Exercise 6 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-06-11

Solution of Problem 16

Given: Alphabet $\mathcal{A}$, blocklength $n \in \mathbb{N}$ and $\mathcal{M} = \mathcal{A}^n = \mathcal{C}$.
$\mathcal{A}^n$ describes all possible streams of n bits.

a) An encryption is an injective function $e_K : \mathcal{M} \to \mathcal{C}$, with $K \in \mathcal{K}$.
Fix key $K \in \mathcal{K}$. As $e(\cdot, K)$ is injective, it holds:

- $\{e(M, K) \mid M \in \mathcal{M}\} \subseteq \mathcal{C}$
- $\{e(M, K) \mid M \in \mathcal{M}\} = \mathcal{M}$
- Since $\mathcal{M} = \mathcal{C} \Rightarrow e(\mathcal{M}, K) = \mathcal{C}$ also surjective
- $\Rightarrow e(\mathcal{M}, K)$ is a bijective function.

A permutation π is a bijective (one-to-one) function $\pi : \mathcal{X} \to \mathcal{X}$.
$\Rightarrow$ For each K, the encryption $e(\cdot, K)$ is a permutation with $\mathcal{X} = \mathcal{A}^n$.

b) With $\mathcal{A} = \{0, 1\} \Rightarrow |\mathcal{A}| = |\{0, 1\}| = 2$, and $n = 6$ there are $N = 2^6 = 64$ elements.
It follows that there are $64! \approx 1.2689 \cdot 10^{89}$ different block ciphers.

Solution of Problem 17

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
57	58	59	60	61	62	63	b_8

C_0 ↑ ↑ 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:

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

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:

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

Solution of Problem 18

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

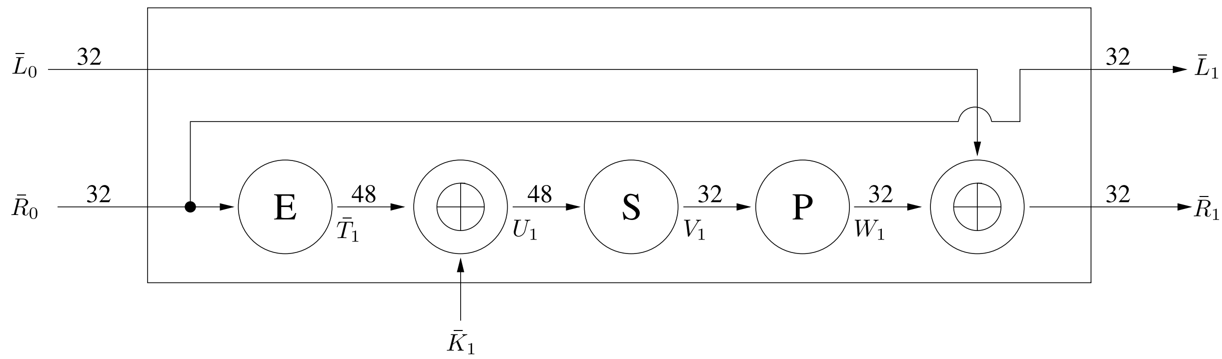
  We have:

$\oplus$	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
- $W_1 \oplus \overline{L_0} = \bar{R}_1$, next input is just complemented
- $L_1 = \overline{R_0} = \bar{L}_1$, next input is just complemented
- $\Rightarrow$ Thus, we obtain $\mathrm{SBB}(\bar{R}_1, \overline{L_1}) = \overline{\mathrm{SBB}(R_1, L_1)}$
- Analogous iterations for each $i = 2, ..., 16$: $(\overline{L_1}, \overline{R_1}) \to \cdots \to (\overline{L_{16}}, \overline{R_{16}})$
- $\mathrm{IP}^{-1}(\overline{R_{16}}, \overline{L_{16}})$, 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 19

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

It is to show that:

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

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:

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