Programming Assignment 2B
CO21BTECH11004

Part 2B: -

- Key1: - b2df
- Key2: - 16c3
- Expanded key1: - b294df5a0b9f7dd7e26de7bd9e0af1ad
- Expanded key2: - 1694c35a7003c61f8fd5e70594684e53
- Secret Plaintext: - paddlingcanoeist

Approach: - (Python Used)

- A meet-in-the-middle attack is done.
- Choose a pair of plaintext and ciphertext.
- Generate all key1 and store the (expandedKey1, ciphertext1) obtained from the encryption of plaintext using all key1. Sort the list in ascending order based on expandedKey1.
- Generate all key2 and store the (expandedKey2, decryptCipherText1) obtained from the decryption of ciphertext using all key2. Sort the list in descending order based on the expandedKey2.
- Now, find expandedKey1 and expandedKey2, for which ciphertext1 and decryptCipherText1 are the same.
- As lists are sorted, we can find such a pair using two pointers in linear time if it exists.

Refer ProgHW2B.ipynb file and meetInMiddleAttack function in it.

The ‘secretInfo.txt’ file contains the key, expanded key, and secret plaintext decrypted from that key found by doing the brute force attack.