

# TD 5 de Cryptologie

Lundi 14 novembre 2005

## 1 Cryptosystème Elgamal

On se place dans un groupe  $G$  cyclique de taille  $q$ , de générateur  $g$ .

### 1.1 Génération de clef

- Alice choisit  $x$  au hasard dans  $\{0, 1, \dots, q - 1\}$ .
- Alice calcule  $h = g^x$  dans  $G$  (si  $G$  est noté multiplicativement).

$x$  est la clef secrète d'Alice;  $h, G, g$  et  $q$  sa clef publique.

1. Pour le groupe  $G = (\mathbb{Z}/13\mathbb{Z}, +)$  calculer  $q$ , le nombre de générateurs et les décrire.
2. Même question pour le groupe  $G = (\mathbb{Z}/42\mathbb{Z}, +)$ .
3. Même question pour le groupe  $G = (\mathbb{F}_{17}^*, *)$ .
4. Dans le groupe  $G = (\mathbb{Z}/13\mathbb{Z}, +)$  on choisit  $g = 2$ . Calculer la clef publique associée à la clef privée  $x = 5$ .
5. Est-il possible de retrouver la clef privée à partir de la clef publique dans  $G = (\mathbb{Z}/42\mathbb{Z}, +)$  ? Généraliser la méthode à  $(\mathbb{Z}/n\mathbb{Z}, +)$  pour  $n \geq 2$ .

### 1.2 Chiffrement

Bob souhaite envoyer un message  $m \in \{0, 1, \dots, q - 1\}$  à Alice.

- Bob choisit  $y \in \{0, 1, \dots, q - 1\}$  au hasard.
  - Bob calcule  $c_1 = g^y, c_2 = m \cdot h^y$ .
  - Bob envoie  $(c_1, c_2)$  à Alice.
6. Retrouver la procédure de déchiffrement d'Alice.
  7. Montrer que le problème de déchiffrer un message sans connaître la clef privée est plus facile que le problème du logarithme discret.
  8. Dans  $G = (\mathbb{F}_{17}^*, *)$  on prend  $x = 13, g = 3$ .
    - Calculer la clef publique correspondante.
    - Calculer le chiffré de  $m = 8$  pour  $y = 9$ .
    - Détailler le déchiffrement.

### 1.3 Sécurité

Pour un groupe cyclique  $G$  de générateur  $g$  on appelle problème Diffie-Hellman calculatoire ( $CDH$ ) celui de trouver  $g^{ab}$  connaissant  $(g, g^a, g^b)$ .

Le problème Diffie-Hellman décisionnel ( $DDH$ ) est celui de savoir distinguer les tuples  $(g, g^a, g^b, g^{ab})$  des couples  $(g, g^a, g^b, t)$  où  $t$  est un élément aléatoire de  $G$ , c'est-à-dire distinguer des tuples "Diffie-Hellman" de tuples aléatoires.

9. Montrer que le problème du logarithme discret est plus difficile que  $CDH$ .
10. Montrer que le problème  $CDH$  est plus difficile que  $DDH$ .
11. Des groupes  $G_1, G_2$  et  $G_3$  dire lequel est le plus sûr *a priori* pour une utilisation dans le cryptosystème Elgamal sachant que :
  - le problème du logarithme discret est dur dans  $G_1$ ,
  - le problème  $CDH$  est dur dans  $G_2$ ,
  - le problème  $DDH$  est dur dans  $G_3$ .
12. Si  $CDH$  est dur mais  $DDH$  facile, que peut faire un attaquant ?

#### 1.3.1 Sécurité du chiffrement Elgamal dans $G = \mathbb{F}_p^*$

Pour  $p$  premier dans le corps  $\mathbb{F}_p$  à  $p$  éléments on dit que  $x \neq 0$  est un résidu quadratique s'il existe  $y \in \mathbb{F}_p$  tel que  $x = y^2$ .

13. Montrer que si  $x$  est un résidu quadratique alors  $x^{(p-1)/2} = 1$ .
14. Montrer que  $\varphi : \begin{cases} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^2 \end{cases}$  est un morphisme et calculer son noyau. En déduire le nombre de résidus quadratiques et de non résidus quadratiques dans  $\mathbb{F}_p$ .
15. Montrer que si  $g$  est un générateur de  $\mathbb{F}_p^*$  alors  $g$  n'est pas un résidu quadratique.
16. Pour  $a \in \{1, p-1\}$ , comment déterminer simplement si  $g^a$  est un résidu quadratique ?
17. On note  $\chi(x) = 1$  si  $x$  est un résidu quadratique,  $-1$  sinon. Calculer  $\chi(g^{ab})$  en fonction de  $\chi(g^a)$  et  $\chi(g^b)$ .
18. En déduire une méthode probabiliste pour répondre au problème  $DDH$ , et calculer l'avantage de l'adversaire.