**LAB 8**

**Exercise**

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

ECB (Electronic Codebook) and CBC (Cipher Block Chaining) are two block cipher modes of operation used in cryptography to securely encrypt data. Their main purpose is to transform plaintext data into cipher text, making it unreadable without the decryption key.

1. **Electronic Codebook (ECB)**

**How it Works:** In ECB mode, the data is divided into fixed-size blocks, and each block is encrypted independently using the same key.

**Purpose:** ECB aims to encrypt each block of data separately, which makes it straightforward and fast.

**Drawbacks:** If the same plaintext block appears multiple times, it will produce the same cipher text block. This means patterns in the data may remain visible, which can compromise security.

1. **Cipher Block Chaining (CBC)**

How it Works: In CBC mode, each plaintext block is XORed (combined) with the previous cipher text block before encryption. An initialization vector (IV) is used for the first block to start the process.

**Purpose:** CBC aims to add randomness to the encryption process, making each cipher text block depend on the previous one.

**Benefits:** Even if the same plaintext block appears multiple times, CBC ensures each cipher text block is unique by using the previous block’s output.

**Differences**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Electronic Codebook (ECB)** | **Cipher Block Chaining (CBC)** |
| Encryption Process | Encrypts each block independently | Each block is XORed with the previous ciphertext block before encryption |
| Pattern Exposure | Patterns in plaintext may appear in ciphertext | Hides patterns by chaining blocks, making each ciphertext block unique |
| Initialization Vector (IV) | Not required | Requires an IV for the first block |
| Security Level | Less secure due to visible patterns | More secure, as it hides patterns in repetitive data |
| Use Cases | Suitable for small, non-repetitive data | Preferred for large data or data with repeated patterns |
| Error Propagation | Errors affect only the specific block | Errors in one block affect subsequent blocks until corrected |

**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.**

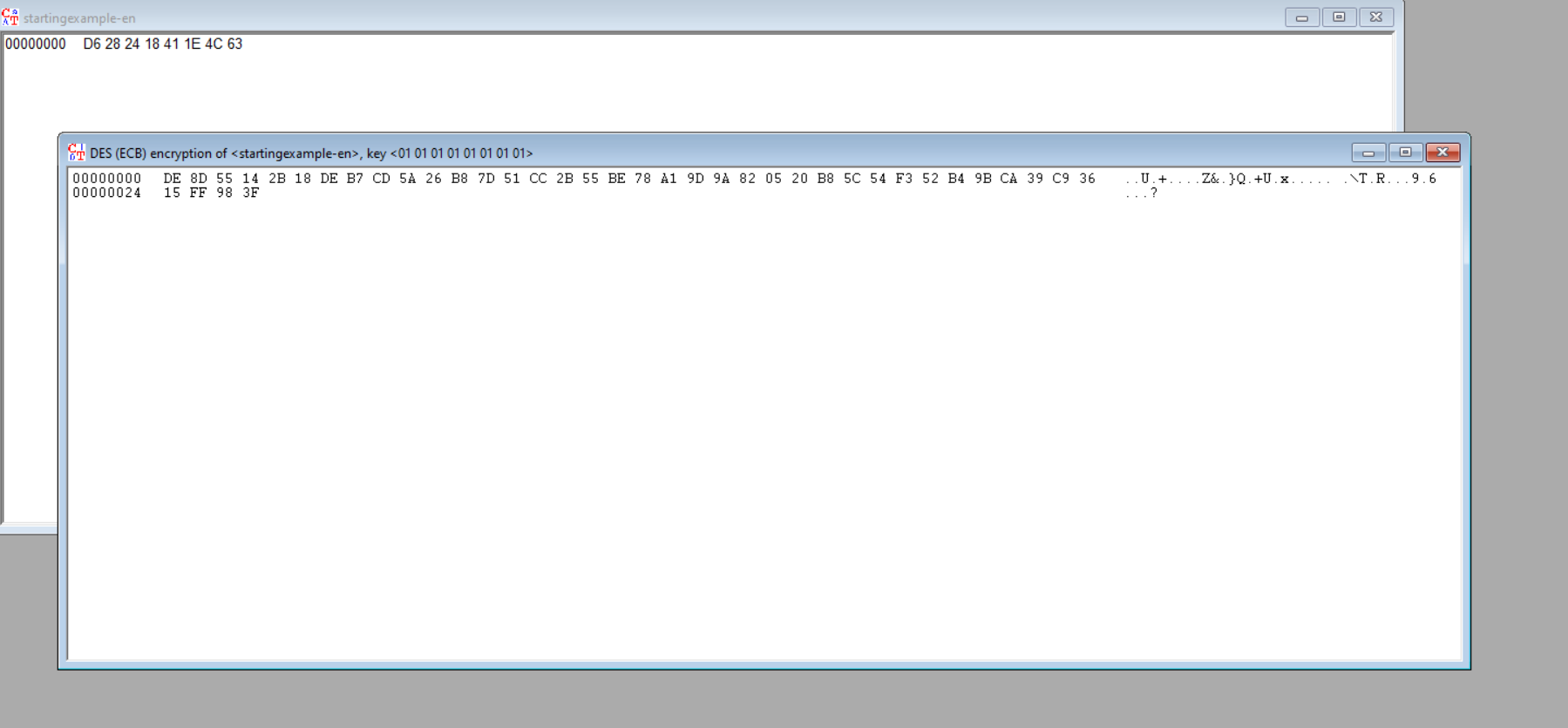
**K1= 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1**

