CENG561 – Homework 2

We encrypt the L byte plaintext value by XORing a randomly selected key of the same length.

Assume plaintext, ciphertext, and key are encoded as hexadecimal.

1) Write a computer program that takes K plaintexts and K ciphertexts as inputs and outputs the correct plaintext-ciphertext pairs and the key. Ciphertexts given as inputs are produced with the same key. Your program should run in O(K^2) time.

Your program should read plaintexts and ciphertexts from two different files and write the output to another file.

Sample Plaintext File

```
ffff1111ffff1111ffff1111ffff1111ffff1111
aaaac2c2aaaac2c2aaaac2c2aaaac2c2aaaac2c2
8888bbbb8888bbbb8888bbbb8888bbbb8888bbbb
```

Sample Ciphertext File

```
eeee2222eeee2222eeee2222eeee2222eeee2222
cccccccccccccccccccccccccccccccccccccccc
0000333300003333000033330000333300003333
```

2) If K>1, with what probability your program will give correct results. Please prove it.

Please provide a readme file for your program. The basic command for running your program should be as follows:

```
program <plaintextfile> <ciphertextfile> <outputfile>
```

Deadline: 3/11/2021 23:59