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

Cryptography methods such as Electronic Code Book (ECB) and Cipher Block Chaining (CBC) are widely used.

ECB is a simple method of encrypting plaintext by dividing it into fixed-size blocks and encrypting each block independently using the same secret key. In other words, if the same plaintext block appears more than once in the message, it will be encrypted into the same ciphertext block (aka will look the same). The ECB encryption method is relatively easy to implement; however, it can be vulnerable to certain types of attacks, such as pattern recognition.

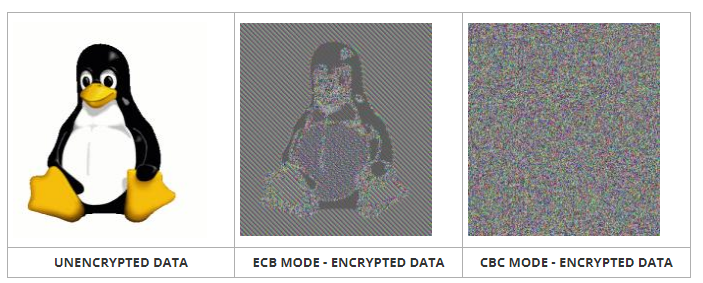
By contrast, CBC is a more secure encryption method that addresses the weaknesses of ECB. CBC encrypts plaintext blocks using the same key and combines them with the previous ciphertext blocks through an operation called an XOR. Thus, even if the same plaintext block appears multiple times in the message, it will be encrypted to a different ciphertext block each time.

The major difference between ECB and CBC is that ECB encrypts each block independently, whereas CBC encrypts each block with the previous block. CBC is therefore considered more secure and resistant to pattern recognition attacks than ECB.

Implementation of CBC mode requires an initialization vector (IV), which is a random value added to the first plaintext block before encryption. An IV is sent along with an encrypted message, so the receiver can use it to decrypt it.

ECB and CBC are symmetric-key encryption methods, meaning that the same key is used for encryption and decryption. As computing power increases, it becomes increasingly important to use more secure encryption methods, such as AES-GCM or RSA-OAEP.

The practical difference is best illustrated with this graphic :



**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**

These DES keys are considered weak because they generate only two different round keys instead of the expected 16. This happens due to the way the DES key schedule works:

Permuted Choice 1 (PC-1): This initial step takes the 56-bit key and selects specific bits to create a 56-bit subkey.

Shifting and Permutation: These operations are performed on the subkey in each round to generate the next subkey.

Let's go through each key and discuss why they are considered weak:

K1 = Alternating 0s and 1s. When these keys undergo PC-1, they essentially become all 0s or all 1s, depending on the initial bit positions chosen. Since the subsequent shifting and permutation operations are deterministic, both keys create identical round keys.

K2 = This key is considered weak because it has a very regular pattern with alternating bits (F and E). The regularity of the key reduces the effective key length, making it more susceptible to certain attacks.

K3 = This key is weak due to its lack of complexity. It contains a repeating pattern of 1xF and 0xE, which diminishes the randomness of the key.

K4 = Similar to K3, this key is weak because it exhibits a repetitive pattern (0xE and 1xF).