**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**

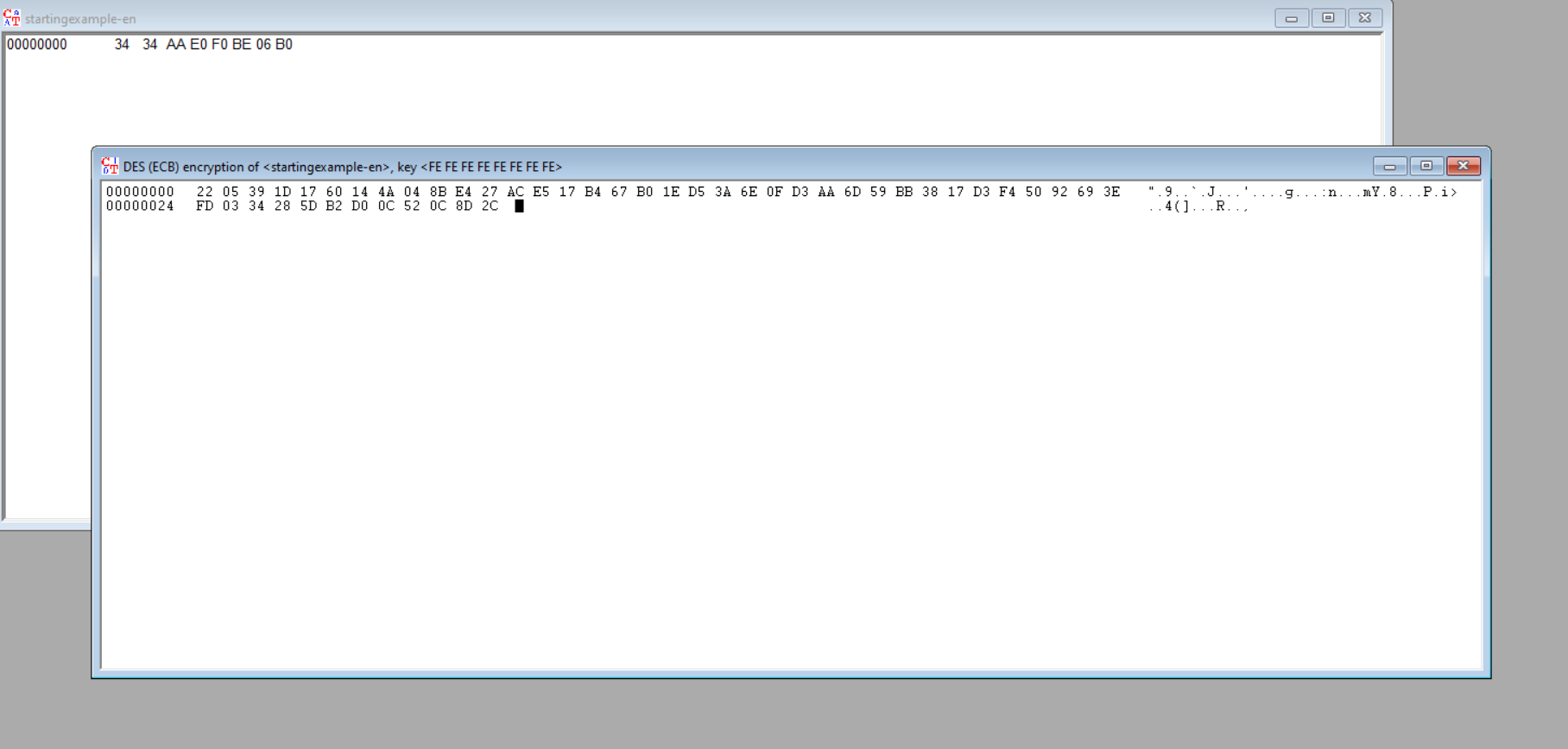
**K4= E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1**

