Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2022–23

Cryptographie à clé publique – Feuille de TD 4

17/02/2023

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/clef-publique.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

Exercice 1. $(\star)$ ElGamal : application directe.

En guise d'exercice d'application, on considère le cryptosystème d'ElGamal « brut » dans le groupe multiplicatif $\mathbb{F}_p^\times$ où $p = 19$. On prend comme générateur $g = 2$.

Alice produit la clé privée $a = 5$.

Question 1.– Quelle est la clé publique ?

Question 2.– Chiffrer le message $m = 10$ avec l'aléa $k = 7$.

Question 3.– Déchiffrer $c = (12, 7)$ avec la clé privée d'Alice.

Exercice 2. $(\star)$ Attaque sur l'homomorphisme du chiffrement d'ElGamal.

Question 1.– Démontrer que le chiffrement d'ElGamal dans sa version « brute », présenté dans un groupe $(\mathbb{G}, \cdot)$, est homomorphe. Autrement dit, démontrez que si m et m' sont deux clairs de chiffrés $c = (c_1, c_2)$ et $c' = (c'_1, c'_2)$, alors un chiffré possible de $m \cdot m'$ est $(c_1 \cdot c'_1, c_2 \cdot c'_2)$.

Application. Bob souhaite acheter une maison à Clara. Pour cela, il doit transmettre sa promesse d'achat à Alice, une notaire. Sur cette promesse d'achat, on suppose qu'il inscrit uniquement la somme qu'il souhaite payer à Clara.

Alice, la notaire, souhaite utilise le chiffrement ElGamal « brut » dans le groupe multiplicatif $\mathbb{F}_p^\times$, afin de sécuriser la valeur entière (en euros) que Bob souhaite inscrire sur sa promesse d'achat.

Précisons que la valeur du nombre premier p a été choisie suffisamment grande par Alice, pour que le logarithme discret dans $\mathbb{F}_p^\times$ soit irrésoluble.

Question 2.– Supposons que Clara arrive à intercepter le message chiffré de Bob. Comment peut-elle modifier ce chiffré pour faire croire à Alice que Bob souhaite payer 2 fois plus que la somme initialement prévue ?

Question 3.– Que proposeriez-vous à la notaire pour empêcher cela ?

Exercice 3. $(\star\star)$ Chiffrement ElGamal avec aléa non-parfait.

Dans cet exercice, on s'intéresse au système de chiffrement ElGamal dans un groupe cyclique $\mathbb{G}$ d'ordre q. On note g un générateur de $\mathbb{G}$, et on rappelle qu'une paire de clefs consiste en un entier $a \in \{1, \ldots, q-1\}$ (la clef privée) et l'élement de groupe $g^a \in \mathbb{G}$ (la clé publique).

On rappelle ci-dessous les algorithmes de chiffrement et déchiffrement d'ElGamal.

Algorithme 1 : Algorithme de chiffrement

Entrée : un message $m \in \mathbb{G}$, la clé publique $\alpha = g^a \in \mathbb{G}$
Sortie : un chiffré $c = (c_1, c_2) \in \mathbb{G}^2$
1 Choisir aléatoirement $r \in \mathbb{Z}/q\mathbb{Z}$.
2 Calculer $c_1 = g^r$.
3 Calculer $c_2 = m\alpha^r$.
4 Retourner $c = (c_1, c_2)$.

Algorithme 2 : Algorithme de déchiffrement

Entrée : un chiffré $c = (c_1, c_2) \in \mathbb{G}^2$, la clé privée $a \in \mathbb{Z}/q\mathbb{Z}$
Sortie : un message $m' \in \mathbb{G}$
1 Calculer $x = c_1^a$.
2 Calculer $m' = c_2/x$.
3 Retourner m'.

Question 1.– Dans cette question, on suppose que :

— le groupe $\mathbb{G}$ est un groupe multiplicatif $\mathbb{F}_p^\times$

— à l'étape 1 de l'algorithme de chiffrement, Bob choisit r uniformément dans $\{0, \ldots, 2^{32} - 1\}$

Que dire de la sécurité du système dans ce contexte ? Donner une réponse quantifiée en nombre de bits, et justifier.

