**Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon**

# Exercise 5
# - Proposed Solution -

Friday, May 27, 2016

## Solution of Problem 1

For an affine cipher in $\mathbb{Z}_{26}$: $e(i,(a,b)) = a \cdot i + b \mod 26$

$$\mathbb{Z}_{26}^* = \{1,3,5,7,9,11,15,17,19,21,23,25\} = \{a|\gcd(a,26)=1\}$$

$$\Rightarrow |\mathcal{K}| = |\mathbb{Z}_{26}^* \times \mathbb{Z}_{26}| = 12 \cdot 26$$

Let $M \in \mathcal{M}$, $C \in \mathcal{C}$

$$\begin{aligned}
P(\hat{C} = C|\hat{M} = M) &= P(e(\hat{M},\hat{K}) = C \mid \hat{M} = M) \\
&\overset{(\hat{K},M \text{ stoch. ind.})}{=} P(e(M,\hat{K}) = C) \\
&\overset{(\hat{K} \text{ unif. distr.})}{=} \frac{1}{|\mathcal{K}|}|\{K \in \mathcal{K} \mid e(M,K) = C\}| \\
&\overset{(*)}{=} \frac{12}{12 \cdot 26} = \frac{1}{26}
\end{aligned}$$

$$(*) : e(M,(a,b)) = C \Leftrightarrow a \cdot M + b = C \mod 26 \Leftrightarrow b = C - aM \mod 26$$

$$\Rightarrow \text{ all keys } (a, C-aM),\ a \in \mathbb{Z}_{26}^* \text{ satisfy this equation}$$

$$\Rightarrow P(\hat{C} = C|\hat{M} = M) = \frac{1}{26} \quad \forall M \in \mathcal{M}_+$$

$$\Rightarrow P(\hat{C} = C) = \frac{1}{26} = P(\hat{C} = C|\hat{M} = M)$$

With Corollary 4.11, the cryptosystem has perfect secrecy, i.e., $\hat{C}$ and $\hat{M}$ are stochastically independent.

## Solution of Problem 2

Recall:

$$\begin{aligned}
|\mathcal{M}_+| &:= \{M \in \mathcal{M}_+ | P(\hat{M} = M > 0)\} \\
|\mathcal{K}_+| &:= \{K \in \mathcal{K}_+ | P(\hat{K} = K > 0)\} \\
|\mathcal{C}_+| &:= \{C \in \mathcal{C}_+ | P(\hat{C} = C > 0)\}
\end{aligned}$$

With Lemma 4.12 a):

$$|\mathcal{M}_+| \leq |\mathcal{C}_+| \leq |\mathcal{C}| = |\mathcal{M}| = |\mathcal{M}_+| \Longrightarrow |\mathcal{C}_+| = |\mathcal{C}| \Longrightarrow \mathcal{C}_+ = C \Longrightarrow P(\hat{C} = C) > 0 \quad \forall C \in \mathcal{C}$$

Let $M \in \mathcal{M}, C \in \mathcal{C}$

$$0 < P(\hat{C} = C) = P(\hat{C} = C|\,\hat{M} = M) = P(e(\hat{M}, \hat{K}) = C) \overset{\hat{M},\hat{K} sto.ind}{=} P(e(M, \hat{K}) = C) =$$

$$= \sum_{K \in \mathcal{K}: e(M,K)=c} P(\hat{K} = K) \neq 0 \Longrightarrow \forall M \in \mathcal{M}, C \in \mathcal{C}, \exists K \in \mathcal{K}: \; e(M, K) = C$$

Fix $M : |\mathcal{C}_+| = |\mathcal{C}| = |\{e(M, K)|K \in \mathcal{K}_+ = K\}| \leq |\mathcal{K}| = |\mathcal{C}| \Longrightarrow$ It follows that K is unique !

Let $M \in \mathcal{M}, C \in \mathcal{C}, \Longrightarrow P(\hat{C} = C) = P(\hat{K} = K(M, C))$
Because of perfect secrecy that is independent of M.

Fix $C_o \in \mathcal{C} \Longrightarrow \{K(M, C_o)|M \in \mathcal{M}\} = \mathcal{K},$ due to the injectivity of $e(\cdot, K)$
and the sets have the same order

$$\Longrightarrow P(\hat{C} = C) = P(\hat{K} = K) \quad \forall C \in \mathcal{C}, K \in \mathcal{K}$$

$$\Longrightarrow P(\hat{K} = K) = \frac{1}{|\mathcal{K}|}$$

## Solution of Problem 3

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 $\pi$ 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 4

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

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 $T_1, U_1, V_1, W_1$.

- $\text{IP}(\overline{M}) = \overline{\text{IP}(M)} = (\overline{L_0}, \overline{R_0})$, permutation does not affect the complement
- $\text{E}(\overline{R_0}) = \overline{\text{E}(R_0)} := \overline{T}_1$, 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

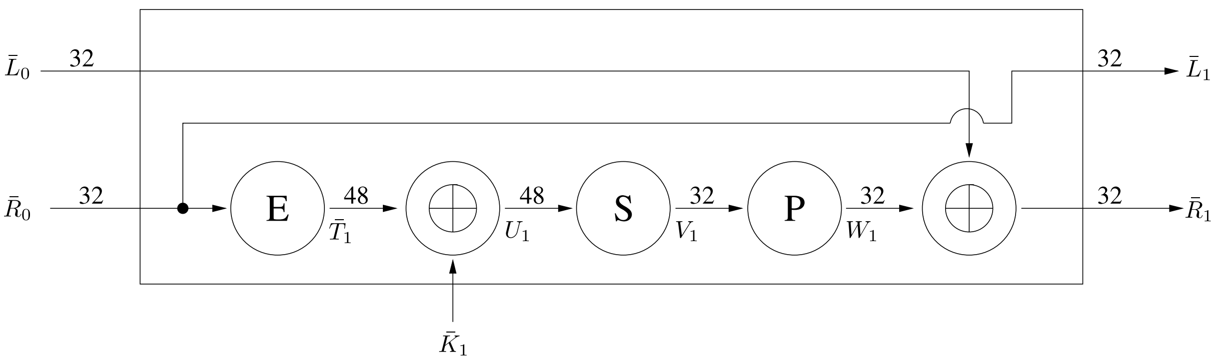
  We have:

  | $\oplus$ | 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 |

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




**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 5

**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 | $b_8$ |

$C_0$ $\uparrow$ $\qquad$ $\uparrow$ $D_0$

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

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

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:

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