Outline for October 11, 2023

Reading: *text*, §10.2

Assignments: Homework 1, due October 9;
Project teams, question, due October 11

1. Symmetric Cryptography
   (a) Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   (b) Example: Caesar (shift) cipher with $k = 3$, `RENAISSANCE` $\rightarrow$ `UHQDLVVDQFH`
   (c) Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   (d) Cryptanalysis: use index of coincidence to see if it is monoalphabetic or polyalphabetic; Kasiski method.
   (e) Problem: eliminate periodicity of key
   (f) 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 M = `DOIT` or M = `DONT`?
2. Product ciphers
   (a) DES