

Exercice

Cet exercice porte sur l'utilisation des chiffrements symétrique et asymétrique.

Bob souhaite envoyer un message confidentiel à Alice sans qu'un espion, Marley, ne puisse le lire ou le modifier. Pour cela, il envisage plusieurs méthodes de chiffrement et de signature numérique.

Rappel des commandes OpenSSL

Avant de commencer, voici un rappel des principales commandes OpenSSL utilisées pour le chiffrement et la signature numérique.

1. Chiffrement symétrique

Pour chiffrer le fichier `toto.txt` : (un fichier `toto.enc` est alors créé)

```
1 openssl enc -bf-cbc -in toto.txt -out toto.enc
```

Pour déchiffrer le fichier `toto.enc` : (un fichier `toto.decode` est alors créé)

```
1 openssl enc -bf-cbc -d -in toto.enc -out toto.decode
```

3. Chiffrement asymétrique

Pour chiffrer le fichier `toto.txt` avec la clé `KeyPub.pem` : (un fichier `toto.enc` est alors créé)

```
1 openssl rsautl -encrypt -in toto.txt -inkey KeyPub.pem -pubin -out toto.enc
```

Pour déchiffrer le fichier `toto.enc` avec la clé `Key.pem` (un fichier `toto.decode` est alors créé) :

```
1 openssl rsautl -decrypt -in toto.enc -inkey Key.pem -out toto.decode
```

4. Signature numérique et vérification

Pour générer une empreinte (avec une fonction de hachage) du document `toto.txt` (un fichier `empreinte.txt` est alors créé)

```
1 openssl dgst -md5 -out empreinte.txt toto.txt
```

Pour générer une signature à partir du fichier `empreinte.txt` et d'une clé `Key.pem` : (un fichier `signature.txt` est alors créé)

```
1 openssl rsautl -sign -in empreinte.txt -inkey Key.pem -out signature.txt
```

Pour retrouver l'empreinte à partir de la signature (`signature.txt`) et d'une clé publique `KeyPub.pem` : (un fichier `empreinte1.txt` est alors créé)

```
1 openssl rsautl -verify -in signature.txt -pubin -inkey KeyPub.pem -out empreinte1.txt
```

Questions

1. Bob envisage d'utiliser un chiffrement symétrique pour sécuriser son message. Il a convenu avec Alice d'une clé permettant l'utilisation de ce chiffrement.

- a. Bob rédige le `message.txt` et le chiffre avec la commande :

```
1 openssl enc -bf-cbc -in message.txt -out message.enc
```

puis il envoie le fichier `message.enc` à Alice. Quelle commande OpenSSL, Alice doit-elle écrire pour déchiffrer le message ?

```
1 openssl enc -bf-cbc -d -in message.enc -out message.decode
```

- b. Expliquer pourquoi Alice ne pourra pas déchiffrer le fichier `message.enc`.

Car elle n'a pas la clé (ou le mot de passe) choisi(e) par Bob.

- c. Citer deux avantages du chiffrement symétrique ?

Le chiffrement et le déchiffrement sont rapides et très sécurisés (si la clé est bien choisie)

- d. Quel est le plus grand inconvénient du chiffrement symétrique ?

La transmission de la clé (ou du mot de passe) doit se faire de façon sécurisée. Il faut utiliser un chiffrement asymétrique pour le faire.

2. Afin d'améliorer la sécurité de la communication avec Alice, Bob découvre le chiffrement asymétrique. Bob et Alice ont tous les deux généré une clé publique (`KeyPubAlice.pem` et `KeyPubBob.pem`) et une clé privée (`KeyPrivAlice.pem` et `KeyPrivBob.pem`)

- a. Quelle est la différence entre clé privée et clé publique ?

La clé publique du destinataire va permettre de chiffrer un message . La clé privée va permettre de déchiffrer le message codé.

- b. Citer un avantage du chiffrement asymétrique.

