Notes for January 14, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 21–46; Garfinkel & Spafford, pp. 139–159, 175–179
2. Puzzle of the day
   a. Just to get you thinking; I'll ask this one again later on to see how your thinking has changed.
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

[*ended here*]

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. Breaking UNIX *crypt*(1)
   a. Purely statistical attack is possible (me) but it takes gobs of ciphertext
   b. Known plaintext attack: that's Reeds and Weinberger's attack, with a nice suggestion by Bob Morris