Outline for January 29, 2016

Reading: *text*, §10 handout (§9 in the book)

Assignments due: Homework 2, due February 5
Project progress report, due February 8

1. Classical 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:
      M = `THETREASUREISBURIED`
      K = `HELLOTHETREASUREISB`
      C = `ALPEFXHWNIIIKVLVQWE`
   b. Running-key cipher:
      M = `THETREASUREISBURIED`
      K = `THESECONDCIPHERISAN`
      C = `MOILVGOFXTMXZFLZAEQ`
      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
   d. Only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?
3. Product ciphers: DES, AES
4. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption computationally feasible (*note*: commutativity not required)
   c. Benefits: can give confidentiality or authentication or both
5. Use of public key cryptosystem
   a. Normally used as key interchange system to exchange secret keys (cheap)
   b. Then use secret key system (too expensive to use public key cryptosystem for this)
6. Diffie-Hellman
   a. Goal is to share a common key (*symmetric key exchange protocol*)
   b. Given n, g, prime p, compute k such that $n = g^k \bmod p$
   c. Choose k as private key, make public key $K = g^k \bmod p$