Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Exercices - Chapitre I

Cryptosystèmes à clés publiques

Exercice 1 (Cryptosystème RSA)

Soit $n \geq 1$ un entier. Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés par des éléments de $\mathbb{Z}/n\mathbb{Z}$. Soit (e, n) sa clé publique.

1) Déterminer sa clé secrète si $(e, n) \in \big\{(139, 265), (31, 3599)\big\}$.
2) Alice choisit le couple $(e, n) = (107, 187)$. Bob lui envoie le cryptogramme 9. Quel est le message secret que Bob souhaite transmettre à Alice ?
3) Alice a perdu sa clé publique et ne possède que sa clé privée égale à $(3, 88)$. Parmi ses papiers, elle retrouve le cryptogramme 7 envoyé par Bob, ainsi que le message décrypté égal à 113. Déterminer sa clé publique.

Exercice 2 (Racines carrées dans $\mathbb{F}_p$)

Soient $p \geq 3$ un nombre premier et a un élément de $\mathbb{F}_p^*$ qui soit un carré dans $\mathbb{F}_p$. Cet exercice concerne la détermination d'une racine carrée x de a dans $\mathbb{F}_p$.

1) Si $p \equiv 3$ mod. 4, montrer que l'on a $x = \pm\, a^{\frac{p+1}{4}}$.
2) Supposons $p \equiv 5$ mod. 8. Justifier l'égalité $a^{\frac{p-1}{4}} = \pm 1$. Montrer que l'on a

$$x = \pm a^{\frac{p+3}{8}} \text{ si } a^{\frac{p-1}{4}} = 1 \quad \text{et que} \quad x = \pm\, 2a.(4a)^{\frac{p-5}{8}} \text{ si } a^{\frac{p-1}{4}} = -1.$$

Le cas où $p \equiv 1$ mod. 8 est moins simple. En toute généralité, on peut procéder comme suit, que p soit ou non congru à 1 modulo 8. On écrit $p - 1$ sous la forme

$$p - 1 = 2^e q \quad \text{avec} \quad q \text{ impair.}$$

Soit G le 2-sous-groupe de Sylow de $\mathbb{F}_p^*$. Il est cyclique d'ordre 2^e. Soit z l'un de ses générateurs.

3) Montrer que a^q appartient à G et que a^q est un carré dans G.
4) Montrer qu'il existe un entier pair k tel que $a^q z^k = 1$ avec $0 \leq k < 2^e$. En déduire que $x = a^{\frac{q+1}{2}} z^{\frac{k}{2}}$ est une racine carrée de a dans $\mathbb{F}_p$.

5) **(Algorithme de Cipolla)** Voici un autre procédé pour extraire des racines carrées dans $\mathbb{F}_p$ qui est dû à Cippola.

5.1) Montrer qu'il y a exactement $\frac{p-1}{2}$ éléments $t \in \mathbb{F}_p$ tels que $t^2 - 4a$ ne soit pas un carré dans $\mathbb{F}_p$.

Soit t un tel élément de $\mathbb{F}_p$. Considérons l'anneau

$$\mathbb{F}_p[X]/(X^2 - tX + a).$$

C'est un corps de cardinal p^2. Soit α la classe de X modulo l'idéal $(X^2 - tX + a)$. (On peut aussi prendre pour α une racine carrée de $t^2 - 4a$ dans $\mathbb{F}_{p^2}$.)

5.2) Montrer que l'on a

$$\left(\alpha^{\frac{p+1}{2}}\right)^2 = a.$$

En particulier, $\alpha^{\frac{p+1}{2}}$ est une racine carrée de a dans $\mathbb{F}_p$.

6) Application : montrer que 5 est un carré dans $\mathbb{F}_{29}$ et déterminer ses racines carrées. On pourra utiliser les deux méthodes précédentes.

Exercice 3 (L'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$)

Soit n un entier naturel non nul. On s'intéresse ici à la description de l'ensemble S des solutions de l'équation $x^2 = 1$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. On notera $|S|$ son cardinal.

1) Supposons n impair. Soit r le nombre de diviseurs premiers de n. Notons

$$n = p_1^{n_1} \cdots p_r^{n_r} \quad \text{avec} \quad n_i \geq 1,$$

la décomposition de n en produit de nombres premiers p_i. Soit A l'ensemble des entiers $a \in \mathbb{Z}$ tels que $a^2 \equiv 1$ mod. n. Soit B l'ensemble des entiers $a \in \mathbb{Z}$ possédant la propriété suivante : pour tout $i = 1, \cdots, r$, il existe $\varepsilon_i = \pm 1$ tel que

$$a \equiv \varepsilon_i \text{ mod. } p_i^{n_i}.$$

1.1) Montrer que $A = B$.

