# DES Example

15CS434E

Network Security

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:

| | |
|---|---|
| **Hexadecimal notation:** | 0 1 2 3 4 5 6 7 8 9 A B C D E F |
| **Binary notation:** | 0000 0001 0010 0011 0100 0101 0110 0111 |
| | 1000 1001 1010 1011 1100 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 Table 3.2.
d. Calculate $A = E[R_0] \oplus K_1$.
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 $R_1 = P(B) \oplus L_0$.
i. Write down the ciphertext.

**a.** First, pass the 64-bit input through PC-1 to produce a 56-bit result. Then perform a left circular shift separately on the two 28-bit halves. Finally, pass the 56-bit result through PC-2 to produce the 48-bit *K*1.:

in binary notation:

0000 1011 0000 0010 0110 0111

1001 1011 0100 1001 1010 0101

in hexadecimal notation: 0 B 0 2 6 7 9 B 4 9 A 5

**b.** L0, R0 are derived by passing the 64-plaintext through IP (Table 3.2a):

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

**c.** The E table (Table 3.2c) expands R0 to 48 bits:

E(R0) = 011110 100001 010101 010101 011110 100001 010101 010101

- **d.** A = 011100 010001 011100 110010 111000 010101 110011 110000

- **e.** (1110) = (14) = 0 (base 10) = 0000 (base 2)
- (1000) = (8) = 12 (base 10) = 1100 (base 2)
- (1110) = (14) = 2 (base 10) = 0010 (base 2)
- (1001) = (9) = 1 (base 10) = 0001 (base 2)
- (1100) = (12) = 6 (base 10) =

- P(B) = 1001 0010 0001 1100 0010 0000 1001 1100

h. R1 = 0101 1110 0001 1100 1110 1100 0110 0011

- **i.** L1 = R0. The ciphertext is the concatenation of L1 and R1.

- If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

- Nine plaintext characters are affected. The plaintext character corresponding to the ciphertext character is obviously altered. In addition, the altered ciphertext character enters the shift register and is not removed until the next eight characters are processed.

# RC4

- What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order.

- Use a key of length 255 bytes. The first two bytes are zero; that is K[0] = K[1] = 0. Thereafter, we have: K[2] = 255; K[3] = 254; … K[255]= 2.