Lecture 13 Outline

April 30, 2018

Reading: §10.2–10.2.4, F

Assignments: Homework 3, due on May 9, 2018 at 11:59pm
Lab 2, due on May 7, 2018 at 11:59pm

1. Symmetric Cryptography
   a. Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   b. Cryptanalysis: first do index of coincidence to see if it is monoalphabetic or polyalphabetic, then Kasiski method.
   c. Problem: eliminate periodicity of key
2. Long key generation
   a. Autokey cipher: key is keyword followed by plaintext or cipher text
   b. Running-key cipher: key is simply text; wedge is that (plaintext, key) letter pairs are not random (`T`/`T`, `H`/`H`, `E`/`E`, `T`/`S`, `R`/`E`, `A`/`O`, `S`/`N`, etc.)
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext; only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?
3. Product ciphers: DES