Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2025–26

Cryptographie à clé publique – Solutions feuille de TD 5

04/03/2026

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. $(\star)$ Signature ElGamal : réutilisation de l'aléa.

On considère le schéma de signature ElGamal dans lequel le message est haché avant d'être signé. On choisit comme groupe $\mathbb{F}_p^\times$, et on a donc à disposition une fonction de hachage $H : \{0,1\}^* \to \mathbb{Z}/(p-1)\mathbb{Z}$.

La génération de clés est identique au cadre du cours, mais l'algorithme de signature est légèrement modifié pour donner l'Algorithme 1. Pour la vérification de la signature, on effectue également un haché du message avant de tester l'égalité requise.

Algorithme 1 : Algorithme de signature d'ElGamal avec fonction de hachage

Entrée : un message $\boldsymbol{m} \in \{0,1\}^*$, la clé privée $a \in \{1,\dots,p-2\}$
Sortie : une signature $s \in \mathbb{F}_p^\times \times \{0,\dots,p-2\}$

1 Choisir $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ inversible.
2 Calculer $b = g^k \mod p$.
3 Calculer $h = H(\boldsymbol{m})$.
4 Calculer $c = (h - ab)k^{-1} \mod (p-1)$.
5 Retourner la signature $s = (b, c)$.

On suppose dans cet exercice qu'**Alice réutilise le même aléa k pour plusieurs de ses signatures**, et l'on souhaite en déduire une faille de sécurité importante.

Question 1.– Soient $s = (b,c)$ et $s' = (b',c')$ les signatures de deux messages distincts m et m' effectuées avec le même aléa k. Comparer b et b', puis déterminer une égalité liant $h = H(\boldsymbol{m})$, $h' = H(\boldsymbol{m}')$, a, b, c et c'.

Question 2.– En déduire une attaque à message connu sur la clé privée d'Alice, qui réussit avec très bonne probabilité.

Solutions de l'Exercice 1.

Solution Q1. Comme k est le même pour toutes les signatures, on a

$$b \equiv g^k \equiv b' \mod p\,.$$

On obtient alors

$$(h-ab)c' \equiv (h-ab)(h'-ab)k^{-1} \equiv (h'-ab)(h-ab)k^{-1} \equiv (h'-ab)c \mod (p-1)$$

Solution Q2. On cherche la clé privée a d'Alice. Pour cela, on demande à Alice deux signatures $s = (b,c)$ et $s' = (b',c')$ quelconques (pour deux messages $\boldsymbol{m}$ et $\boldsymbol{m}'$ connus mais non-choisis). On a alors :

$$(h-ab)c' \equiv (h'-ab)c \mod (p-1) \quad \iff \quad a \equiv \frac{h'c - hc'}{b(c-c')} \mod (p-1)$$

Pour résumer :

1. On calcule $h = H(\boldsymbol{m})$ et $h' = H(\boldsymbol{m}')$.
2. On calcule l'inverse de $b(c-c')$ modulo $p-1$ (s'il est inversible).
3. On retourne $a = \frac{h'c-hc'}{b(c-c')} \mod (p-1)$

Cette attaque fonctionne si b et $c-c'$ sont inversibles modulo $p-1$, ce qui est vérifié avec bonne probabilité en les considérant comme des éléments aléatoires de $\mathbb{Z}/(p-1)\mathbb{Z}$.

Remarque. On pourrait également demander à Alice davantage de signatures pour augmenter la probabilité de réussite.

Exercice 2. $(\star\star)$ Une proposition de schéma de signature.

Dans cet exercice, on considère un nombre premier p pour lequel le problème du logarithme discret dans $\mathbb{F}_p^\times$ est supposé difficile. On note g un générateur du groupe cyclique $\mathbb{F}_p^\times$. Enfin, on considère une fonction de hachage $H : \{0,1\}^* \to \mathbb{Z}/(p-1)\mathbb{Z}$.

Un schéma de signature est décrit par les trois algorithmes suivants.

Algorithme 2 : Génération de clefs

Entrée : les paramètres du système
Sortie : une paire de clefs publique/privée

1 Tirer x aléatoirement dans $\mathbb{Z}/(p-1)\mathbb{Z}$.
2 Tirer y aléatoirement dans $\mathbb{Z}/(p-1)\mathbb{Z}$.
3 Calculer $X = g^x \mod p$ et $Y = g^y \mod p$.
4 La clef publique est $\mathtt{pk} = (X,Y)$, la clef privée est $\mathtt{sk} = (x,y)$.

