Cryptography Midterm Checklist

1. **Chapter 1 - Classical Cryptography**

   Definitions and Theorems
   (a) Definition of Encryption Scheme
   (b) Kerchoffs Principle
   (c) Ciphertext-only Attack
   (d) Known Plaintext Attack
   (e) Chosen-plaintext Attack
   (f) Chosen-ciphertext Attack
   (g) Shift Cipher
   (h) Vigenere Cipher

2. **Chapter 2 - Perfect Secrecy**

   Definitions and Theorems
   (a) Perfect Secrecy
   (b) Lemmas on Perfect Secrecy
   (c) Perfect indistinguishability
   (d) Adversarial indistinguishability
   (e) One Time Pad
   (f) Prove One Time Pad is perfectly secret
   (g) Limitations of Perfect Secrecy

3. **Chapter 3 - Computational Secrecy**

   Definitions and Theorems
   (a) Negligble Functions
   (b) Asymptotic Security
   (c) Psuedorandom generators
   (d) Psuedo-one Time Pad
   (e) Multimessage securitu
   (f) CPA Security
   (g) Psuedorandom Functions and Permuatations

Problems

(1) See in class handouts and homeworks