1.2) En déduire que $|S| = 2^r$.

2) Supposons que n soit une puissance de 2. Posons $n = 2^t$ avec $t \geq 1$.

2.1) Expliciter S si $t = 1$ et $t = 2$.

2.2) Supposons $t \geq 3$. Montrer que l'on a

$$S = \Big\{ \pm 1 + 2^t\mathbb{Z}, \pm 1 + 2^{t-1} + 2^t\mathbb{Z} \Big\}.$$

En particulier, on a dans ce cas $|S| = 4$.

3) En déduire $|S|$.

4) Expliciter S si $n = 128$ et $n = 735$.

Remarque. La résolution de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ nécessite, a priori, la connaissance de la factorisation de n en produit de nombres premiers. Si l'on savait résoudre cette équation sans utiliser cette factorisation, il serait alors facile de trouver la factorisation de n. En effet, si a est un entier tel que $a^2 \equiv 1 \bmod. n$ et $a \not\equiv \pm 1 \bmod. n$, le calcul du pgcd de $a+1$ (ou $a-1$) avec n fournit un diviseur non trivial de n. Le problème de la factorisation des entiers serait ainsi résolu, et la sécurité de nombreux cryptosystèmes serait complètement remise en cause.

Exercice 4 (Cryptosystème de Massey-Omura)

Alice souhaite envoyer un message à Bob codé par un élément m d'un groupe cyclique G d'ordre n. Ils utilisent le cryptosystème (sans clé) suivant :

(1) Alice choisit secrètement un entier x_A, premier avec n, tel que $1 < x_A < n$, et elle envoie à Bob l'élément $a = m^{x_A}$.

(2) Bob choisit secrètement un entier x_B, premier avec n, tel que $1 < x_B < n$, et il renvoie à Alice l'élément $b = a^{x_B}$.

(3) Alice calcule l'entier y_A tel que $1 < y_A < n$ et $x_A y_A \equiv 1 \bmod. n$, et elle renvoie à Bob l'élément $c = b^{y_A}$.

(4) Bob calcule l'entier y_B tel que $1 < y_B < n$ et $x_B y_B \equiv 1 \bmod. n$, et il détermine c^{y_B}.

1) Montrer que l'on a $m = c^{y_B}$.

2) On prend $G = \mathbb{F}_{19}^*$. Supposons qu'Alice choisisse l'entier $x_A = 5$ et qu'elle envoie à Bob $a = \overline{2}$. Trouver l'élément m correspondant.

Exercice 5 (Algorithme de El Gamal)

Alice souhaite se faire envoyer des messages confidentiellement en utilisant cet algorithme. Elle considère pour cela le corps

$$K = \mathbb{F}_2[X]/(X^4 + X + 1).$$

Soit α la classe de X modulo $(X^4 + X + 1)$.

1) Justifier que K est un corps et montrer que α est un générateur de K^*.

Alice rend public le triplet $(K, \alpha, \alpha^2 + 1)$, et Bob envoie des messages à Alice en utilisant cette clé publique.

2) Bob veut coder le message $1 + \alpha$ pour l'envoyer à Alice. Conformément à l'algorithme, il choisit un entier x compris entre 2 et 14, par exemple $x = 3$. Que transmet-il à Alice ?

3) Vous interceptez le message $(\alpha^3, \alpha^3+\alpha^2+\alpha)$. Quel était le message envoyé par Bob ?

Exercice 6 (Protocole de Diffie-Hellman)

Alice et Bob décident d'utiliser ce protocole pour se fabriquer une clé secrète. Pour cela, ils rendent public le couple (K, α) où

$$K = \mathbb{F}_3[X]/(X^3+2X+1) \quad \text{et} \quad \alpha = X + (X^3+2X+1).$$

1) Vérifier que K est un corps et que α est un générateur de K^*.

Conformément à ce protocole, Alice choisit un entier a compris entre 2 et 25, par exemple $a = 9$, et transmet α^9 à Bob. Ce dernier choisit un entier b compris entre 2 et 25 et lui renvoie l'élément $\alpha^b = 2+\alpha+2\alpha^2$.