Algorithme 3 : Signature

Entrée : un message $\boldsymbol{m} \in \{0,1\}^*$, la clé privée $\mathtt{sk} = (x,y)$
Sortie : une signature $s \in \mathbb{Z}/(p-1)\mathbb{Z}$

1 Calculer $h = H(\boldsymbol{m}) \in \mathbb{Z}/(p-1)\mathbb{Z}$
2 Calculer et retourner l'élément $s = xh + y \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Algorithme 4 : Vérification

Entrée : une signature $s \in \mathbb{Z}/(p-1)\mathbb{Z}$, un message $\boldsymbol{m} \in \{0,1\}^*$, la clé publique $\mathtt{pk} = (X, Y)$

Sortie : vrai ou faux

1 Calculer $h = H(\boldsymbol{m}) \in \mathbb{Z}/(p-1)\mathbb{Z}$.

2 Calculer $a = g^s \mod p$ et $b = X^h Y \mod p$.

3 Faire le test $a \equiv b \mod p$ et retourner le booléen associé.

Question 1.– Vérifier que le schéma de signature est valide.

Question 2.– Proposer une attaque sur la clé privée $\mathtt{sk} = (x, y)$. On précisera le moyen d'attaque utilisé.

Solutions de l'Exercice 2.

Solution Q1. On a bien

$$a \equiv g^s \equiv g^{xh+y} \equiv (g^x)^h g^y \equiv X^h Y \mod p$$

Solution Q2. L'idée est de chercher un système d'équations linéaires satisfaites par les éléments (x, y) de la clé privée. Si $\boldsymbol{m}$ et $\boldsymbol{m}'$ sont deux messages, alors on a :

$$\begin{aligned} s &= x\,H(\boldsymbol{m}) + y \mod (p-1) \\ s' &= x\,H(\boldsymbol{m}') + y \mod (p-1) \end{aligned}$$

Puis, si $H(\boldsymbol{m}) - H(\boldsymbol{m}')$ est inversible modulo $p-1$, on obtient :

$$x = (s - s')(H(\boldsymbol{m}) - H(\boldsymbol{m}'))^{-1} \mod (p-1)$$

et

$$y = s - x\,H(\boldsymbol{m}) \mod (p-1)\,.$$

De ces calculs, on déduit qu'il est possible de monter une attaque sur la clé, avec des **messages connus** (KMA). En effet, quelques messages (2 avec bonne probabilité) suffisent pour obtenir $H(\boldsymbol{m}) - H(\boldsymbol{m}')$ inversible modulo $p-1$, et il n'est pas nécessaire de les choisir. On retrouve ensuite x et y avec les formules ci-dessus.

Exercice 3. $(\star)$ Signatures et fonctions de hachage.

Soit H une fonction de hachage à valeurs dans $\{0,1\}^t$, où $t \geq 1$ est un entier fixé. On rappelle qu'une *collision* sur H est un couple de messages distincts $\boldsymbol{m} \neq \boldsymbol{m}'$ tels que $H(\boldsymbol{m}) = H(\boldsymbol{m}')$.

Question 1.– Théoriquement, on peut obtenir une collision sur la fonction de hachage H par un compromis temps-mémoire, et exploiter ainsi le *paradoxe des anniversaires*. Décrire la méthode qui permet d'obtenir cette collision, et donner une approximation de sa complexité en fonction de t. Pour cela, on supposera que le coût d'évaluation de H, et le test d'appartenance d'un haché h à une liste de hachés L se font en temps constant.

On considère maintenant le schéma de signature DSA dans le groupe multiplicatif $\mathbb{F}_p^\times$, et on note g un générateur d'un sous-groupe d'ordre q de $\mathbb{F}_p^\times$, où q divise $p-1$. Pour simplifier,

on suppose également que la fonction de hachage H est utilisée **sans schéma de remplissage** additionnel. Les algorithmes de signature et de vérification de DSA sont rappelés ci-dessous. On note $\mathcal{S} = (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ l'espace des signatures.

