Lecture 7: Cryptography Part 1

Date: October 11, 2013 ***Homework Due***: Oct. 18 at 5:00pm

1. Cryptography and cryptanalysis
   a. What it does
   b. When it is used
   c. Basic assumptions
2. Terms
   a. Ciphers and codes
   b. Plaintext, ciphertext, key
   c. Code book
   d. Encipher, decipher
   e. Adversary
3. Types of attacks
   a. Ciphertext only — given ciphertext, find plaintext and/or key
   b. Known plaintext — given plaintext and corresponding ciphertext, find key
   c. Chosen plaintext — given the ability to select a plaintext and get the corresponding ciphertext, find the key
4. Types of cipher transformations
   a. Substitution ciphers
   b. Transposition ciphers
   c. Product ciphers
   d. Superencipherment
5. A brief history
6. Classical cryptography
   a. Simple substitution
   b. Cæsar cipher; example, with key 'D' (3), RENAISSANCE → UHQDLVVDQFH