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)
text=PKCS7Encoder.encode(Message)
cryptogram = aes_encryptor.encrypt(text)
result = IV || cryptogram
open("file.enc",'wb').write(result)
```

   - `a^b` significa a$\oplus$b i a||b concatenació d'a i b.
   - `KS`: 16 bytes aleatoris.
   - `kiv`: 1 byte aleatori.

Referències

- Federal Information Processing Standards Publication (FIPS) 197: Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
- Padding PKCS7: section 6.3 RFC 5652. http://tools.ietf.org/html/rfc5652#section-6.3

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.