Notes for October 27, 1999

1. Greetings and Felicitations!
   a. Midterm moved to Friday, November 5, 1999
   b. Example program put out in ~cs153/bin; it’s dec-where, hp-where, pc-where, sgi-where (one per type of system)

2. Puzzle of the Day

3. Classical
   a. monoalphabetic (simple substitution): \( f(a) = a + k \mod n \)
   b. example: Caesar with \( k = 3 \), RENAISSANCE \( \rightarrow \) UHQDLVVDQFH
   c. polyalphabetic: Vigenère, \( f_i(a) = (a + k_i) \mod n \)
   d. cryptanalysis: first do index of coincidence to see if it’s monoalphabetic or polyalphabetic, then Kasiski method.
   e. problem: eliminate periodicity of key

4. Long key generation
   a. 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.)
   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?

5. DES
   a. Go through the algorithm

6. 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