# Exercise

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

Electronic Codebook (ECB) and Cipher Block Chaining (CBC) are two fundamental modes of operation in block cipher cryptography, differing significantly in their approach to encrypting data. In ECB, each block of plaintext is treated independently, and the same encryption key is applied to each block. While this mode allows for straightforward implementation and parallel processing, it is susceptible to revealing patterns in the data, particularly when identical or repetitive blocks are present. In contrast, CBC introduces inter-block dependencies by XORing each plaintext block with the ciphertext of the previous block before encryption. This introduces a feedback mechanism, enhancing resistance to certain vulnerabilities present in ECB, such as pattern-based attacks. However, CBC is less amenable to parallelization due to the sequential nature of block dependencies.

1. **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**

1. **K1: 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1**

Applying this key twice to DES encryption using cryptool would result in the original plaintext. This is because the key effectively has a pattern that leads to the same transformation when applied twice.

1. **K2: F E F E F E F E F E F E F E F E**

Similar to K1, this key is weak, and applying it twice would result in the original plaintext. The repetitive pattern in the key causes the encryption process to cancel itself out.

1. **K3: 1 F 1 F 1 F 1 F 0 E 0 E 0 E 0 E**

This key is also weak, and applying it twice leads to the original plaintext. The alternating pattern in the key contributes to its weakness.

1. **K4: E 0 E 0 E 0 E 0 F 1 F 1 F 1 F 1**

Like the previous keys, K4 is weak, and applying it twice results in the original plaintext. The alternating pattern in this key also causes the encryption process to cancel itself out.