Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2025–26

Cryptographie à clé publique – Solutions feuille de TD 3

11/02/2026

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`https://lvzl.fr/teaching/2025-26/cp.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.

Solutions de l'Exercice 1.

Solution Q1. La clé publique est $\alpha = g^a = 2^5 \equiv 13 \mod p$.

Solution Q2. Pour chiffrer le message $m = 10$ avec la valeur aléatoire $k = 7$, on calcule $b_1 = g^k$ et $b_2 = m\alpha^k$. Concrètement, on obtient :

$$b_1 = 2^7 \equiv 14 \mod p \qquad \text{et} \qquad b_2 = 10 \times 2^{13} \equiv 5 \mod p$$

Solution Q3. On obtient $m' = 7 \times 12^{-5} \equiv 8 \mod p$.

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

Informellement, on dit d'un chiffrement est homomorphe si une certaine opération sur les clairs (par exemple, la somme des clairs) se retranscrit par une opération sur les chiffrés que l'on peut effectuer sans connaître la clé privée (par exemple, le produit des chiffrés).

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 ?

Solutions de l'Exercice 2.

Solution Q1. Soit n l'ordre de $\mathbb{G}$, et $\alpha = g^a$ la clef publique. Le chiffré c a été construit de la sorte : une valeur $k \in \mathbb{Z}/n\mathbb{Z}$ a été tirée aléatoirement, puis on a défini :

$$c = (c_1, c_2) = (g^k, m\alpha^k)$$

De même, $c' = (c'_1, c'_2) = (g^{k'}, m'\alpha^{k'})$ avec un certain $k' \in \mathbb{Z}/n\mathbb{Z}$ tiré aléatoirement et indépendamment de k. On a donc :

$$c_1 c'_1 = g^k g^{k'} = g^{k+k'}$$

d'une part, et d'autre part :

$$c_2 c'_2 = m\alpha^k m'\alpha^{k'} = (mm')\alpha^{k+k'}$$

Le couple $(c_1 c'_1, c_2 c'_2)$ correspond donc à un chiffré de mm' avec l'aléa $k + k'$.

Solution Q2. Clara intercepte $c = (c_1, c_2) = (g^k, m\alpha^k)$, où m est la somme en euros. Pour faire croire que Bob souhaite payer deux fois plus, il lui suffit de transformer (c_1, c_2) en $(c_1, 2c_2)$.

Solution Q3. La notaire peut utiliser OAEP pour empêcher cette attaque.

Exercice 3. ($\star\star$) ElGamal : réutilisation de l'aléa pour le chiffrement.

Dans cet exercice, on suppose que Bob veut envoyer plusieurs messages $(m_1, \ldots, m_\ell)$ à Alice, en utilisant le schéma de chiffrement d'ElGamal. On se place dans un groupe $\mathbb{G}$ d'ordre n et de générateur γ, et la clef publique d'Alice est $\alpha = \gamma^a \in \mathbb{G}$.

Question 1.– Pour économiser des calculs, Bob utilise le même élément aléatoire $k \in \mathbb{Z}/n\mathbb{Z}$ pour chiffrer tous les messages m_i. Expliquer en quoi ce choix fragilise le système.

On suppose maintenant que Bob engendre un nouvel aléa pour chiffrer chaque message m_i. Pour cela, il utilise un générateur d'aléa, mais cet aléa est biaisé. En effet, la i-ème valeur $k_i \in \mathbb{Z}/n\mathbb{Z}$ engendrée par le générateur satisfait la relation

$$k_i = k_{i-1} + r \mod n\,,$$

où $r \in \mathbb{Z}/n\mathbb{Z}$ est un élément connu de tous.

Question 2.– Déterminer une relation entre le chiffré du i-ème message m_i et celui de m_1. En déduire une attaque à clair connu sur le système.

Solutions de l'Exercice 3.

Solution Q1. Le chiffré c_i du message m_i vaut $c_i = (g^k, m_i\alpha^k)$ pour tout i.

On peut alors justifier la fragilité du système de différentes manières.

1. Le premier élément du chiffré ne dépend pas de i (il est constant égal à g^k). On peut donc distinguer une série de chiffrés d'une série d'élements aléatoires de $\mathbb{G} \times \mathbb{G}$. Le schéma de chiffrement n'est donc pas indistinguable, quel que soit le mode d'attaque.
2. Si l'on connaît l'un des m_i, alors on peut retrouver tous les autres m_j, pour $j \neq i$. En effet, le second terme de c_i permet de retrouver $\alpha^k = c_i[2]/m_i$, puis de calculer $m_j = c_j[2]/\alpha^k$. On peut donc mettre en place une attaque à clair connu.

Solution Q2. Notons $c_i = (\beta_{1,i}, \beta_{2,i})$ le chiffré de m_i. On a alors :

$$\beta_{1,i} = \gamma^{k_i} = \gamma^{k_1 + r(i-1)} \quad \text{et} \quad \beta_{2,i} = m_i \alpha^{k_i} = m_i \alpha^{k_1 + r(i-1)}.$$

Le message m_1 est inversible dans le groupe $\mathbb{G}$ donc on obtient

$$\beta_{1,i} = \beta_{1,1} \gamma^{r(i-1)} \quad \text{et} \quad \beta_{2,i} = m_i m_1^{-1} \beta_{2,1} \alpha^{r(i-1)}$$

L'attaque à clair connu se déduit aisément de la dernière formule. Supposons que l'on connaisse, par exemple, la valeur du message m_1 et de son chiffré associé c_1. Comme on connaît également r, on peut en déduire la valeur d'un message m_i qui a été chiffré en c_i :

$$m_i = m_1 \frac{\beta_{2,i}}{\beta_{2,1}} \alpha^{-r(i-1)}.$$

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 1 : 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.

Solutions de l'Exercice 4.

Solution Q1.

Algorithme 2 : Algorithme de déchiffrement

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

1 Calculer $m' = c_2 - (c_1)^a \mod p$.
2 Retourner m'.

Sa complexité est $O(\log(p))$ opérations (multiplications, carrés ou additions) dans $\mathbb{F}_p$.

Solution Q2. On peut monter une attaque à clair connu, par exemple. Soit $(c_1 = g^r, c_2 = \alpha^r + m)$ à déchiffrer. On demande un échantillon clair/chiffré quelconque, disons $(c_1' = g^r, c_2' = \alpha^r + m')$ où m' est connu de l'attaquant. Il suffit alors de calculer $m = c_1 - c_1' + m'$.

Solution Q3. Il faut voir que, dans le système décrit ci-dessus, il faut savoir additionner et multiplier dans la structure algébrique proposée. C'est possible dans $\mathbb{F}_p$, mais impossible (directement) dans $E(\mathbb{F}_p)$.

On peut donc répondre « non » avec la justification ci-dessus.

Une réponse « oui » était également possible : l'idée est de considérer une fonctionde de hachage $H : E(\mathbb{F}_p) \to \{0,1\}^t$, en supposant que le message est de longueur t (quitte à le décomposer). Puis, étant donnée une paire de clefs $(\texttt{sk} = a, \texttt{pk} = A = aG)$, le chiffré devient $(C_1, \boldsymbol{c}_2) = (rG, H(rA) \oplus \boldsymbol{m})$, et le déchiffrement consiste à calculer $H(aC_1) \oplus \boldsymbol{c}_2$.
