Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 5
- Proposed Solution -

Friday, May 26, 2017

Solution of Problem 1

a) DES decryption is the same as DES encryption with keys applied in the reversed order.

b) With $K_0 = (\texttt{01FE 01FE 01FE 01FE})$, we obtain:

$$
C_0 \uparrow \quad
\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}
\quad \uparrow D_0
$$

Thus we read (C_0, D_0) column-wise. (C_1, D_1) are computed by a cyclic left-shift by 1 position:

$$
\begin{aligned}
C_0 &= (1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010)_2 = (AAAAAAA)_{16} \\
D_0 &= (1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010)_2 = (AAAAAAA)_{16} \\
C_1 &= (0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101)_2 = (5555555)_{16} \\
D_1 &= (0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101)_2 = (5555555)_{16}
\end{aligned}
$$

For $\hat{K}_0 = (\texttt{FE01 FE01 FE01 FE01})$, we obtain $(\hat{C}_0, \hat{D}_0)$ analogously. $(\hat{C}_1, \hat{D}_1)$ are computed by a cyclic left-shift by 1 position:

$$
\begin{aligned}
\hat{C}_0 &= (0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101)_2 = (5555555)_{16} \\
\hat{D}_0 &= (0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101)_2 = (5555555)_{16} \\
\hat{C}_1 &= (1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010)_2 = (AAAAAAA)_{16} \\
\hat{D}_1 &= (1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010)_2 = (AAAAAAA)_{16}
\end{aligned}
$$

We have $C_0 = D_0 = \hat{C}_1 = \hat{D}_1$ and $C_1 = D_1 = \hat{C}_0 = \hat{D}_0$.

c) When K_0 is used, we obtain (C_0, D_0) as in (a). The bits of (C_{n-1}, D_{n-1}) are cyclically left-shifted by s_n positions to generate (C_i, D_i) for $i = 1, ..., 16$. Due to the structure of (C_0, D_0), cyclic right-shifts provide only two different keys:

- An even number of positions provides the identical key.
- An odd number of positions provides the alternative key.

Thus from the definition of s_n for $n = 1, ..., 16$, we observe that:

$$K_1 = K_9 = K_{10} = K_{11} = K_{12} = K_{13} = K_{14} = K_{15},$$
$$K_2 = K_3 = K_4 = K_5 = K_6 = K_7 = K_8 = K_{16}$$

d) The key K_0 generates $(K_1...K_{16}) = K_1K_2K_2K_2K_2K_2K_2K_2K_1K_1K_1K_1K_1K_1K_1K_2$
The key $\hat{K}_0$ generates $(\hat{K}_1...\hat{K}_{16}) = K_2K_1K_1K_1K_1K_1K_1K_1K_2K_2K_2K_2K_2K_2K_2K_1$

Since $\hat{K}_0$ has the reverse ordering of K_0, we obtain $\mathrm{DES}_{\hat{K}_0}(\mathrm{DES}_{K_0}(M)) = M$.

Solution of Problem 2

a) Show the validity of the complementation property: $\mathrm{DES}(M, K) = \overline{\mathrm{DES}(\overline{M}, \overline{K})}$.

Consider each operation of the DES encryption for the complemented input. In order to track the impact of the complemented input, we will introduce auxiliary variables T_1, U_1, V_1, W_1.

- $\mathrm{IP}(\overline{M}) = \overline{\mathrm{IP}(M)} = (\overline{L_0}, \overline{R_0})$, permutation does not affect the complement
- $\mathrm{E}(\overline{R_0}) = \overline{\mathrm{E}(R_0)} := \overline{T}_1$, the doubled/expanded bits are also complemented
- $\overline{T_1} \oplus \overline{K_1} = T_1 \oplus K_1 := U_1$, XOR ($\oplus$) of complements is unchanged

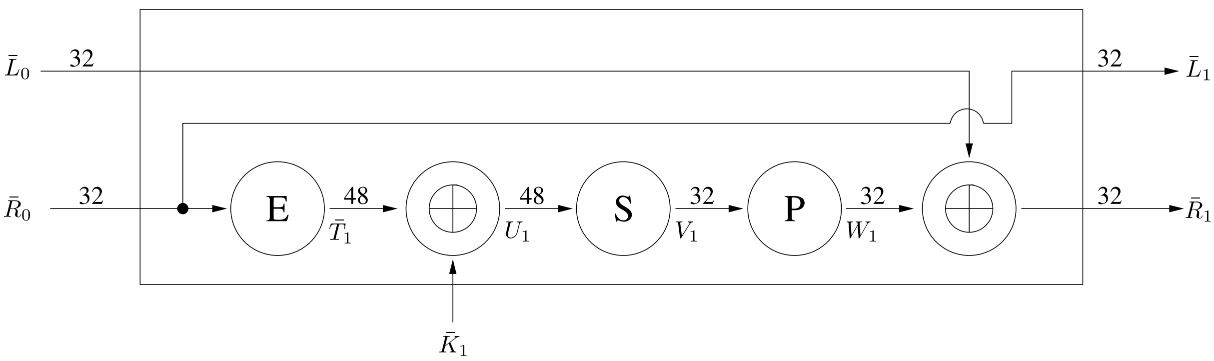
  We have:

