Lecture 19 Outline

Reading: *text*, §9.2 **Assignments due:** Homework 3, due May 13, 2011

1. Cryptography
   a. Codes vs. ciphers
2. 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
3. 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`?
4. Product ciphers: DES, AES