Criptografia de clau secreta

Entrega

1. Desxifreu el primer fitxer que heu rebut.
2. Desxifreu el segon fitxer que heu rebut i que ha sigut xifrat amb el següent codi:

```
KS=random(16)
kiv=random(1)
for i in range(0,16) {IV[i]=KS[i]^kiv}
aes_encryptor = AES.new(KS, AES.MODE_CBC,IV)
cryptogram = aes_encryptor.encrypt(Message)
result = IV || cryptogram
open("file.enc",'wb').write(result)
```

Referències

- Federal Information Processing Standards Publication (FIPS) 197: Advanced Encryption Standard (AES)
- NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation
- Padding PKCS7: section 6.3 RFC 5652

Per llegir

- Bruce Schneier *NSA and Bush's Illegal Eavesdropping.*
- Schmid, Gerhard (11 July 2001). *On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098(INI))*. European Parliament: Temporary Committee on the ECHELON Interception System.