Va permettre de transmettre une clé pour le chiffrement symétrique.
On a besoin d'une seule clé privée pour déchiffrer les messages qui nous sont adressés.

- c. Voici la commande que Bob écrit pour chiffrer le `message.txt` qu'il souhaite transmettre à Alice :

```
1 openssl rsautl -encrypt -in message.txt -inkey KeyPubliqueBob.pem -pubin -out message.enc
```

Il envoie le fichier `message.enc` à Alice. Expliquer pourquoi Alice n'arrivera pas à déchiffrer le fichier `message.enc`

Pour chiffrer, Bob a utilisé sa clé publique au lieu d'utiliser la clé publique d'Alice.

- d. Bob a enfin réussi à chiffrer correctement : `message.txt` en `message.enc`. Expliquer comment Alice doit procéder pour déchiffrer le message. On pourra écrire la commande OpenSSL ou expliquer la démarche.

Alice va utiliser sa clé privée pour déchiffrer le message.

```
1 openssl rsautl -decrypt -in message.enc -inkey KeyPrivAlice.pem -out message.decode
```

- e. Maintenant Bob souhaite transmettre un diaporama à Alice. Malheureusement, et malgré l'exactitude de la commande OpenSSL utilisé par Bob, le chiffrement asymétrique ne fonctionne pas. Expliquer pourquoi ?

Le chiffrement asymétrique ne permet pas de chiffrer des fichier trop volumineux. (Le fichier chiffré prends environ 10 fois plus d'espace mémoire que le fichier à chiffrer)

- f. Bob a compris son erreur et voici les commandes OpenSSL qu'il a tapé pour pouvoir envoyer

son diaporama de façon sécurisé :

```
1 openssl rsautl -encrypt -in password.txt -inkey KeyPubAlice.pem -pubin -out password.enc
2 openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
```

i. Quels sont les fichiers qu'il doit transmettre à Alice ?

Il doit transmettre `message.enc` qui a été chiffré avec le chiffrement symétrique et le fichier `password.enc` chiffré avec le chiffrement asymétrique

ii. Comment Alice va t-elle faire pour déchiffrer le fichier `diaporama.enc` ? (On pourra écrire les commandes OpenSSL ou expliquer la démarche.)

Alice doit déchiffrer `password.enc` avec sa clé privée afin d'avoir la clé (ou mot de passe) pour déchiffrer le fichier `message.enc`.

```
1 openssl rsautl -decrypt -in password.enc -inkey KeyPrivAlice.pem -out password.decode
2 # prendre connaissance du contenu du fichier password.decode
3 # avant de passer à la commande suivante :
4 openssl enc -bf-cbc -d -in diaporama.enc -out diaporama.decode
```

3. Bob veut s'assurer que le diaporama qu'il envoie n'est pas altéré et qu'Alice peut vérifier son authenticité. Dans cette partie, on suppose que Alice et Bob ont échangé une clé (ou mot de passe) permettant de communiquer via un chiffrement symétrique.

a. Voici la démarche faite par Bob pour mettre en place cela :

— Il prépare son fichier `diaporama.pdf`.

— Il chiffre son fichier : `diaporama.pdf` avec un chiffrement symétrique :

```
1 openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
```

— Avec une fonction de hachage, il génère une empreinte de son diaporama :

```
1 openssl dgst -md5 -out empreinte.txt diaporama.pdf
```

— En utilisant sa clé privée, il génère une signature (`signature.txt`) à partir du fichier `empreinte.txt` :

```
1 openssl rsautl -sign -in empreinte.txt -inkey KeyPrivBob.pem -out signature.txt
```

Quels sont les fichiers que Bob va transmettre à Alice ?

`signature.txt` et `diaporama.enc`

- b. Comment Alice va t-elle faire pour déchiffrer le diaporama et s'assurer qu'il n'a pas été modifié ? (On pourra écrire les commandes OpenSSL ou expliquer la démarche à l'aide de phrases.)