2) Déterminer b.

3) Quelle est la clé secrète d'Alice et Bob ? On déterminera ses coordonnées dans la base $(1, \alpha, \alpha^2)$ de K sur $\mathbb{F}_3$.

Exercice 7 (Protocole de Diffie-Hellman dans un corps de cardinal p^2)

Soit p un nombre premier de Mersenne : on a $p = 2^\ell - 1$ où ℓ est un nombre premier. Posons

$$K = \mathbb{F}_p[X]/(X^2+1).$$

Notons i la classe de X modulo (X^2+1).

1) Montrer que K est « le » corps à p^2 éléments.

2) Soient a et b des éléments de $\mathbb{F}_p$ tels que a^2+b^2 soit un générateur de $\mathbb{F}_p^*$.

2.1) Soit $m \geq 1$ un entier. Montrer que si $(a+ib)^m$ est dans $\mathbb{F}_p$, alors $p+1$ divise m.

2.2) En déduire que $a+ib$ est un générateur de K^*.

3) Montrer que l'hypothèse faite dans la question précédente n'est pas restrictive, autrement dit que tout élément de $\mathbb{F}_p$, et plus généralement d'un corps fini, est somme de deux carrés.

4) En déduire que $3+2i$ et $4+i$ sont des générateurs du groupe $\mathbb{F}_{31^2}^*$.

5) Deux personnes Alice et Bob souhaitent se construire une clé de chiffrement commune en utilisant le protocole de Diffie-Hellman dans le groupe $\mathbb{F}_{31^2}^*$, avec le générateur $4+i$.

5.1) Alice choisit secrètement l'entier 193 et Bob envoie à Alice l'élément $1+19i$. Quelle est la clé commune de chiffrement ?

5.2) Quel est élément de K^* que doit envoyer Alice à Bob pour qu'il connaisse la clé ?

Exercice 8 (Cryptosystème de Rabin)

Une personne Alice souhaite communiquer de manière sécurisée en utilisant le cryptosystème de Rabin. Pour cela, elle choisit deux nombres premiers p et q et publie l'entier $n = pq$.

Bob souhaite faire parvenir à Alice le message 22. Il lui transmet pour cela le cryptogramme 1. Par ailleurs, Alice reçoit le cryptogramme 2 envoyé par Bernard.

1) Déterminer l'entier n.
2) Quels sont les quatre décryptages possibles du message envoyé par Bernard ?

Exercice 9 (Sac à dos)

1) Pour les suites d'entiers et « volumes » V suivants, résoudre le problème du sac à dos correspondant :

$$(2, 3, 7, 20, 35, 69) \text{ et } V = 45, \quad (1, 2, 5, 9, 20, 49) \text{ et } V = 73,$$

$$(1, 3, 7, 12, 22, 45) \text{ et } V = 67, \quad (4, 5, 10, 30, 50, 101) \text{ et } V = 186.$$

2) Soit $(v_i)_{i\geq 0}$ une suite d'entiers positifs telle que l'on ait $v_{i+1} > 2v_i$ pour tout i. Montrer qu'elle est super croissante, i.e. que l'on a

$$v_i > \sum_{k=0}^{i-1} v_k \quad \text{pour tout } i \geq 1.$$

3) Montrer que la suite d'entiers strictement positifs super croissante dont chaque terme est le plus petit possible est la suite $(2^i)_{i\geq 0}$.

Exercice 10 (Cryptosystème de Merkle-Hellman)

Alice et Bob utilisent le cryptosystème du sac à dos de Merkle-Hellman pour communiquer. L'alphabet utilisé est l'alphabet usuel, chaque lettre étant codée par un entier écrit en binaire avec cinq composantes $(a_4a_3a_2a_1a_0)_2$ (on a A=$(00000)_2$, $\cdots$, Z=$(11001)_2$). Les unités de message sont des mots de trois lettres (ils ont donc quinze composantes). Les notations étant celles figurant dans le paragraphe 7 du cours, Alice choisit la suite d'entiers $(4, 5, 12, 23, 45)$, ainsi que $m = 400$ et $a = 381$.

1) Vérifier que ces données sont conformes au principe d'utilisation de ce cryptosystème.
2) Déterminer la clé publique d'Alice.
3) Bob veut envoyer à Alice le message OUI. Indiquer le procédé qu'il doit suivre et comment Alice retrouve-t-elle le message.