Problem Set 3

Due on Wednesday, October 22, 2008.

In the problems below, "textbook" refers to Douglas R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, 2006.

Problem 1: Feistel Network

Textbook, problem 3.2.

Problem 2: DES Complementation Property

Textbook, problem 3.3.

Problem 3: DES S-box S_4

Textbook, problem 3.11(a). [Omit part (b).]

Problem 4: Practice with mod

Read pages 3–4 of textbook and then work the following:

(a) Textbook, problem 1.1.

(b) Textbook, problem 1.2.

(c) Textbook, problem 1.3.

(d) Textbook, problem 1.4.

Problem 5: Extended Euclidean Algorithm

Textbook, problem 5.3. Show your work.

Problem 6: Linear Diophantine Equations

Textbook, problem 5.4. Show your work.

Problem 7: RSA Encryption

[This is problem 6.8.2 from Trapp & Washington, "Introduction to Cryptography with Coding Theory, Second Edition", Pearson Prentice Hall, 2006.]
Suppose your RSA modulus is $n = 55 = 5 \times 11$ and your encryption exponent is $e = 3$.

(a) Find the decryption modulus d.

(b) Assume that $\gcd(m, 55) = 1$. Show that if $c \equiv m^3 \pmod{55}$ is the ciphertext, then the plaintext is $m \equiv c^d \pmod{55}$. Do not quote the fact that RSA decryption works. That is what you are showing in this specific case.