Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 5
- Proposed Solution -

Friday, May 17, 2019

Solution of Problem 1

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	
C_0 ↑	49	50	51	52	53	54	55	b_7	↑ D_0
	57	58	59	60	61	62	63	b_8	

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

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

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:

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

Solution of Problem 2

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \in \mathbb{F}_{2^8}^4 \tag{1}$$

It is to show that:

$$(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \equiv \textstyle\sum_{i=0}^{3} r_i u^i \pmod{(u^4+1)}. \tag{2}$$

We expand the multiplication on the left hand side of (2), reduce it modulo $u^4 + 1 \in \mathbb{F}_{2^8}[u]$, and use the abbreviations $(r_0, r_1, r_2, r_3)'$ according to (1).

$$\begin{aligned}
&(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \\
= \;&c_3(x+1)u^6 + c_3u^5 + c_3u^4 + c_3xu^3 + \\
&c_2(x+1)u^5 + c_2u^4 + c_2u^3 + c_2xu^2 + \\
&c_1(x+1)u^4 + c_1u^3 + c_1u^2 + c_1xu + \\
&c_0(x+1)u^3 + c_0u^2 + c_0u + c_0x \\
= \;&[c_3(x+1)]u^6 + [c_3 + c_2(x+1)]u^5 + [c_3 + c_2 + c_1(x+1)]u^4 \\
&+ [c_3x + c_2 + c_1 + c_0(x+1)]u^3 + [c_2x + c_1 + c_0]u^2 + [c_1x + c_0]u + c_0x.
\end{aligned}$$

Now, we apply the modulo operation and merge terms:

$$\begin{aligned}
&\equiv [c_3x + c_2 + c_1 + (x+1)c_0]u^3 + [c_3(x+1) + c_2x + c_1 + c_0]u^2 + \\
&\quad [c_3 + c_2(x+1) + c_1x + c_0]u + [c_3 + c_2 + c_1(x+1) + c_0x] \\
&\overset{(1)}{\equiv} r_3u^3 + r_2u^2 + r_1u + r_0 \equiv \sum\nolimits_{i=0}^{3} r_iu^i \pmod{(u^4+1)}
\end{aligned}$$