**现代密码学**

**实验一**

1. Coursera Dan Boneh Week 1 Program Assignment

Many Time Pad

1. 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.

1. http://www.cryptopals.com/sets/1
2. Convert hex to base64
3. Fixed XOR
4. Single-byte XOR cipher
5. Detect single-character XOR
6. Implement repeating-key XOR
7. Break repeating-key XOR
8. MTC3 Cracking SHA1-Hashed Passwords

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