Authentification d'un document

Pour signer un gros document on calcule d'abord une empreinte de ce document (avec une fonction de hachage). La commande `dgst` permet de le faire.

```
openssl dgst <hachage> −out <empreinte> <fichier_entree>
```

où `hachage` est une fonction de hachage. Avec `openssl`, plusieurs fonctions de hachage sont proposées dont :

— MD5 (option -md5), qui calcule des empreintes de 128 bits,
— SHA1 (option -sha1), qui calcule des empreintes de 160 bits,
— SHA256 (option -sha256), qui calcule des empreintes de 256 bits,
— RIPEMD160 (option -ripemd160), qui calcule des empreintes de 160 bits.

Signer un document revient à signer son empreinte avec sa clé privée. Pour cela, on utilise l'option `-sign` de la commande `rsautl`

```
openssl rsautl -sign -in <empreinte> -inkey <cle> -out <signature>
```

On envoie cette signature ainsi que le document qui a servie à produire l'empreinte.
Le destinataire recoit la signature et le document. Pour vérifier l'authentification, il doit :

1. Utiliser la clef publique de l'expéditeur pour avoir l'empreinte.
   ```
   openssl rsautl -verify -in <signature> -pubin -inkey <cle> -out <empreinte1>
   ```

2. Vérifier que le document recu fournit la même empreinte :
   ```
   openssl dgst <hachage> -out <empreinte2> <fichier_entree>

   diff <empreinte2> <empreinte1>
   ```

Exercice n° 1

Récupérez l'archive exo8.zip qui contient deux fichiers accompagnés d'une signature. L'expéditeur a signé les fichiers txt grace à sa clef privée.
Vous avez à disposition :

— un fichier : `quinquin.txt` ayant pour signature : `signature1`
— un fichier : `mirabeau.txt` ayant pour signature : `signature2`
— la clef publique l'expéditeur des fichiers : uneClePublique.pem.

De ces deux fichiers, lequel n'est pas authentifiable ?

Remarque : Pour savoir quel type de hachage choisir (-md5, -sha256, . . .) , regarder la taille de l'empreinte.

BILAN DU CHAPITRE

1. Quel est l'inconvénient majeur du chiffrement symétrique ?
2. Quel est l'inconvénient majeur du chiffrement asymétrique ?
3. Quel est le plus grand avantage du chiffrement symétrique ?
4. Quel est le plus grand avantage du chiffrement asymétrique ?
5. Expliquer comment les deux chiffrements cohabitent afin de sécuriser au mieux les communications.
6. Pourquoi tout document envoyé doit être signé par l'expéditeur ?
7. Comment signe t-on un document ?
8. Qu'est ce qui garanti la fiabilité d'une signature numérique ?
9. Citer un type de chiffrement asymétrique ainsi que l'année de sa création.
10. Sur quel principe de base repose le chiffrement symétrique ?
11. Quelle est la différence entre l'action de déchiffrer et l'action de décrypter ?
12. Connaissez-vous une méthode permettant de décrypter un message codé avec chiffrement symétrique ?
13. Quel autre nom donne t-on au chiffrement asymétrique ou chiffrement de type RSA ?
14. D'où proviennent les lettres RSA ?