Documentation de la librairie PyCrypto

Laurent PARMENTIER
Quentin DERORY
Jean-Baptiste MAURANYAPIN

Encadrant : Patrick LACHARME

04/10/2014

Contents

Chapter 1

Fonction de hachage

1.1 MD5

L'algorithme MD5, est une fonction de Hash, qui était très utilisé dans le domaine web [1].

```
#!/usr/bin/python
from Crypto.Hash import MD5

hash = MD5.new()
hash.update("hello world")
print hash.hexdigest()
```

1.2 SHA-256

```
#!/usr/bin/python
from Crypto.Hash import SHA256

hash = SHA256.new()
hash.update("hello world")
print hash.hexdigest() # print hash sha256 of "hello world"
```

[1] https://github.com/

Chapter 2

Chiffrement a cle prive

2.1 3DES

```
#!/usr/bin/python
from Crypto import Random
from Crypto.Cipher import DES3

key = b'une cle 16 octet'
iv = Random.new().read(DES3.block_size)
des3 = DES3.new(key, DES3.MODE_ECB, iv)
print des3.encrypt("hello wo") # obligatoire d'avoir une longueur de
    mot multiple de 8
#TODO mot sur dechiffrement
```

2.2 AES

```
#!/usr/bin/python
from Crypto import Random
from Crypto.Cipher import AES

key = b'une cle 16 octet'
iv = Random.new().read(AES.block_size)
aes = AES.new(key, AES.MODE_ECB, iv)
print aes.encrypt("hello world     ") # obligatoire d'avoir une
    longueur de mot multiple de 16
#TODO mot sur dechiffrement
```

2.3 ARC4

```
#!/usr/bin/python
from Crypto.Cipher import ARC4
key = b'Tres longue cle confidentielle'
arc4 = ARC4.new(key)
print arc4.encrypt("Un message     ")
```

2.4 CAST

2.5 BLOWFISH