CO21BTECH11002
Aayush Kumar

Method:

Two for loops are run in range 0 to 1<<16. In each iteration, a key is generated using the expandKey function. In the first loop, the key corresponding to each ciphertext - key pair for the given message is stored in a dictionary in the form of an array. The second loop similarly stores plaintext - key pairs. The ciphertext obtained in the first loop must be the same as the plaintext obtained in the second loop for some (key1, key2) pair. So, in the dictionary, there will be an element whose size is 2 and it will hold the values of these 2 corresponding keys.

Results:

Key1 = b294df5a0b9f7dd7e26de7bd9e0af1ad
Key2 = 1694c35a7003c61f8fd5e70594684e53

Secret Message = paddlingcanoeist