Pour déchiffrer `diaporama.enc`, elle utilise la clé (ou mot de passe) du chiffrement symétrique.

```
1 openssl enc -bf-cbc -d -in diaporama.enc -out diaporama.decode
```

Pour s'assurer que le fichier n'a pas été modifié :

- i. Elle utilise la clé publique de Bob et le fichier `signature.txt` pour retrouver l'empreinte `empreinte.txt`

```
1 openssl rsautl -verify -in signature.txt -pubin -inkey KeyPubBob.pem -out empreinte.txt
```

- ii. Elle calcule l'empreinte à partir du fichier `diaporama.decode`

```
1 openssl dgst -md5 -out empreinte1.txt diaporama.encode
```

- iii. Elle vérifie que les deux empreintes sont identiques.

```
1 diff empreinte.txt empreinte1.txt
```

- c. **Attaque 1 :** Marley réussi à se procurer le fichier `signature.txt`, peut-il déchiffrer ce fichier ? Si oui, que dire de son contenu ? si non, expliquer pourquoi ?

Oui, car il se déchiffre avec la clé publique de Bob. Cette clé est publique. Son contenu est lisible mais inexploitable car une fonction de hachage a permis de "réduire" le diaporama initial.

- d. **Attaque 2 :** Marley a réussi à se procurer le fichier `diaporama.enc` et a aussi réussi à déchiffrer le fichier `signature.txt`, peut-il alors réussir à déchiffrer le fichier `diaporama.enc` ?

Pour déchiffrer `diaporama.enc` il faut connaître la clé privée d'Alice. Cette clé n'est ni présente dans `signature.txt`, ni dans `diaporama.enc`, ni dans `KeyPubAlice.pem`. Donc Marley ne peut pas déchiffrer le fichier.

e. Attaque 3 : Marley a réussi à se procurer la clé que Bob et Alice utilise pour le chiffrement symétrique ainsi que le fichier `diaporama.enc`.

i. Marley peut-il déchiffrer le fichier `diaporama.enc` ?

Oui car le diaporama a été chiffré avec un chiffrement symétrique et Marley connaît la clé.

ii. Marley décide alors de remplacer le fichier `diaporama.enc` de Bob et par un nouveau diaporama `diaporama.pdf`. Expliquer comment Alice va s'en rendre compte. (On ne demande par de commande OpenSSL)

Pour vérifier l'authenticité, Alice va comparer l'empreinte du diaporama créé par Marley avec l'empreinte provenant du fichier `signature.txt` généré avec la clé privée de Bob. Comme Marley n'a pas fait de modification que le fichiers `signature.txt`, il y aura une différence entre les deux empreintes, cela signifie qu'il y a eu une altération du fichier.

f. Attaque 4 : Marley décide non seulement de remplacer le fichier `diaporama.enc` mais aussi de remplacer le fichier `signature.txt` avec les commandes :

```
1 openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
2 openssl dgst -md5 -out empreinte.txt diaporama.pdf
3 openssl rsautl -sign -in empreinte.txt -inkey KeyPrivMarley.pem -out signature.txt
```

Expliquer comment Alice va s'en rendre compte. (On ne demande par de commande OpenSSL)

Comme précédemment, Alice va comparer l'empreinte du diaporama créé par Marley avec l'empreinte provenant du fichier `signature.txt` généré avec la clé privée de Marley. Mais comme Alice, va utiliser la clé privée de Bob (car elle discute avec Bob) pour faire la dernière action cela va rendre cette action impossible (ou généré une empreinte différente de celle obtenue avec le diaporama reçu)

g. Attaque 5 : Proposer une autre idée à Marley afin de réussir à déjouer la sécurité mise en place par Bob et Alice.

- i. Marley arrive a obtenir la clé privée de Bob.
- ii. Marley se fait passer pour Bob (Attaque de l'homme du milieu).