Programming Assignment 2A
CO21BTECH11004

Part 2A: -

- Key: - 8e6330
- Expanded key:- 8e94635ae87bde371e30e71d3b6b516e
- Secret Plaintext: - mediumaquamarine

Approach: - (Python Used)

- A brute force attack generates all 24-bit keys with the last 4 bits 0.
- Choose a pair of plaintext and ciphertext from the files given.
- Generate ciphertext corresponding to the plaintext using all the keys, and check if the obtained ciphertext is the same as ciphertext (corresponding to plaintext given in .txt file), then the key is found.

Refer ProgHW2A.ipynb file and bruteForceAttack 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.