ISIFC-informatique pour la santé (sécurité).
oct. 2021, 2 heures.

Tous les supports sont autorisés. Les codes sont transmis par mel.

J.-F. COUCHOT

Prénom et nom des deux membres du binôme :

Vous êtes en charge du développement d'un dispositif D qui :
— construit des images médicales (de type coupes d'images) et
— capture un diagnostic énoncé à l'oral et le transforme en un diagnostic écrit.

Chacun des éléments de santé (images, diagnostics oraux et diagnostics écrits) est enregistré dans une base de données B située à distance et accessible via un réseau interne.

1 Entre D et B initialement

Entre le dispositif D et la base de données B, des données vont transiter.

1. Que doit être mis en place pour éviter que quiconque puisse lire des données médicales entre l'envoi de celles-ci par D et la réception par B (0,5 pt.) ?

2. Justifier le choix de l'utilisation d'un algorithme comme AES avec le mode CBC dans ce contexte (1 pt.)

3. Dans ce contexte que doit être partagé entre D et B initialement (0,5 pt.) ?

4. Quel type d'algorihtme va-t-on déployer pour réaliser ce partage ? Justifier (1 pt.).

5. La figure 1 contient trois codes qui pourraient servir pour atteindre cet objectif de partage.

   (a) Quel est l'objectif du code placé entre les lignes 4 et 14 du code donné à la figure (1a) ? Préciser en particulier ce que contiennent les fichiers '`mPubKey.pem`' et '`mPrivKey.pem`' et à quoi ils vont servir. Sur quel dispositif ce code devrait-il être exécuté (2 pts.) ?

   (b) Quel est l'objectif du code placé aux lignes 6 et 7 de la figure (1c) ? Sur quel dispositif ce code devrait-il être exécuté (1 pt) ?

   (c) Qu'est-ce que le fichier '`mPubKey.pem`' référencé à la ligne 9 du code donné à la figure (1c) ? D'où provient-il (1 pt.) ?

   (d) Quel est l'objectif du code placé entre les lignes 12 et 20 de la figure (1c) ? Détaillez. Vous préciserez en particulier le contenu des fichiers '`k_e.txt`' et '`iv_e.txt`' (2 pts).

   (e) Quel est l'objectif du code placé entre les lignes 9 et 15 de la figure (1b) ? Sur quel dispositif ce code devrait-il être exécuté (2 pts.) ?

   (f) Faire un schéma résumant ces étapes.

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

rsa_obj = RSA.generate(2048)
rsa_pub = rsa_obj.publickey()

f = open('mPubKey.pem','w')
st = rsa_pub.exportKey('PEM')
f.write(st.decode('utf-8'))
f.close()

f = open('mPrivKey.pem','w')
st = rsa_obj.exportKey('PEM')
f.write(st.decode('utf-8'))
f.close()
```

(a) Code 1

```python
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

mpk= open('mPrivKey.pem').read()
privKey = RSA.importKey(mpk)
decryptor = PKCS1_OAEP.new(privKey)


fc = open("k_e.txt","rb")
k_ciphertext = fc.read()
kp = decryptor.decrypt(k_ciphertext)

fc = open("iv_e.txt","rb")
iv_ciphertext = fc.read()
ivp = decryptor.decrypt(iv_ciphertext)
```

(b) Code 2

```python
from Crypto import Random
from Crypto.Cipher import AES
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

k  = Random.new().read(AES.block_size)
iv = Random.new().read(AES.block_size)

pubKey = RSA.importKey(open('mPubKey.pem').read())
encryptor = PKCS1_OAEP.new(pubKey)

ciphertext = encryptor.encrypt(k)
fc = open("k_e.txt","wb")
fc.write(ciphertext)
fc.close()

ciphertext = encryptor.encrypt(iv)
fc = open("iv_e.txt","wb")
fc.write(ciphertext)
fc.close()
```

(c) Code 3

FIGURE 1 – Partage d'informations à l'initialisation entre D et B

2 Echange sécurisé de données entre D et B par AES-CBC

Dans la partie précédente a été justifié le fait qu'AES dans le mode CBC va être utilisé pour échanger des données entre le dispositif D et la base B. On considère ici que sur les deux dispositifs D et B, le vecteur d'initialisation est *iv*, la clef est k et tous deux sont codés sur 128 bits.

On considère les deux codes donnés à la figure 2.

```python
from Crypto.Cipher import AES

f_in = open("diag.txt","r")
msg = f_in.read().encode('utf-8')
aes_cbc_e = AES.new(k, AES.MODE_CBC,iv)
ciphertext_aes_cbc = aes_cbc_e.encrypt(msg)

f_out = open("diag_c.txt","wb")
f_out.write(ciphertext_aes_cbc)
```

(a) Code 4

```python
from Crypto.Cipher import AES

fp_in = open("diag_c.txt","rb")
ciphertext_aes_cbc = fp_in.read()

aes_cbc_d = AES.new(k, AES.MODE_CBC, iv)
res=aes_cbc_d.decrypt(ciphertext_aes_cbc)
print(res.decode('utf-8'))
```

(b) Code 5

FIGURE 2 – Chiffrement/déchiffrement par AES d'un diagnostic textuel.

1. Quel est l'objectif du code présenté à la figure (2a) ? Expliquez le code. Quel sera le contenu du fichier '`diag_c.txt`' à la fin de ce programme ? Sur quel dispositif ce code devrait-il être exécuté (2 pts.) ?

2. Quel est l'objectif du code présenté à la figure (2b) ? Expliquez le code. Sur quel dispositif ce code devrait-il être exécuté (2 pts.) ?

3. Qu'est-ce qui changerait dans les codes précédents si l'on voulait non plus chiffrer/déchiffrer des diagnostics textuels, mais des images (radiographie, par exemple). Dire précisément quelles lignes seraient modifiées dans quels fichiers et comment (2 pts.) ?

3 Garantir l'intégrité

Pour garantir qu'aucun bit n'est modifié entre l'envoi par le dispositif D et la réception par B, une démarche est mise en place.

1. Quelle méthode devrait être mise en place ici ? Quel outil va-t-on utiliser précisément ? Avec quels paramètres (2 pts.) ?

2. Préciser quels codes vont être modifiés exactement et définir les modifications (2 pts.).