Exercitiul 1

May 8, 2018

0.0.1 Seminarul 1 (mirunarosca@gmail.com)

m1 c1

m2 c2

Encrypted(Encrypted(mi)) = ci pentru oricare i=1,2

AES Meet in the middle attack = when a plaintext is encrypted twice, with two different keys.

You must know something about the key format. In this example the sample keygen is written with all bits being 0, untill last 24 bits.

We need to create a new key generator method according to your case.

```
In [5]: from Crypto.Cipher import AES

        def solve(plaintext,ciphertext,KeyGen):
            encrypted = {}
            for key in KeyGen():
                AEScipher = newAES(key)
                encrypted[AEScipher.encrypt(plaintext)] = key
            for key in KeyGen():
                AEScipher = newAES(key)
                decrypted = AEScipher.decrypt(ciphertext)
                if(decrypted in encrypted):
                    # We got a match between encrypted and decrypted texts
                    Key1 = encrypted[decrypted]
                    Key2 = key
                    return (Key1,Key2)

        def newAES(key):
            return AES.new(key, mode=AES.MODE_ECB)

        def sample_KeyGen():
            # Here we define the key - 29 bytes of 0, and 3 bytes that are
            # generating with 0 or 1 in for loops in order to find the key
```

```
    baseString = bytes([0])*29
    for a in range(256):
        StringA = baseString + bytes([a])
        for b in range(256):
            StringB = StringA + bytes([b])
            for c in range(256):
                yield StringB + bytes([c])

def testAESMITM():
    import base64
    message1    =  base64.b64decode("QUVTLTI1NiBFQ0IgbW9kZSB0d2ljZSwgdHdvIGtleXM=")
    encrypted   =  base64.b64decode("THbpB4bE82Rq35khemTQ10ntxZ8sf7s2WK8ErwcdDEc=")
    print("Here are the results: ")
    print("Message 1: ", message1)
    (Key1,Key2) =  solve(message1,encrypted,sample_KeyGen)
    AES1 = newAES(Key1)
    AES2 = newAES(Key2)
    message2    =  base64.b64decode("RWFjaCBrZXkgemVybyB1bnRpbCBsYXN0IDI0IGJpdHM=")
    encrypted   =  base64.b64decode("01YZbSrta2N+1p0eQppmPETzoT/Yqb816yGlyceuE0E=")
    print("Message 2: ", message2)
    assert AES1.encrypt(message2) == AES2.decrypt(encrypted)
    print("Test passed")
    ciphertext  =  base64.b64decode("s5hd0ThTkv1U44r9aRyUhaX5qJe561MZ16071nlvM9U=")
    print("Decrypted cipher text with AES 1 and AES 2:")
    print(AES1.decrypt(AES2.decrypt(ciphertext)))

testAESMITM()
```

```
Here are the results:
Message 1:  b'AES-256 ECB mode twice, two keys'
Message 2:  b'Each key zero until last 24 bits'
Test passed
Decrypted cipher text with AES 1 and AES 2:
b"This time I didn't include sol'n"
```