MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Recycled One-Time Pad

Author: George Ho

November 2012

Introduction

The classical one-time pad (OTP) is an encryption method that is essentially a Vigenère cipher using a long and random sequence of letters as key. The strength of the OTP comes from the fact that the key is completely random, and that there is no repetition that can be exploited, e.g., by the Kasiski or Friedman tests. Although the OTP offers perfect security, the drawback is that the random key can only be used once and has to be of the same length as the message. Otherwise the perfect security of the OTP is compromised.

Challenge

In this challenge, you need to decipher three messages, all of which have been enciphered by a OTP using the **same** random key. The plaintexts of all three messages are in English, and are military communication during a war.

As your solution, please submit the name of the village/town/city found in one of the ciphertexts, in capital letters. For example, if the solution is Massachusetts, please enter MASSACHUSETTS.

Hint: If you can guess a part of the plaintext, you can then find the corresponding part of the key.

Chiffretexte

PERLSTXZDBFONKKYTQPQJFDEKKJODP

QHNNFIJNWSSOTGUJRNOPLMHRESMHVP

OERZTOHXANSASLKWELZBAOJNKSOUOV

Credits

This challenge was inspired by a class presentation during the course "Cryptology", summer 2012, at the Center for Talented Youth, Hong Kong University of Science and Technology.