Homework for Cryptographers

1. **Read:** Chap 1 Sec 1, 2; Chap 2 Sec 1, 2; Chap 3 Sec 1, 2, 3
   Do by hand: Section 2.13 # 1, 2, 3
   Computer Problems: Section 2.14 # 1, 2; Section 3.14 # 1

2. **Read:** Chap 2 Sec 3, 4, 5
   Do by hand: Section 2.13 # 5, 6, 8, 10, 11; Section 3.13 # 1, 3, 4
   Computer Problems: Section 2.14 # 3, 4

3. **Read:** Chap 2 Sec 6, 7, 8, 9
   Do by hand: Look up the adjoint method for calculating inverses of matrices; use it to invert
   $$\begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 3 \\ 1 & 2 & 1 \end{pmatrix}$$
   Also do playfair/adfgx problems from handout
   Computer Problems: Section 2.14 # 7, 8, 9

4. **Read:** Chap 2 Sec 10, 12, Chap 4 Sec 1, 2
   Do by hand: Section 2.13 # 13, 14, 15, 16a, 17; Section 3.13 # 18, 19
   Using Paper Enigma, rotors ordered III,I,II, keyword "APE", encrypt 'mystery'
   Using Paper Enigma, rotors ordered I,II,III, keyword "MCK", decrypt 'MJIDO MZWZJFJR'
   Computer Problems: Section 2.14 # 10

5. **Read:** Chap 4 Sections 4, 5, 6, 7
   Do by hand: DES practice problems from handout
   Computer Problems: None

6. **Read:** Any of the above sections that you haven't yet read
   Do by hand: Section 4.9 # 1, 2, 4, 5, 6, 7, 8
   Also, work through Exam 1 Funpack, and study for test!
   Computer Problems: None

7. **Read:** Chapter 5 all, Chapter 3 sections 5, 6, Chapter 6 Sections 1, 2
   Do by hand: Section 3.13 # 33, 34, and

   (a) Show that $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

   (b) Show that $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field

   (c) Recognize $\mathbb{Z}_2[x]/(x^2 + x + 1)$ as a field that you know and love, and prove it's what you think it is.

   Computer Problems: None

8. **Read:** Chapter 6 Sections 1-5
   Do by hand: Section 3.13 # 33, 34; Section 5.5 # 1,2, and
   Calculate $(45_{16})^{-1}$ in $GF(2^8)$ [I think you should get 31_{16}]
   Computer Problems: None

9. **Read:** None
   Do by hand: Section 3.13 # 11, 12, 13, 14, 15, 16, 26
   Computer Problems: None

10. **Read:** None
    Do by hand: Section 3.13 # 14, 15, 16; Section 6.8 # 1, 3, 4, 5, 8
    Computer Problems: Section 6.9 # 1, 2, 3

11. (For Friday) **Read:** Chapter 6 Sections 1-5, if you haven't already
    Do by hand: Section 6.8 # 11, 12, 14, 16, 17, 18, 19
    Computer Problems: Section 6.9 # 4, 5, 6, 8, 9, 10