Outline for October 6, 2021

Reading: *text*, §10.2 **Assignments:** Homework 1, due October 6; Project selection, due Oct 8

1. Symmetric Cryptography
   (a) Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   (b) Example: Caesar (shift) cipher with $k = 3$, `RENAISSANCE` $\rightarrow$ `UHQDLVVDQFH`
2. Symmetric Cryptography
   (a) Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   (b) Cryptanalysis: use index of coincidence to see if it is monoalphabetic or polyalphabetic; Kasiski method.
   (c) Problem: eliminate periodicity of key
   (d) Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext; only cipher with perfect secrecy: one-time pads; C = `AZPR`; is that `DOIT` or `DONT`?