Problem with one-time pad. We need a computer program that takes as input a plaintext length L, the number N of messages, N plaintext messages (encoded in hexadecimal) of length L, and N ciphertext messages (encoded in hexadecimal) of length L. Assuming each given ciphertext is generated by encrypting one of the given plaintexts by XORing with the same key (unknown to the program) of length L, the program outputs the plaintext-ciphertext pairs in the input and the key.

Example:

input: N=3 messages, L=60 hexadecimal characters,

Plaintext 1: 576973687468617449686164626565e626f726e6c6f6e676265666f7265,
Plaintext 2: 4d7962726f7468657273676f746d657570616761696e737474686577616c
Plaintext 3: 4f6e656d6f7265646179616e644977696c6c62655468656b696e67466f72

Ciphertext 1: d7e1b2e3e7432e2eb0fb14e84c4a77e1f6331f8eceed0b4ce72e0760ebde
Ciphertext 2: d5f6b5fce745232fa3f112e95c6e65fdea3e1a8af3eb1d53fa280551e5c0
Ciphertext 3: cdf1a3f9fc5f273f8be012e35a4277fae43d0a81cbec165ff1230478f8d7

output:

pairs:

(Plaintext 1, Ciphertext 3), (Plaintext 2, Ciphertext 1), (Plaintext 3, Ciphertext 2)

key:

9a98d0918837464bc2887387382712948652 78efa7837838934662178ab2

1. (10points) Regarding the above problem, prove that for N=2, if the key is uniformly picked from the space defined by the length L, there exists no program that can give the correct output with probability more than ½.

2. (20 points) Regarding the above problem, prove that for N>2, even if the key is uniformly picked from the space defined by the length L, there exists a program that can always give the correct output with probability 1.

3. (70 points) Design and write a computer program in any language you choose. Your program should run in $O(N^2L)$ time, so show that it indeed does by analyzing the pseudocode of your program.

Upload your text answers as a separate pdf file. Also, compress the programming project as a .zip file for upload. Include a readme file for instructions to a quick run of your program. For full point, a pdf file for answers and a .zip file for project should be provided.

not: A separate file for input test will also be provided.