Algorithme 5 : Signature DSA

Entrée : un message $\boldsymbol{m}$, la clé privée a
Sortie : une signature $s \in \mathcal{S}$

1 Calculer l'entier h associé à $H(\boldsymbol{m}) \in \{0,1\}^t$.
2 Choisir $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ aléatoirement.
3 Calculer $b = (g^k \mod p) \mod q$.
4 Calculer $c = (h + ab)k^{-1} \mod q$.
5 Si b ou c n'est pas inversible $\mod q$, revenir à l'étape 2.
6 Sinon, retourner $s = (b, c)$.

Algorithme 6 : Vérification DSA

Entrée : une signature $s \in \mathcal{S}$, un message $\boldsymbol{m}$, la clé publique $\alpha = g^a$
Sortie : vrai ou faux

1 Calculer l'entier h associé à $H(\boldsymbol{m}) \in \{0,1\}^t$.
2 Calculer $x = g^{hc^{-1} \bmod q}\, \alpha^{bc^{-1} \bmod q}$.
3 Faire le test $x \equiv b \mod q$ et retourner le booléen associé.

Question 2.– Expliquer comment une collision sur H peut mener à une attaque sur le schéma de signature. On précisera la nature et les moyens de l'attaque.

Question 3.– En déduire la valeur de t minimale pour **espérer** obtenir une sécurité EUF-CMA (infalsifiabilité existentielle à message choisi) de 128 bits.

Solutions de l'Exercice 3.

Solution Q1. Le paradoxe des anniversaires stipule que, si l'on tire M fois avec remise un élément dans un ensemble à N éléments, alors la probabilité d'avoir tiré des éléments deux-à-deux distincts décroît asymptotiquement en

$$e^{-M^2/2N}.$$

Autrement dit, en tirant $M \gg \sqrt{N}$ éléments aléatoirement, on peut espérer avoir deux éléments identiques avec bonne probabilité.

La preuve de ce résultat est la suivante. Soit X_i la valeur du i-ème élément tiré, et $S_i = \{X_1, \ldots, X_i\}$ la liste des i premiers éléments tirés. On note également E_i l'évènement « les éléments tirés sont deux à deux distincts ». Alors, si l'on suppose les tirages de X_i indépendants, on a :

$$\begin{aligned}\mathbb{P}(E_M) &= \mathbb{P}(X_2 \notin S_1 \text{ et } X_3 \notin S_2 \text{ et } \ldots \text{ et } X_M \notin S_{M-1}) \\ &= \mathbb{P}(X_2 \notin S_1)\mathbb{P}(X_3 \notin S_2 \mid \#S_2 = 2) \cdots \mathbb{P}(X_M \notin S_{M-1} \mid \#S_{M-1} = M-1) \\ &= (1 - 1/N)(1 - 2/N) \cdots (1 - (M-1)/N) \simeq e^{-M^2/2N}\end{aligned}$$

Étant donné ce résultat de probabilités, pour construire une collision sur H, voici une idée d'algorithme :

1. Initialiser une table $T = [\,]$
2. **Faire** :
   (a) tirer $\boldsymbol{m}$ aléatoirement et calculer $H(\boldsymbol{m})$
   (b) s'il existe $H(\boldsymbol{m}_i) \in T$ tel que $H(\boldsymbol{m}) = H(\boldsymbol{m}_i)$, alors **retourner** la paire $(H(\boldsymbol{m}), H(\boldsymbol{m}_i))$
   (c) sinon, ajouter $H(\boldsymbol{m})$ à T

D'après l'analyse asymptotique précédente, la complexité de l'algorithme est en moyenne $O(2^{t/2})$, si l'on considère que le calcul de $H(\cdot)$ et le test $h \in T$ ont un coût $O(1)$.

Solution Q2. Si un attaquant connaît deux messages $\boldsymbol{m} \neq \boldsymbol{m}'$ tels que $H(\boldsymbol{m}) = H(\boldsymbol{m}')$, alors il peut simplement :

- demander une signature s de $\boldsymbol{m}$,
- retourner la falsification $(\boldsymbol{m}', s)$.

On observe que s est bien une signature valide de $\boldsymbol{m}'$.

C'est une attaque existentielle (l'attaquant ne choisit pas le message attaqué, car il ne maîtrise pas la collision de $\boldsymbol{m}$ et $\boldsymbol{m}'$) à message choisi (il demande la signature d'un message spécifique).

Solution Q3. Il faut rendre la recherche de collision impossible, ce qui nécessite :

$$2^{t/2} \geq 2^{128} \implies t \geq 256\,.$$
