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 h.hexdigest()
```

1.2 SHA-256

```
#!/usr/bin/python
from Crypto.Hash import SHA256
h = SHA256.new()
h.update("hello world")
print h.hexdigest() # print hash sha256 of "hello world"
```

[1] https://github.com/

Chapter 2

Chiffrement a cle prive

2.1 DES

```
#!/usr/bin/python
from Crypto.Cipher import DES3
from Crypto import Random
key = b'Sixteen byte key'
iv = Random.new().read(DES3.block_size)
des3c = DES3.new(key, DES3.MODE_ECB, iv)
msge = des3c.encrypt("hello world")
print msge
```