Programming Homework 2A
Aaryan, CO21BTECH11001

The file named “`findKey_hw2a.py`” is a python program to find the key and the secret message using brute force attack.

Here are the steps involved in the program:

1. Read the plaintexts and ciphertexts from the files and convert them to bytes.

2. Use the first (plaintext, ciphertext) pair to find the key using brute force attack.

3. In the attack, we iterate over the numbers in $[0, 2^{20} - 1]$and shift the numbers 4 bits to the left. This is done because the expansion subroutine ignores the last 4 bits of the short key. Then this short key is fed into the expansion subroutine to get a 128-bit key.
   The message is encrypted using the expanded key and compared with the ciphertext.
   If there is a match, we have found the key. Otherwise, we check the next number.

After finding the key, we find the secret message by decrypting the last ciphertext using the key.

Note: To run the program, execute the command: “`python3 findKey_hw2a.py`”.

Key (hexadecimal string format): “8e94635ae87bde371e30e71d3b6b516e” (excluding the quotes).

Secret message: “mediumaquamarine” (excluding the quotes).