Outline for April 14, 1997

1. Greetings and Felicitations
2. Simple substitution ciphers
   a. Do Caesar cipher
   b. Go through how to break it
   c. Present Vigenère tableau
   d. Discuss breaking it (Kasiski method). Note index of coincidence is probability 2 letters chosen at random from ciphertext are alike
   e. Generalize to very long keys and show running key and autokey
   f. Go through rotor systems (Enigma)
   g. Go through one-time pads
3. Polygram substitution cipher: Playfair
   a. Key is 5 by 5 grid
   b. If m_1, m_2 in same row, c_1, c_2 are to immediate right of m_1, m_2 respectively
   c. If m_1, m_2 in same column, c_1, c2 are below m_1, m_2
   d. If $m_1 = m_2$, insert null in text
   e. if m_1, m_2 in different rows and columns, c_1, c_2 form rectangle with c_1 in m_1's row and c_2 in m_2's row
   f. if odd number of characters in message, append null.