**K1**

****

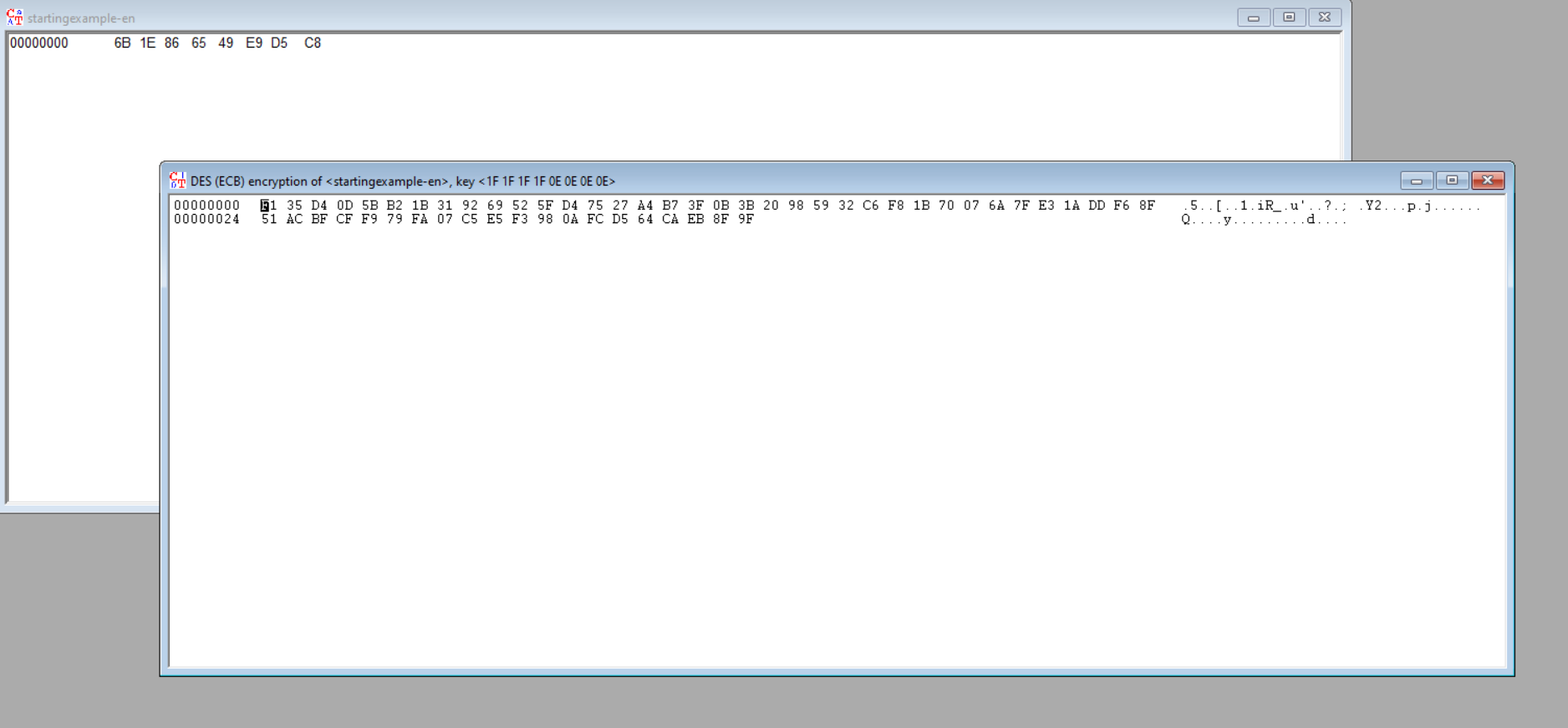
This output is not weak because its shows the key is not same after double encrypting the cipher text

