**LAB 7**

**Exercise:**

**1. What are ECB and CBC and their purpose? How do they differ?**

ECB (Electronic Codebook) is essentially the first generation of the AES. It is the most basic form of block cipher encryption. CBC (Cipher Blocker Chaining) is an advanced form of block cipher encryption. With CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point.

ECB mode's issues arise from the fact that each block of the plaintext is encrypted completely independently. CBC mode eliminates this problem by carrying information from the encryption or decryption of one block to the next.

**2. Why are the following keys considered to be weak keys of DES. Think about applying these keys to cryptool preferably trying to encrypt text with these keys twice.**

**K1= 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1**

**K2= F E F E F E F E F E F E F E F E**

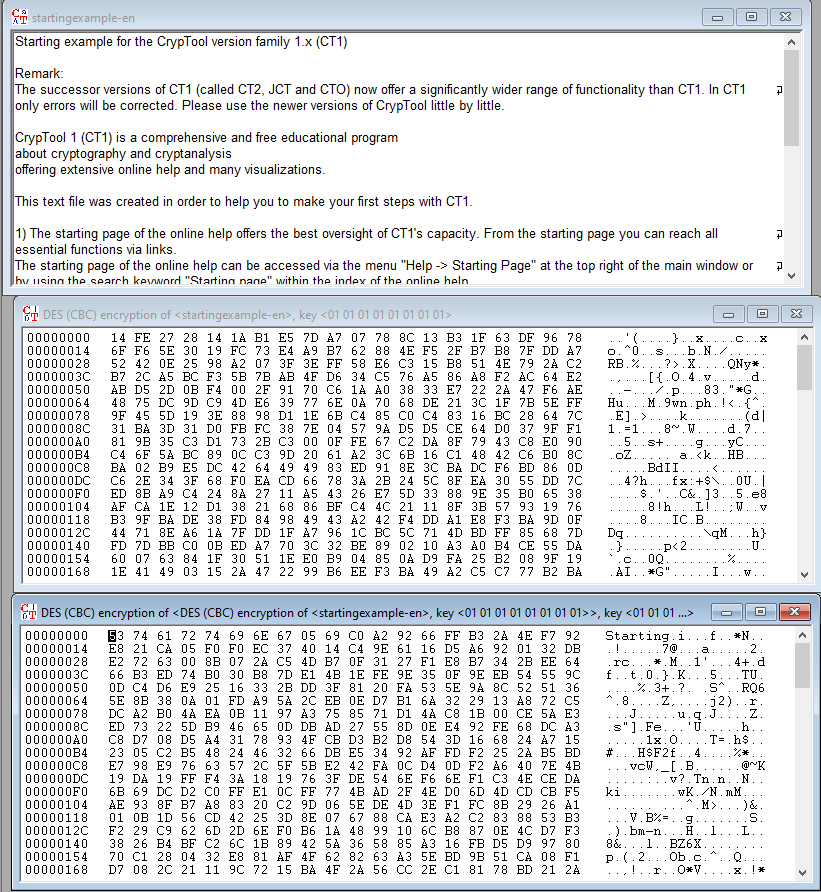
**K3= 1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E**

