

## TD4 : Chiffrements asymétriques

### 1. Exemple de clé partagée Diffie-Hellman

Alice et Bob souhaitent convenir ensemble d'une clé secrète pour chiffrer leurs futures communications, sans pour autant prendre le risque de se rencontrer. Ils vont pour cela utiliser le protocole de Diffie-Hellman pour établir une clé partagée, détaillé ci-dessous. Alice et Bob ont accès à deux nombres publics : un nombre premier  $p = 17$  et un nombre compris entre 2 et  $p - 1$ , appelé générateur et noté  $g$ .  $p$  est en théorie très grand pour assurer la sécurité. Alice tire un entier aléatoire  $a$  compris entre 2 et  $p - 1$ , et Bob tire un entier aléatoire  $b$  compris entre 2 et  $p - 1$ . Ici on prend  $a = 3$  et  $b = 4$ . Le protocole de Diffie-Hellman pour échanger une clé fonctionne comme suit :

- (a) Alice envoie à Bob :  $A = g^a \mod p$ .
- (b) Bob envoie à Alice :  $B = g^b \mod p$
- (c) Alice et Bob calculent ensuite un nombre commun  $K = A^b \mod p = B^a \mod p = g^{ab} \mod p$

Calculez un générateur  $g$ , et la clé  $DH$  partagée par Alice et Bob correspondante.

### 2. Chiffrement ElGamal

On rappelle que le schéma de chiffrement El Gamal fonctionne de la manière suivante : soit  $m$  un message et  $r$  un élément aléatoire de  $\{1, \dots, p - 1\}$ , on a :

$$c = (c_1, c_2) \text{ avec } c_1 = g^r \mod p \text{ et } c_2 = m \cdot h^r \mod p$$

où  $(g, p, h = g^x \mod p)$  est la clé publique du destinataire construite à partir d'un élément secret  $x$  tiré aléatoirement dans  $\{1, \dots, p - 1\}$ . L'élément  $x$  est la clef privée.

- (a) Comment déchiffrons t-on le mchiffré ?
- (b) Soit  $x = 2$  et  $(p, g) = (17, 3)$ , déchiffrez  $c = (4, 2)$ .
- (c) Quelle est la valeur de  $r$  correspondant au chiffré précédent ?
- (d) Rappelez le problème du logarithme discret.
- (e) Montrez que si l'on sait résoudre le logarithme discret alors on sait déchiffrer le chiffrement d'ElGamal.
- (f) On suppose qu'Alice envoie des message à Bob. Comme elle est fainéante, elle choisit d'utiliser plusieurs fois le même  $r$ . Quelle pourrait être les conséquences d'une telle paresse ? (On suppose qu'Eve connaît le message clair  $m$  d'un chiffré envoyé par Alice.)
- (g) Que pouvez vous dire de la malléabilité du chiffrement ElGamal ?

### 3. Courbe elliptique

Une courbe elliptique est l'ensemble des solutions d'une équation du type  $y^2 = x^3 + ax + b$ , où les coefficients, ainsi que les solutions recherchées, appartiennent à un corps fini. On manipule ici un petit exemple sur  $\mathbb{Z}/5\mathbb{Z}$ , qui est un corps : on peut effectuer dedans des additions (modulo 5) et des produits (modulo 5). En outre, chaque élément non nul possède un inverse.

- (a) Quels sont les éléments de  $\mathbb{Z}/5\mathbb{Z}$  ? Pour chacun, donner deux entiers de  $\mathbb{Z}$  représentant ce même élément de  $\mathbb{Z}/5\mathbb{Z}$ .

- (b) Pour chaque élément de  $\mathbb{Z}/5\mathbb{Z}$ , calculer son carré dans  $\mathbb{Z}/5\mathbb{Z}$ . Combien le carré prend-il de valeurs distinctes sur  $\mathbb{Z}/5\mathbb{Z}$  ?
- (c) Pour chaque élément de  $\mathbb{Z}/5\mathbb{Z}$ , calculer  $f(x) = x^3 - 1$ . En déduire les solutions de l'équation

$$(E) \quad y^2 = x^3 - 1$$

(il y a 5 solutions distinctes).

- (d) Quelle est l'équation de la droite  $\Delta$  passant par les points de coordonnées  $(0, 2)$  et  $(1, 0)$  ?
- (e) Soit  $(x, y)$  un point de la droite  $\Delta$  satisfaisant aussi l'équation  $(E)$ . L'abscisse  $x$  est alors solution d'une équation qu'on notera  $P$ . Quelle est cette équation (l'écrire – c'est une équation de degré 3).
- (f) Que peut-on dire de la somme des racines de  $P$  ? Connaissez-vous déjà les racines ? En déduire une nouvelle.
- (g) Si on "dessine" les points solution de  $(E)$ , la droite  $\Delta$  ressemble-t-elle à une droite ? Faire un dessin plus convaincant sur une feuille à petits carreaux, en répétant plusieurs fois un carré de côté 5 dans lequel vous aurez placé les points (ainsi, le "même" point a vocation à apparaître plusieurs fois sur votre dessin).

$\times$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1