CEN 448
Security and Internet Protocols
Instructor: Dr. Mostafa Dahshan
Teaching Assistant: Eng. Nasir Hussain
First Semester 1430/1431 H

Homework 2

Due Date: Monday, 02/11/2009.

Review Questions

1. Compare between a monoalphabetic cipher and a polyalphabetic cipher?

2. What are two problems with the one-time pad?

3. What is the importance of Feistel Cipher?

4. What are the parameters of Feistel Cipher that determine the actual algorithm?

Problems

1. In Feistel cipher, show that RD2 = LE14 and LD2 = RE14.

2. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key K and the plaintext, namely:

in hexadecimal notation: 0 1 2 3 4 5 6 7 8 9 A B C D E F

in binary notation: 0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 0100 1101 1110 1111

a. Derive K_1, the first-round subkey.
b. Derive L_0, R_0.
c. Expand R_0 to get $E[R_0]$, where $E[\cdot]$ is the expansion function of Figure 3.8.
d. Calculate $A = E[R_0] \oplus K1$.
e. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
f. Concatenate the results of (e) to get a 32-bit result, B.
g. Apply the permutation to get P(B).
h. Calculate $R_1 = P(B) \oplus L0$.
i. Write down the ciphertext.