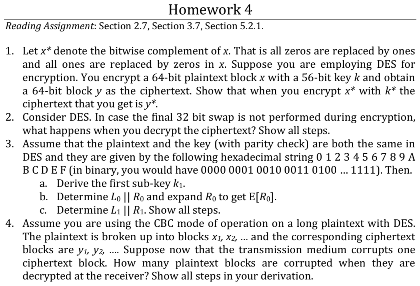


Homework 4

Reading Assignment: Section 2.7, Section 3.7, Section 5.2.1.

1. Let x^* denote the bitwise complement of x. That is all zeros are replaced by ones and all ones are replaced by zeros in x. Suppose you are employing DES for encryption. You encrypt a 64-bit plaintext block x with a 56-bit key k and obtain a 64-bit block y as the ciphertext. Show that when you encrypt x^* with k^* the ciphertext that you get is y^*.
2. Consider DES. In case the final 32 bit swap is not performed during encryption, what happens when you decrypt the ciphertext? Show all steps.
3. Assume that the plaintext and the key (with parity check) are both the same in DES and they are given by the following hexadecimal string 0 1 2 3 4 5 6 7 8 9 A B C D E F (in binary, you would have 0000 0001 0010 0011 0100 ... 1111). Then.
   a. Derive the first sub-key k_1.
   b. Determine $L_0 \,||\, R_0$ and expand R_0 to get $E[R_0]$.
   c. Determine $L_1 \,||\, R_1$. Show all steps.
4. Assume you are using the CBC mode of operation on a long plaintext with DES. The plaintext is broken up into blocks $x_1, x_2, \ldots$ and the corresponding ciphertext blocks are $y_1, y_2, \ldots$. Suppose now that the transmission medium corrupts one ciphertext block. How many plaintext blocks are corrupted when they are decrypted at the receiver? Show all steps in your derivation.

1) Given: $L^i = R^{i-1}$ & $R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$, let $i=1$

i) The init. permutation, $IP(x^*)$, $= [IP(x)]^*$, since the permutation operation preserves complements.

ii) The expansion operation also preserves complements, $E(x^*) = [E(x)]^*$

iii) The key schedule operation also reserves the complement since this is comprised of permutations and shifts.

iv) $K^i \oplus E(x^*) = K^i \oplus [E(x)]^*$ from (ii)

v) $K^{i*} \oplus [E(x)]^* = K^i \oplus [E(x)]$ since, in general, $a^* \oplus b^* = a \oplus b$.

$\Rightarrow$ vi) $f(R^{i-1*}, K^{i*}) = f(R^{i-1}, K^i)$ from (v)

$\Rightarrow L^{i-1*} \oplus f(R^{i-1*}, K^{i*}) = L^{i-1*} \oplus f(R^{i-1}, K^i) = [L^{i-1} \oplus f(R^{i-1}, K^i)]^*$

$\Rightarrow R^i(x^*) = [R^i(x)]^*$ & $L^i = R^{i-1}$ $\forall i$ in the rounds

$\Rightarrow d_k[e_k(x^*, k^*)] = d_k[[e_k(x, k)]^*] = d_k^* = y^*$

2) Given i) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, ii) $a \oplus a = 0$, iii) $a \oplus 0 = a$, let e = encryption, d = decryption

$\Rightarrow L_e^{16} = R_e^{15}$ & $R_e^{16} = L_e^{15} \oplus f(R_e^{15}, K^{16})$;

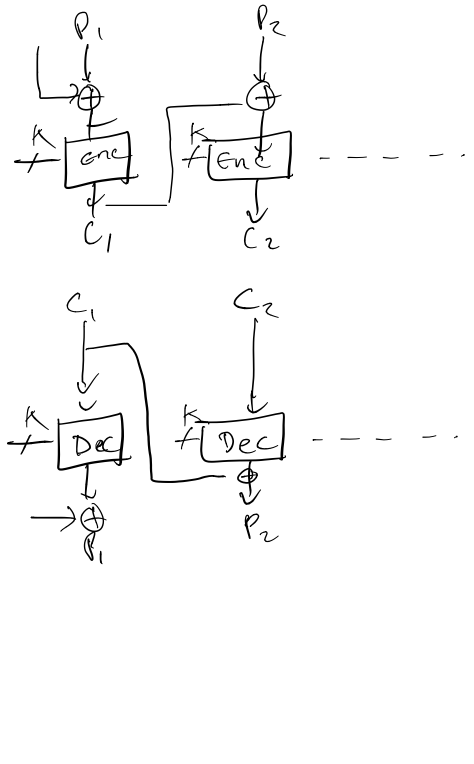
$L_d^1 = R_d^0 = L_e^{16} = R_e^{15}$ & $R_d^1 = L_d^0 \oplus f(R_d^0, K^{16})$

$\Rightarrow R_d^1 = R_e^{16} \oplus f(R_e^{15}, K^{16}) = [L_e^{15} \oplus f(R_e^{15}, K^{16})] \oplus f(R_e^{15}, K^{16})$

Since $L_d^1 = R_e^{15}$ & $R_d^1 = L_e^{15}$, if we failed to complete the last 32 bit swap & then attempted to decrypt, we would obtain the 32 bit swap of the input to the last encryption round.

3) See attached excel sheet

4) Only one plaintext block is corrupted.


P1
P2
K
Enc
K
Enc
C1
C2
C1
C2
K
Dec
K
Dec
P2
P1