Notes for January 13, 1997

1. Hello
   a. Office hours on MW moved to 10:00–11:00AM; office hours for Wednesday are cancelled
2. Puzzle of the day
   a. Thought some ruminations on what is possible would be appropriate in light of Friday's lecture …
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=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