Mathys Domergue

RT2 App

TP

1.Chiffrement

Générateur aléatoire

a) Un générateur alétoire est un programme qui créer un nombre pseudo-aléatoire basé sur une seed, graine en français.

b)

```
lucky@lucky:~$ openssl rand -hex 2
bfe3
lucky@lucky:~$ openssl rand -hex 32
2b12a28bea481def5f5156d597fe3a06a62ea708750682d8f61afb51308d7daa
```

Pratique

d)

```
lucky@lucky:~$ openssl aes-256-cbc -nosalt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hello
◆!_◆{@◆lucky@lucky:~$
```

```
lucky@lucky:~$ openssl aes-128-cbc -nosalt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hello
◆◆嫔◆
◆i◆_◆&Blucky@lucky:~$
```

e)

```
lucky@lucky:~$ openssl aes-128-cbc -nosalt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hello
f◆◆3◆-◆V◆0◆◆-c◆◆lucky@lucky:~$
```

on peut remarquer que le mot hello change bien selon le mot de passe.