Notes for October 29, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Long key generation
   a. Running-key cipher: M=THETREASUREISBURIED; K=THESECONDCIPHERISAN; C=MOIL-VGOFXTMXZFLZAEQ; 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. Enigma/rotor systems; wheels, 3 rotors and a reflecting one. Go through it; UNIX uses this for *crypt*(1) command.
   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. DES
   a. Go through the algorithm
5. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. given public key, CI 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