 = 216 \times 319 + 265$;
• $133^3 \equiv 12(mod\ 319)$; $133^{25} \equiv 133(mod\ 319)$;
• $11^2 \equiv 121(mod\ 280)$; $11^4 \equiv 81(mod\ 280)$; $11^8 \equiv 121(mod\ 280)$; $11^{16} \equiv 81(mod\ 280)$;
• $81 \times 11 \equiv 51(mod\ 280)$; $81 \times 121 \equiv 1(mod\ 280)$.

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 $M = 100$?
2. Calculer d la clé privée correspondant à la clé publique e.
3. Déchiffrer le message $C = 133$.
4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

Exercice 13 *(Cryptographie RSA et authentification)* Un professeur envoie ses notes au secrétariat de l'école par mail. La clé publique du professeur est $(55, 3)$, celle du secrétariat $(33, 3)$.
1. Déterminer la clé privée du professeur et du secrétariat de l'Ecole.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clé RSA du secrétariat. Quel message chiffré correspond à la note 12?
3. Pour assurer l'authenticité de ses messages, le professeur signe chaque note avec sa clé privée et chiffre le résultat avec la clef RSA du secrétariat. Le secrétariat reçoit ainsi le message 23. Quelle est la note correspondante ?

Exercice 14 *(Connaître p et q c'est connaitre $\varphi(n)$)* On suppose que n est un entier naturel non nul dont la décomposition en facteurs premiers est $n = pq$.
1. Exprimer $\varphi(n)$ en fonction de p et q.
2. Exprimer pq et $p+q$ en fonction de n et $\varphi(n)$. En déduire une méthode pour obtenir p et q lorsque l'on connait n et $\varphi(n)$.
3. Si $n = 17063$ et $\varphi(n) = 16800$ calculer p et q.

Exercice 15 *(Attaque RSA par module commun)* Une implémentation de RSA donne à deux personnes (Alice et Bob) le même nombre n (produit de deux nombres premiers) mais des clés (e_A, d_A) et (e_B, d_B) différentes. On suppose de plus que e_A et e_B sont premiers entre eux (ce qui est le plus général). Supposons alors que Alice et Bob chiffrent un même message m et que Oscar intercepte les deux messages $c_A = m^{e_A} \ (mod\ n)$ et $c_B = m^{e_B} \ (mod\ n)$ qu'il sait être deux chiffrements du même message m. Montrer qu'Oscar peut alors très facilement découvrir le message m.

5 Arithmétique : Générateur et problème du logarithme discret

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

1. Donner les éléments inversibles.

2. On note $(\mathbb{Z}/7\mathbb{Z})^\times$ l'ensemble des éléments inversibles et $< a >$ le sous-groupe constitué des éléments suivants $< a >= \{1, a, a^2, a^3, ...\}$.
   L'ordre de a est défini comme le nombre d'éléments distincts de $< a >$.
   Quel est le nombre maximal d'éléments distincts que peut avoir $< a >$ pour $a \in (\mathbb{Z}/7\mathbb{Z})^\times$.

(a) Donner $< 2 >$ puis $< 3 >$. Donner l'ordre de 2 puis de 3. Comparer ces nombres au nombre d'éléments inversibles.

(b) 2 est-il un générateur de $\mathbb{Z}/7\mathbb{Z}$. Même question pour 3.

3. On se place maintenant dans $\mathbb{Z}/9\mathbb{Z}$.

(a) Donner $(\mathbb{Z}/9\mathbb{Z})^\times$.

(b) Donner l'ordre de 4, 7 et 2 dans $(\mathbb{Z}/9\mathbb{Z})^\times$.

(c) Quels sont les générateurs de $(\mathbb{Z}/9\mathbb{Z})^\times$

Exercice 17 Soit $G = (\mathbb{Z}/20\mathbb{Z})^\times$ le groupe des éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.

1. Donner la liste de tous les éléments de G.
2. Pour tout $a \in G$, déterminer le sous groupe $< a >$ engendré par a.
3. G muni de la multiplication est-il un groupe cyclique ?

6 Echange de clés Diffie-Hellman

Exercice 18

1. Soit $p = 17$, prouvez que $g = 3$ est un générateur de $(\mathbb{Z}/17\mathbb{Z})^\times$.
2. 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.

Exercice 19 *Protocole d'échange de clé de Diffie et Hellman*
Supposons qu'Alice et Bob utilisent le protocole d'échange de clés de Diffie et Hellman avec le groupe multiplicatif $\mathbb{Z}_p^*$ des entiers non nuls modulo $p = 367$ avec l'entier $g = 6$ comme générateur.

1. Vérifiez, en utilisant une calculatrice et l'algorithme d'exponentiation rapide, que

   - $g^{p-1} = 1 \pmod p$,
   - et $g^d \neq 1 \pmod p$ pour tout diviseur d de $p - 1$.

   On donne la factorisation de $p - 1$:

   $$p - 1 = 2 \times 3 \times 61.$$

2. En supposant que l'aléa généré par Alice est $x_A = 17$ et celui généré par Bob est $x_B = 33$, calculez la clé commune qu'ils partageront à la fin du protocole.
3. Quelle est la charge de travail d'Ève qui espionne la communication entre Alice et Bob, et qui connaît donc les paramètres p et g, ainsi que les valeurs k_A et k_B échangées durant le protocole, pour trouver le secret commun k, en supposant qu'elle le fait par une recherche exhaustive ?