Notes for October 24, 2000

1. Greetings and Felicitations!
   a. More questions … send to cs153@cs.ucdavis.edu the csif address seems to fail intermittently)
   b. Homework #2 will be available tomorrow on the web page
2. Puzzle of the day
3. Classical
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. polyalphabetic: Vigenère, $f_i(a) = (a + k_i) \bmod n$
   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=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?
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 authentiction or both

Puzzle of the Day

Some programs use passwords for access control, but do not protect the passwords in a very sophisticated manner (for example, by saving them in a file) or make determining the correct password very easy (for example, the Microsoft Word 5.0 encipherment scheme). The argument for using simple passwords and weak encipherment is that the data or programs being protected are of little value and the passwords give a small measure of privacy.

Given that what they are protecting is truly of little value, why is the use of such simple passwords and easily-broken encipherment bad?