现代密码学

实验一

1. Coursera Dan Boneh Week 1 Program Assignment

   Many Time Pad

2. PA1 option

   Write a program that allows you to "crack" ciphertexts generated using a Vigenere-like cipher, where byte-wise XOR is used instead of addition modulo 26.

3. http://www.cryptopals.com/sets/1

   (1) Convert hex to base64

   (2) Fixed XOR

   (3) Single-byte XOR cipher

   (4) Detect single-character XOR

   (5) Implement repeating-key XOR

   (6) Break repeating-key XOR

4. MTC3 Cracking SHA1-Hashed Passwords

   https://www.mysterytwisterc3.org/en/challenges/level-2/cracking-sha1-hashed-passwords