KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH
TRƯỜNG ĐH BÁCH KHOA TP.HCM

Cryptography and Network Security
Tutorial 2

Hieu Nguyen

Ngày 2 tháng 2 năm 2015

Exercise 1. Consider the substitution defined by row 1 of S-box S1 in Table 3.3. Show a block diagram similar to Figure 3.2 that corresponds to this substitution

Exercise 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 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:

```
0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111
```

EXPRESS YOUR ANSWERS IN BINARY NOTATION IN 4-BIT GROUPS WITH SPACE SEPERATORS (I.E., 0010 1100 1110, ETC.)!

Part a. Derive K_1, the first round key.
Part b. Derive L_0, R_0
Part c. Expand R_0 to get $E[R_0]$, where E is the expansion function of Table 3.2.
Part d. Calculate $A = E[R_0] \oplus K_1$
Part e. Group the 48-bit result of part d into sets of 6 bits and evaluate the coresponding S-box substitutions. Express your answers in decimal and binary.

Hint: Be sure you count 0, 1, 2, 3, etc for row and column position when doing the S-box lookup.
Part f. Concatenate the results of part e to get a 32-bit result, B. Express the answer in binary.
Part g. Apply the permutation to get P(B).
Part h. Calculate $R_1 = P(B) \oplus L_0$
Part i. Write down the cipher text.

Exercise 3. Using S-DES, decrypt the string (10100010) using the key (0111111101) by hand.
Show intermediate results after each function (IP, FK, SW, FK, IP-1). Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2 (i.e., A = 0000, B = 0001, ..., P = 1111). Hint: As a midway check, after the application of SW, the string should be (00010011).