**K4= E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1**

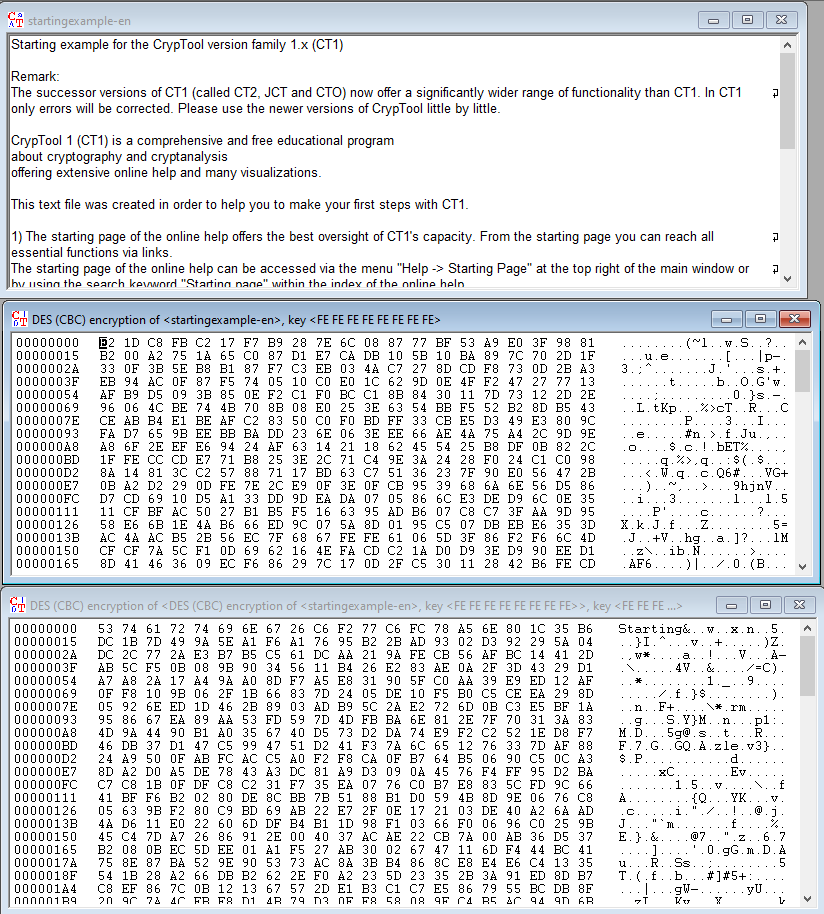
This is weak keys because one reason is that after applying this twice we get some plaintext in the ciphertext and the other reason is that applying same key twice with DES gives the plaintext.

For

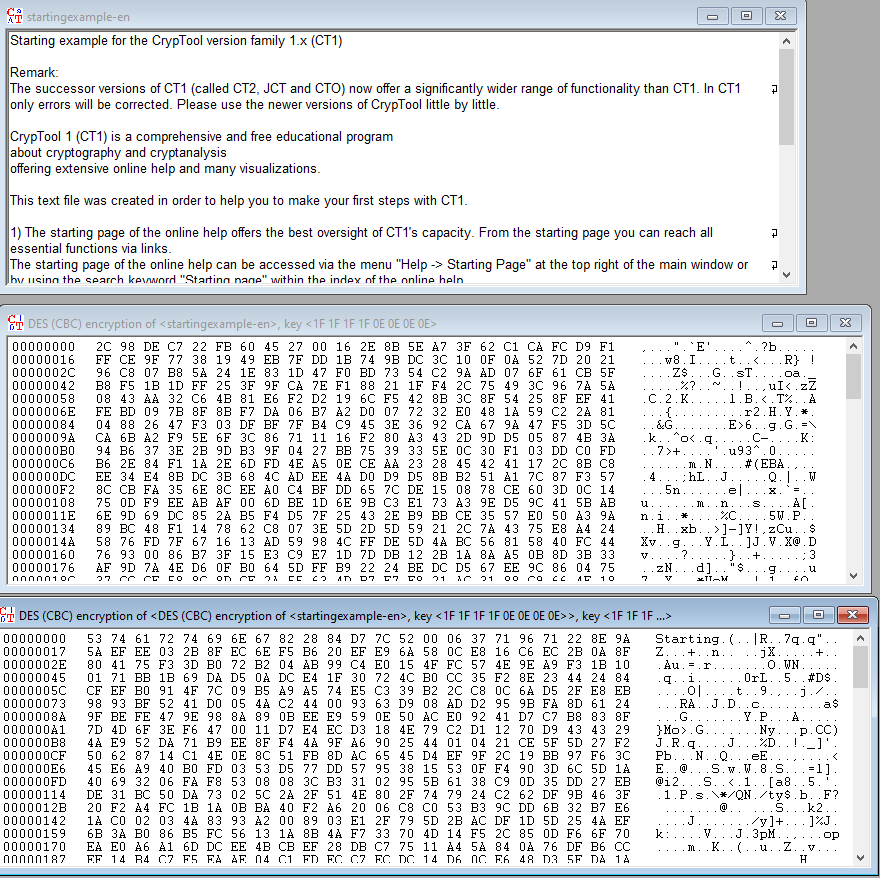
K1= 01 01 01 01 01 01 01 01



K2 = FE FE FE FE FE FE FE FE



K3 = 1F 1F 1F 1F 0E 0E 0E 0E



K4 = E0 E0 E0 E0 F1 F1 F1 F1

