ENSIBS
2023/2024

Mathématiques pour la cryptographie
Troisième année/A. ABBAR

T.D. 3 : RSA

Exercice 1. Voici un principe simple de cryptographie. Le carré blanc □ est représenté par le chiffre 0. Les lettres A, . . . , Z par les nombres 1, . . . , 26. Le nombre 27 correspond au point et le nombre 28, à la virgule. La table ci-dessous résume ceci :

Symbole à coder	□	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nombre associé	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Symbole à coder	O	P	Q	R	S	T	U	V	W	X	Y	Z	·	,
Nombre associé	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Voici comment on code un mot :

- on remplace les symboles par leurs nombres associés ;
- on multiplie par 2 le nombre associé à chaque symbole ;
- on réduit le résultat obtenu modulo 29 ;
- on trouve les symboles correspondant aux nombres obtenus : ceci nous donne le mot codé.

Par exemple, pour coder le mot «LA» on remplace ses lettres par les nombres $12, 1$. On les multiplie par 2 et on obtient $24, 2$. On les réduit modulo 29 (ici, ce n'est pas nécessaire). La lettre associée à 24 est X ; celle associée à 2 est B. Le mot codé représentant «LA» est «XB».

(1) Coder le mot «MATHS».

(2) Expliquer pourquoi le code est inversible et comment on s'y prend pour décoder.

(3) Décoder le mot «FAHJ».

Exercice 2.

(1) (a) Trouver deux entiers relatifs u_0 et v_0 tels que $7u_0 - 13v_0 = 1$.

(b) En déduire deux entiers relatifs u et v tels que $14u - 26v = 4$.

(c) Déterminer tous les couples (a, k) d'entiers relatifs tels que $14a - 26k = 4$.

(2) On considère deux entiers naturels a et b. Pour tout entier n, on note $r(n)$ le reste de la division euclidienne de $an + b$ par 26. Pour coder un message, on associe d'abord à chaque lettre de l'alphabet un entier compris entre 0 et 25, selon le tableau :

Lettre à coder	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nombre associé	0	1	2	3	4	5	6	7	8	9	10	11	12	13

Lettre à coder	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre associé	14	15	16	17	18	19	20	21	22	23	24	25

Puis pour chaque lettre α du message, on détermine l'entier n associé puis on calcule $r(n)$. La lettre α est alors codée par la lettre associée à $r(n)$.

Supposons dans la suite que F est codée par K et T est codée par O.

(a) Montrer que les entiers a et b sont tels que $5a + b \equiv 10\,[26]$ et $19a + b \equiv 14\,[26]$.

(b) En déduire qu'il existe un entier k tel que $14a - 26k = 4$.

(c) Déterminer tous les couples d'entiers (a, b) compris entre 0 et 25 (inclus) tels que :

$$5a + b \equiv 10\,[26] \quad \text{et} \quad 19a + b \equiv 14\,[26].$$

(3) On suppose que $a = 17$ et $b = 3$.

(a) Coder le message «GAUSS».

(b) Soient n et p deux entiers naturels quelconques. Montrer que si $r(n) = r(p)$, alors $17(n - p) \equiv 0[26]$.

(c) En déduire que deux lettres distinctes de l'alphabet sont codées par deux lettres distinctes.

(4) On suppose que $a = 17$ et $b = 3$.
   (a) Soit n un entier naturel. Montrer que $23r(n) + 9 - n$ est divisible par 26.
   (b) En déduire un procédé de décodage.
   (c) En déduire le décodage de «KTGZDO».

Exercice 3. On se donne un code RSA avec clé $n = 23 \times 37 = 851$ et clé de cryptage $e = 47$. Trouver la clé de décryptage $d \in \{1, \ldots, \varphi(n) - 1\}$ qui satisfait

$$ed \equiv 1 (\mathrm{mod}\, \varphi(n)).$$

Exercice 4. On considère la clef publique RSA $(e, n) = (11, 319)$. Dans toute la suite, on pourra utiliser les résultats numériques suivants :

$$319 = 11 \times 29; \quad 10^{11} \equiv 263 \,(\mathrm{mod}\, 319); \quad 263^2 = 319 \times 216 + 265;$$
$$133^3 \equiv 12 \,(\mathrm{mod}\, 319); \quad 133^{25} \equiv 133 \,(\mathrm{mod}\, 319);$$
$$11^2 \equiv 121 \,(\mathrm{mod}\, 280); \quad 11^4 \equiv 81 \,(\mathrm{mod}\, 280); \quad 11^8 \equiv 121 \,(\mathrm{mod}\, 280);$$
$$11^{16} \equiv 81 \,(\mathrm{mod}\, 280); \quad 95 = 64 + 31; \quad 81 \times 11 \equiv 51 \,(\mathrm{mod}\, 280);$$
$$81 \times 121 \equiv 1 \,(\mathrm{mod}\, 280).$$

(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 5. Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est $(3, 55)$, celle du secrétariat $(3, 33)$.

(1) Déterminer la clé privée du professeur et celle du secrétariat.
(2) Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef 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 6. Alice décide d'utiliser RSA pour permettre aux autres de lui envoyer des messages, et elle choisit comme module $N = pq = 3259499$. Par une faille de sécurité, Eve découvre que $\varphi(N) = (p-1)(q-1) = 3255840$. Déterminer p et q sans demander à un ordinateur de factoriser N (vous pouvez utiliser un ordinateur ou une calculatrice pour les étapes intermédiaires).

Exercice 7. L'objectif de cet exercice est de factoriser $N = 642401$ comme produit de deux nombres premiers distincts, sans demander un ordinateur de le faire. Supposons que vous découvriez que

$$516107^2 \equiv 7 \,(\mathrm{mod}\, N),$$

et que

$$187722^2 \equiv 2^2 \times 7 \,(\mathrm{mod}\, N).$$

Utiliser ces informations pour factoriser N (vous pouvez utiliser un ordinateur ou une calculatrice pour les étapes intermédiaires).

Exercice 8. Une implémentation de RSA donne à deux personnes (Alice et Bob) le même nombre n (produit de deux nombres premiers) mais des clefs (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 $c_A \equiv m^{e_A} \,(\mathrm{mod}\, n)$ et $c_B \equiv m^{e_B} \,(\mathrm{mod}\, n)$ qu'il sait être deux chiffrements du même message m.

Montrer que Oscar peut alors très facilement découvrir le message m.

Exercice 9. (Attaque RSA par texte chiffré bien choisi) Eve intercepte le message c chiffré envoyé par Bob à Alice : $c \equiv m^{e_A} \,(\mathrm{mod}\, n_A)$. Pour déchiffrer c, Eve procède comme suit :

- Eve choisit un entier $0 < r < n_A$ inversible modulo n_A au hasard et calcule $x :\equiv r^{e_A} \,(\mathrm{mod}\, n_A)$;
- Eve calcule $y \equiv x.c \,(\mathrm{mod}\, n_A)$;
- Eve demande à Alice de signer y avec sa clef privée ; Alice renvoie à Eve $u \equiv y^{d_A} \,(\mathrm{mod} n_A)$.

Montrer que Eve peut alors facilement découvrir le message m émis par Bob (on calculera $u.r'$, où r' est un inverse de r modulo n_A. Moralité ?