**K2**



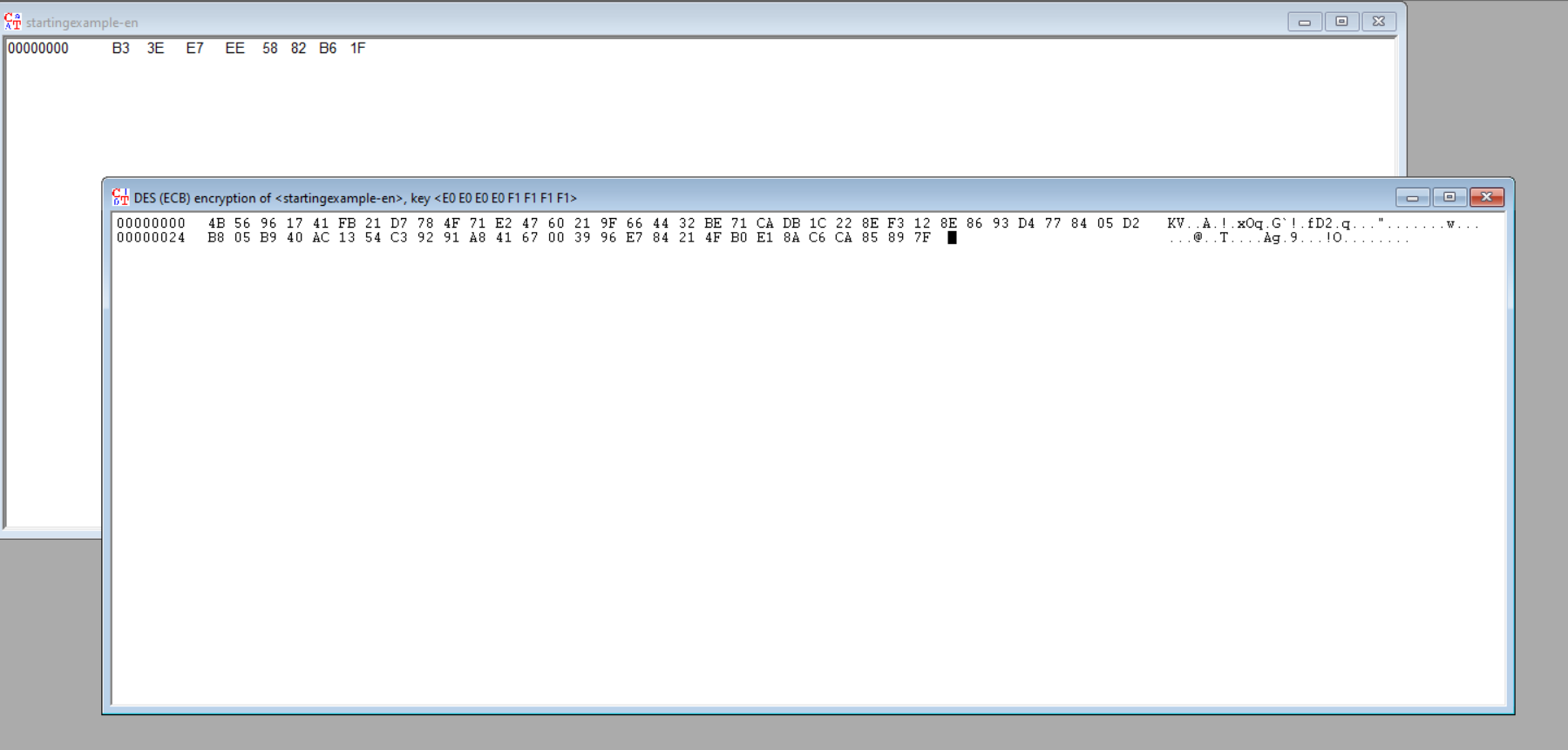
This output is not weak because its shows the key is not same after double encrypting the cipher text

**K3**



This output is not weak because its shows the key is not same after double encrypting the cipher text

**K4**

****

This output is not weak because its shows the key is not same after double encrypting the cipher text