Chritopher LaJon Morgan
Oct 17, 2013
CS 465

Homework 7

AES

```
Locate an AES encryption library for a programming language of your
choice. Write a short program to encrypt and decrypt the following
file. Determine how to specify the mode and padding.
```

Submit the following (typeset it so that it is readable):

- **Description of the AES library you used (e.g., URL)**

  https://www.dlitz.net/software/pycrypto/

  Pycrypto is a crypto package intended for python users. It aims at providing a reliable and stable base for writing programs that require cryptography.

- **Source code snippets showing how to encrypt/decrypt using the library**

```
from Crypto.Cipher import AES

    obj = AES.new(456Key, AES.MODE_ECB)

    message = "The answer is no"

    ciphertext = obj.encrypt(message)

        ciphertext == 'o\x1aq_{P+\xd0\x07\xce\x89\xd1=M\x989'

    obj2 = AES.new(456Key, AES.MODE_ECB)

    ans = obj2.decrypt(ciphertext)

        ans == 'The answer is no'
```

My Code:

```
message = "The answer is noThe answer is noThe answer is no"
k  = 'aoqirj.xmbnajsiq'
iv = '29581948572-1948'
print "\nECB Mode:"

obj = AES.new(k, AES.MODE_ECB)
ciphertext = obj.encrypt(message)
```

```
print ":".join("{00:x}".format(ord(c)) for c in ciphertext)

obj2 = AES.new(k,AES.MODE_ECB)
ans  = obj2.decrypt(ciphertext)
print ans

print "\nCBC Mode:"
obj3 = AES.new(k, AES.MODE_CBC,iv)
ciphertext = obj3.encrypt(message)
print ":".join("{00:x}".format(ord(c)) for c in ciphertext)

obj4 = AES.new(k,AES.MODE_CBC,iv)
ans  = obj4.decrypt(ciphertext)
print ans
```

- **Hex output of ciphertext in at least two modes (e.g., ECB and CBC)**

ECB Mode:

```
ec:c:60:6b:a2:1b:1d:54:e6:3b:e4:bb:83:f6:17:62:ec:c:60:6b:a2:1b:1d:54:e6:3b:e4:bb:83:f6:17:
62:ec:c:60:6b:a2:1b:1d:54:e6:3b:e4:bb:83:f6:17:62

The answer is noThe answer is noThe answer is no
```

CBC Mode:

```
4a:8b:88:ca:56:c8:d4:df:f9:34:9c:df:b4:35:2f:cb:62:c2:8e:7b:37:1c:3d:ff:26:c6:d1:6a:aa:23:89:
b9:90:25:db:4a:1f:b8:a1:eb:98:6b:c8:94:1f:1c:a9:c5

The answer is noThe answer is noThe answer is no
```

- **Lessons learned - list of 2-5 items about your experience**

Relearned that AES operates on a 128 bit boundary. So if one's message is identical on that boundary and one use EBC mode, then one will see that same pattern in the cipher text.

Forgot that CBC mode requires a 16 byte IV. Also noticed that, as expected, the pattern in the message was not repeated in the ciphertext when CBC mode was used.

When doing something simple like this homework python is really nice. I learned about Pycrypto.