GLO - 3100 : Cryptographie et Sécurité informatique
Session A-2020

TP3 - ex1

Par :
Guillaume Doucet 111 123 716

Date de remise : 12 décembre 2020

Faculté des sciences et de génie

Exercice 1 :

1.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl genrsa -des3 -passout pass:foobar -out alice-privatekey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
......+++++
e is 65537 (0x010001)
```

2.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl rsa -in alice-privatekey.pem -passin pass:foobar -pubout -out alice-publickey.pem
writing RSA key
```

3.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl genrsa -des3 -passout pass:foobar2 -out bob-privatekey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.....+++++
e is 65537 (0x010001)

┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl rsa -in bob-privatekey.pem -passin pass:foobar2 -pubout -out bob-publickey.pem
writing RSA key
```

4.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  echo "Doucet Guillaume" >> message.txt

┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  ls
alice-privatekey.pem  alice-publickey.pem  bob-privatekey.pem  bob-publickey.pem  message.txt

┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  cat message.txt
Doucet Guillaume
```

5.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl dgst -sha1 -sign alice-privatekey.pem -passin pass:foobar -out alice_signed.sha1 message.txt

┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl enc -base64 -in alice_signed.sha1 -out alice_signed.sha1.base64
```

6.

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl enc -base64 -d -in alice_signed.sha1.base64 -out alice_signed.sha1

┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl dgst -sha1 -verify alice-publickey.pem -signature alice_signed.sha1 message.txt
Verified OK
```

7.

a)

```
┌─[kali] as root in ~/Desktop/GLO-3100/tp3
└──➤  openssl rand -base64 -out key.bin 128
```

b)

```
┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  openssl enc -aes-128-cbc -base64 -pass file:key.bin -in message.txt -out protected-message.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  cat protected-message.txt
U2FsdGVkX1+2+fL2n90ZXIcYauY98C/VfYLgSDxlXA4Yhxh1LYQw1upyrCpMr/QJ
```

c)

```
┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  openssl rsautl -encrypt -inkey bob-publickey.pem -pubin -in key.bin -out protected-key.bin
```

8.

```
┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  openssl rsautl -decrypt -passin pass:foobar2 -inkey bob-privatekey.pem -in protected-key.bin -out key-bob.bin

┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  openssl enc -d -base64 -aes-128-cbc -pass file:key-bob.bin -in protected-message.txt -out result.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──[kali] as root in ~/Desktop/GLO-3100/tp3
└─➤  cat result.txt
Doucet Guillaume
```