**现代密码学**

**实验二**

1. MTC3 AES key — encoded in the machine readable zone of a European ePassport https://www.mysterytwisterc3.org/en/challenges/level-2/aes-key--encoded-in-the-machine-readable-zone-of-a-european-epassport
2. http://www.cryptopals.com/sets/2
3. Implement PKCS#7 padding
4. Implement CBC mode
5. An ECB/CBC detection oracle
6. Byte-at-a-time ECB decryption (Simple)
7. ECB cut-and-paste
8. Byte-at-a-time ECB decryption (Harder)
9. PKCS#7 padding validation
10. CBC bit flipping attacks