On suppose maintenant, et dans toute la suite de l'exercice, que lors de l'étape 1 de l'algorithme de chiffrement, Bob utilise un générateur d'aléa de mauvaise qualité, défini ainsi :

— la première valeur aléatoire r_0 est engendrée par un tirage uniforme dans $\mathbb{Z}/q\mathbb{Z}$

— les valeurs aléatoires notées $r_1, r_2, \ldots, r_i, \ldots$ qui sont ensuite engendrées par le générateur, satisfont :

$$r_{i+1} = ur_i + v \mod q$$

où u et v sont des éléments fixes de $\mathbb{Z}/q\mathbb{Z}$.

Question 2.– Supposons qu'un attaquant connaisse u et v. Présenter une attaque contre le système permettant de déchiffrer un chiffré $\boldsymbol{c} = (c_1, c_2)$. On indiquera **précisément** le mode d'attaque.

Question 3.– On suppose maintenant que les valeurs de u et v sont inconnues de l'attaquant, mais restent inférieures à une constante K. Peut-on adapter l'attaque précédente ? Si oui, donner la complexité de l'attaque en fonction de K.

Exercice 4. $(\star\star)$ Une variante du chiffrement ElGamal.

Dans cet exercice, on se place dans le corps $\mathbb{F}_p$, avec p premier, et on considère g un générateur de $\mathbb{F}_p^\times$.

On s'intéresse à une variante du chiffrement ElGamal. La clé privée est toujous un élément aléatoire $a \in \mathbb{Z}/(p-1)\mathbb{Z}$, et la clé publique est toujours $\alpha = g^a$. En revanche, l'espace des clairs du système est $\mathbb{F}_p$, et celui des chiffrés est $\mathbb{F}_p \times \mathbb{F}_p^\times$. Enfin, l'algorithme de chiffrement est le suivant.

Algorithme 3 : Algorithme de chiffrement

Entrée : un message $m \in \mathbb{F}_p$, une clé publique α
Sortie : un chiffré $c = (c_1, c_2) \in \mathbb{F}_p^\times \times \mathbb{F}_p$

1 Choisir aléatoirement $r \in \mathbb{Z}/(p-1)\mathbb{Z}$.
2 Calculer $c_1 = g^r \mod p$.
3 Calculer $c_2 = \alpha^r + m$.
4 Retourner $c = (c_1, c_2)$.

Question 1.– Décrire précisément l'algorithme de déchiffrement associé (entrées, sortie, étapes), ainsi que sa complexité en fonction de p.

Question 2.– Supposons que Bob réutilise le même aléa à chaque chiffrement. Présenter une attaque contre le système en indiquant le mode d'attaque utilisé (c'est-à-dire, les moyens de l'attaquant).

Question 3.– Pourriez-vous instancier ce cryptosystème dans le groupe de points d'une courbe elliptique (au lieu de $\mathbb{F}_p$) ? Justifier : si oui, préciser les changements à effectuer ; si non, donner les obstacles.

Exercice 5. 💻 $(\star)$ Implantation de *baby-step giant-step*.

Question 1.– Implanter l'algorithme de calcul de logarithme discret dit « pas de bébé – pas de géant », dans le groupe multiplicatif d'un corps fini $\mathbb{F}_p^\times$.

Question 2.– Trouver les logarithmes discrets de $y \in \mathbb{F}_p^\times$ en base g pour les valeurs de p, g et y suivantes :

p	g	y
101	2	78
10007	5	8804
1000003	2	832469
100000007	5	29220559
10000000019	2	9521998688
1000000000039	3	855427796771

Jusqu'à quelle valeur de p le temps de calcul du logarithme discret par l'algorithme « pas de bébé – pas de géant » reste-t-il raisonnable sur votre machine ?

Et pour la recherche exhaustive ?