$\oplus$	0	1
0	0	1
1	1	0

  and for the complements:

$\oplus$	$\bar{0}$	$\bar{1}$
$\bar{0}$	0	1
$\bar{1}$	1	0

- $\mathrm{S}(U_1) := V_1$ is unchanged w.r.t. the non-complementary case
- $\mathrm{P}(V_1) := W_1$ is unchanged w.r.t. the non-complementary case
- $W_1 \oplus \overline{L_0} = \overline{R}_1$, next input is just complemented
- $L_1 = \overline{R_0} = \overline{L}_1$, next input is just complemented
- $\Rightarrow$ Thus, we obtain $\mathrm{SBB}(\overline{R}_1, \overline{L_1}) = \overline{\mathrm{SBB}(R_1, L_1)}$
- Analogous iterations for each $i = 2, ..., 16$: $(\overline{L}_1, \overline{R}_1) \rightarrow \cdots \rightarrow (\overline{L_{16}}, \overline{R_{16}})$
- $\mathrm{IP}^{-1}(\overline{R_{16}}, \overline{L_{16}})$, permutation does not affect the complement
- As a result, $\mathrm{DES}(\overline{M}, \overline{K}) = \overline{\mathrm{DES}(M, K)}$ ✓



b)
- In a brute-force attack, the amount of cases is halved since we can apply a chosen-plaintext attack with M and $\overline{M}$.

Solution of Problem 3

a) Let us first take a look at Table 5.1 (Permutation Choice 1). Which bits are used to construct C_0 and D_0 from K_0?

C_0 is constructed from:

- Bits $1, 2, 3$ of the first 4 bytes, and
- bits $1, 2, 3, 4$ of the last 4 bytes

D_0 is constructed from:

- Bits $4, 5, 6, 7$ of the first 4 bytes, and
- bits $5, 6, 7$ of the last 4 bytes

Note that this particular structure is also indicated by the given weak key.

This construction can also be seen in the following table:

	1	2	3	4	5	6	7	b_1	
	9	10	11	12	13	14	15	b_2	
	17	18	19	20	21	22	23	b_3	
	25	26	27	28	29	30	31	b_4	
	33	34	35	36	37	38	39	b_5	
	41	42	43	44	45	46	47	b_6	
	49	50	51	52	53	54	55	b_7	
C_0 $\uparrow$	57	58	59	60	61	62	63	b_8	$\uparrow$ D_0

When considering C_0, read columnwise (bottom to top) and from left to right. Table 5.1 (PC1) has exactly the same sequence, i.e., we have discovered a part of its construction principle. Similar steps are applied to construct D_0.

When regarding the bit-sequence of the given round key $K_0 =$ `0x1F1F 1F1F 0E0E 0E0E`, we now easily see that:

- All bits of C_0 are 0, and all bits of D_0 are 1.
- For the given C_0 and D_0, cyclic shifting does not change the bits at all.
  $\Rightarrow$ We obtain $C_i = C_0$ and $D_i = D_0$ for all rounds $i = 1, ..., 16$.
  $\Rightarrow$ All round keys are the same: $K_1 = K_2 = \ldots = K_{16}$.
- Since decryption in DES is executing the encryption with round keys in reverse order, we observe that encryption acts identically to decryption for given weak key. Thus, a twofold encryption with the weak key, yields the original plaintext:

$$\mathrm{DES}_K(\mathrm{DES}_K(M)) = M \quad \forall M \in \mathcal{M}$$

b) In order to find further weak keys, we intend to produce $K_1 = K_2 = \ldots = K_{16}$. It suffices to generate C_0 and D_0 such that they contain only either zeros or ones only. In particular, we choose the bits $K = XXXXYYYY$ with the first 4 bytes X and the last 4 bytes Y such that:

$$X = bbbcccc* \,, \quad Y = bbbbccc* \,, \quad b, c \in \{0, 1\} \,.$$

with $*$ fulfilling the corresponding parity check condition. Then C_0 and D_0 become

$$C_0 = bb \ldots b \,, \quad D_0 = cc \ldots c$$

and it holds that

$$C_0 = C_n \,, \quad D_0 = D_n \quad \forall\, 0 \leq n \leq 16 \,,$$

because C_n, D_n are created by a cyclic shift of C_0, D_0 respectively.

The 4 weak keys are simply all possible cases of $b, c \in \{0, 1\}$ with the proper parity bits:

$$\begin{aligned}
K_1 &= \texttt{0x0101 0101 0101 0101} \,, \quad b = c = 0 \,, \quad d = e = 1 \\
K_2 &= \texttt{0x1F1F 1F1F 0E0E 0E0E} \,, \quad b = 0 \,, \quad c = 1 \,, \quad d = 1 \,, \quad e = 0 \\
K_3 &= \texttt{0xE0E0 E0E0 F1F1 F1F1} \,, \quad b = 1 \,, \quad c = 0 \,, \quad d = 0 \,, \quad e = 1 \\
K_4 &= \texttt{0xFEFE FEFE FEFE FEFE} \,, \quad b = c = 1 \,, \quad d = e = 0
\end{aligned}$$