

Outline for February 22, 2006

Reading: text, §9.2

1. Greetings and felicitations!
 - a. Puzzle of the day
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's monoalphabetic or polyalphabetic, then Kasiski method.
 - c. Problem: eliminate periodicity of key
3. Long key generation
 - a. Running-key cipher: $M = \text{THETREASUREISBURIED}$; $K = \text{THESECONDCIPHERISAN}$; $C = \text{MOILVGOFXTMXZFLZAEQ}$; 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.)
 - b. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
 - c. Only cipher with perfect secrecy: one-time pads; $C = \text{AZPR}$; is that DOIT or DONT?
4. DES