Université Paris 8 — Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Devoir semaine 5

devoir du 25/02/2022
à rendre jusqu'au 11/03/2022

Exercice 1. Implantation de RSA-FDH.

Dans cet exercice, on considère le schéma de signature RSA-FDH (*full-domain-hash*), implanté avec la fonction de hachage SHA-3, de sortie 224 bits.

On note $\boldsymbol{m}$ le message à signer, qui est vu comme une chaîne de caractères. Afin d'obtenir des hachés à valeur dans $\mathbb{Z}/n\mathbb{Z}$ (où n est le module public), on procède ainsi :

1. On note t le nombre de bits de p et q, les facteurs de n.
2. On calcule d'abord une séquence de hachés $\boldsymbol{h}$ suivant le schéma de remplissage :

$$\boldsymbol{h} = \texttt{SHA3\_224}(\boldsymbol{m} \,\|\, 0) \,\|\, \texttt{SHA3\_224}(\boldsymbol{m} \,\|\, 1) \,\|\, \cdots\cdots \,\|\, \texttt{SHA3\_224}(\boldsymbol{m} \,\|\, r)$$

   où « $\boldsymbol{m} \,\|\, i$ » est la chaîne de caractère associée à la concaténation de $\boldsymbol{m}$ et de l'entier i, et où r est tel que $\boldsymbol{h}$ est de longueur $\ell > 2t$ bits. Autrement dit, on prend $r = \lfloor 2t/224 \rfloor$.
3. Enfin, on convertit $\boldsymbol{h} \in \{0,1\}^\ell$ en un entier (les bits de poids fort étant devant), et on le réduit modulo n.

Aide (en python).

— On pourra utiliser la bibliothèque `pycryptodome` pour accéder à la fonction de hachage `SHA3_224`, voir la documentation ici : `[lien]`. Cette fonction prend en entrée une séquence d'octets.

— On peut également convertir une chaine de caractères $\boldsymbol{m}$ (encodée en `utf-8`) en une chaîne d'octets par la fonction `bytes(m, 'utf-8')`. Ainsi, pour transformer une chaîne `m` en haché `h` sous forme hexadécimale, grâce à la fonction de hachage `SHA3_224`, on aura le code python suivant :

```
from Cryptodome.Hash import SHA3_224
h = SHA3_224.new(bytes(m, "utf-8")).hexdigest()
```

— Il est également possible d'utiliser la bibliothèque `hashlib`.

— Pour lire le contenu d'un fichier, il existe les fonction `open()` et `read()`. Exemple d'utilisation :

```
# pour ouvrir l'objet fichier
f = open("nom_du_fichier.txt", 'r')
# pour lire le contenu  et le stocker dans une chaine de caracteres
s = f.read()
# pour fermer le fichier (important)
f.close()
```

— Pour transformer un nombre `a` sous forme hexadécimale en entier, on peut utiliser `int(a, 16)`.

Question 1.– Implanter le schéma de remplissage pour la fonction de hachage `SHA3_224`. Vérifier que pour le message $\boldsymbol{m}$ = « test » (ne pas considérer les guillemets) et la valeur $t = 128$, on obtient le haché

$$\boldsymbol{h} = 3489e8bf24b660896180884567a6c1bb971fe104137e713de8a7bc98$$
$$d6e981ecb4de6889ecd6d33a5022bffee9af2aa272c2060fb86f098a$$

en écriture hexadécimale [1].

Question 2.– Implanter les algorithmes de signature et de vérification du schéma de signature RSA-FDH, en accord avec le schéma de remplissage présenté ci-dessus. On appellera ces fonctions `sign` et `verif`.

Question 3.– Exemple-jouet [2]. On prend $t = 16$ pour simplifier.

1. Vérifier que pour $n = 3089616301$ et $d = 1118240705$, la signature de $\boldsymbol{m}$ = « exemple » est $s = 2870643504$.
2. Vérifier que pour $n = 2509359689$ et $e = 65537$, la valeur $s = 520203729$ est une signature correcte de $\boldsymbol{m}$ = « jouet ».

On fixe maintenant $t = 1024$ afin d'avoir au moins 80 bits de sécurité. On donne également un en ensemble de fichiers accessibles à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/docs/CP/devoirs/D5/devoir5-aux.zip`

Décompresser l'archive `.zip`. Vous y trouverez :

1. un fichier `lebateauivre.txt`,
2. un fichier `pk.txt` dans lequel se trouve le module public n,
3. trois fichiers `s1.txt`, `s2.txt`, `s3.txt` dans lequels se trouvent trois signatures potentielles du texte dans `lebateauivre.txt`.

On appelle $\boldsymbol{m}$ la chaîne de caractères correspondant au fichier `lebateauivre.txt`. Vérifiez que la chaîne de caractère commence par :

```
Le Bateau Ivre.

Comme je descendais des Fleuves impassibles,
Je ne me sentis plus guidé par les haleurs:
Des Peaux-Rouges criards les avaient pris pour cibles,
Les ayant cloués nus aux poteaux de couleurs.
```

Faites notamment attention à l'encodage des accents, et à la présence de retours à la ligne par exemple.

1. on pourra s'aider par exemple de `https://emn178.github.io/online-tools/sha3_224.html` pour vérifier la valeur des hachés.
2. c'est-à-dire, avec des valeurs « petites »

Question 4.– Vérifier que le haché de m, selon le schéma de remplissage décrit ci-dessus, a pour écriture hexadécimale :

```
d79227398fb4bf19d182410afcb19bc72f8c0a8390b7f4fe071e52caf15d73cfb347ad3d1456e60
667a75ef47ab32dc6f41bf8f5542e6ef55d16abc0eda0992feff93e51fb5756341fa28144e6d2ad
72b113d97b6dddb90b12f701bf835d633d78d6dd29ba78f355772316d53e6f77c2063a61f95187e
e5cb3a9ef760f2da35a145522f1d02de2f9eed9f67f4fcc7a72a3a615b7dd5c60dd4f50d3bbbb4a
61310f51d1d21b08d2a657cd9803f28dd3d6dc280f6ebc98c9833d58b4d6a16fe5e7d0ca55331b6
92c8163dc0c9c9b2284ca014c30590596948e22240e307e695574ef9fee6de8df46065719c2f403
bb3ba780e428d94369016d6029415e94474cbf50fbbeef652911fe01995f593d4560a7d8e580e85
957867b
```

Question 5.– Alice engendre une clef publique $\texttt{pk} = (n, e)$ où $e = 65537$ et n est l'entier écrit dans le fichier `pk.txt`.

Parmi les entiers donnés dans les fichiers `s1.txt`, `s2.txt` et `s3.txt`, lequel correspond à une signature de m avec la clé publique d'Alice ?