Due Date: 24 Sep 2023 CS6160: Cryptology

Programming Assignment 1

Many-time pad is insecure.

Consider the one-time pad encryption where the ciphertext is the XOR of the message and the key. Reusing the key makes the system insecure, as we see in this assignment.

A set of 12 messages, each message an English sentence, has been encrypted, using a common key, and the ciphertext file is given to you. Write a program and find the key; also output the first and last plaintext messages.

Hints:

1. The XOR of the space character with a letter changes the case (from upper to lower/lower to upper).
2. Compute pairwise XORs of the ciphertexts.