Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Feuille de TD 6

18/03/2022

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

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/clef-publique.html`

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

---

Exercice 1. $(\star)$ Signatures et fonctions de hachage.

Soit H une fonction de hachage à valeurs dans $\{0,1\}^t$. 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.– 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 1 : 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 2 : 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.

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 3 : 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 4 : 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 5 : 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.

Exercice 3. $(\star\star\star)$ Compression de clefs ECDSA.

On considère une paire de clefs publique/privée pour le schéma de signature ECDSA, instantié dans une courbe elliptique E sur $\mathbb{F}_p$. L'équation de la courbe est donnée comme un paramètre publique, ainsi qu'un générateur G du plus grand sous-groupe cyclique $\mathbb{G}$ de $E(\mathbb{F}_p)$. On note enfin n l'ordre de $\mathbb{G}$. On se place dans un cas favorable où $n \sim p$.

Question 1.– Rappeler une description de la clef publique et de la clef privée du système. Quelle est la taille mimimale de p pour obtenir une sécurité de 128 bits ? En déduire la taille minimale de la clef publique, lorsqu'on n'utilise aucune stratégie d'encodage particulière.

Question 2.– Donner une majoration la plus fine possible du nombre de bits nécessaires pour encoder un point fini de $E(\mathbb{F}_p)$.

Question 3.– Soit $P = (x_P, y_P)$ un point fini de $E(\mathbb{F}_p)$. Comment peut-on déduire la valeur de y_P à partir de celle de x_P, au signe près ? En déduire une description unique de P qui utilise au plus $\lceil \log_2 p \rceil + 1$ bits.

Exercice 4. 💻 Découverte d'un certificat.

Cet exercice « pratique » a pour but de vous faire découvrir les informations incluses dans un certificat.

Dans un navigateur de votre choix, entrer l'URL de l'université

`https://www.univ-paris8.fr/`

Chercher ensuite l'emplacement des certificats dans la barre d'adresse. Par exemple, sous `Mozilla Firefox`, on l'obtient en

1. cliquant d'abord sur le cadenas à gauche de l'adresse,
2. puis sur le chevron à droite de « connexion sécurisée »,
3. puis « plus d'information ».

Un bouton « Afficher le certificat » est alors disponible.

Question 1.– Combien de certificats trouve-t-on ? Pour chacun des certificats, préciser les émetteurs et sujets correspondants. Comment expliquer la présence de plusieurs certificats ? Que dire de celui qui a comme sujet *DigiCert Inc* ?

Question 2.– Pour chacun de ces certificats, quel algorithme de signature a été utilisé ?
Trouver également :

— la clef publique utilisée pour la signature
— la signature obtenue,
— la durée de validité,
— le contexte d'utilisation du certificat.