Problem 1. We consider the Data Encryption Standard (DES) algorithm.

a) How can the same encryption algorithm of DES be used for decryption?

DES encrypts blocks of 64 bits using a key of 56 bits. For each 7 key bits, one (odd) parity bit for error detection is added. The key of a DES cipher is of the form:

\[ K_0 = (k_1, \ldots, k_7, b_1, k_9, \ldots, k_{15}, b_2, k_{17}, \ldots, k_{57}, \ldots, k_{63}, b_8) \]

From this key \( K_0 \), 16 round keys \( K_1, K_2, \ldots, K_{16} \) are generated. The 56 key bits of \( K_0 \) are divided into two blocks \( C_0 \) and \( D_0 \) of 28 bits each as described in the left table below.

<table>
<thead>
<tr>
<th>1 2 3 4 5 6 7</th>
<th>b1</th>
<th>14 17 11 24 1 5</th>
<th>b2</th>
<th>14 17 11 24 1 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 10 11 12 13 14 15</td>
<td>b3</td>
<td>3 28 15 6 21 10</td>
<td>b4</td>
<td>3 28 15 6 21 10</td>
</tr>
<tr>
<td>17 18 19 20 21 22 23</td>
<td>b5</td>
<td>23 19 12 4 26 8</td>
<td>b6</td>
<td>23 19 12 4 26 8</td>
</tr>
<tr>
<td>25 26 27 28 29 30 31</td>
<td>b7</td>
<td>16 7 27 20 13 2</td>
<td>b8</td>
<td>16 7 27 20 13 2</td>
</tr>
<tr>
<td>33 34 35 36 37 38 39</td>
<td>PC2</td>
<td>41 52 31 37 47 55</td>
<td>46 42 50 36 29 32</td>
<td></td>
</tr>
<tr>
<td>41 42 43 44 45 46 47</td>
<td></td>
<td>41 52 31 37 47 55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49 50 51 52 53 54 55</td>
<td></td>
<td>41 52 31 37 47 55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57 58 59 60 61 62 63</td>
<td></td>
<td>41 52 31 37 47 55</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\( C_0 \) is read column-wise from 57 to 36 and \( D_0 \) column-wise from 63 to 4.

In a second step, \( C_n \) and \( D_n \) for \( n = 1, \ldots, 16 \), are each generated from \( C_{n-1} \) and \( D_{n-1} \) by a cyclic left-shift of \( s_n \) positions, where \( s_n \) is defined by:

\[ s_n = \begin{cases} 1, & \text{if } n \in \{1, 2, 9, 16\} \\ 2, & \text{otherwise} \end{cases} \]

From each of these \((C_n, D_n)\), with \( n = 1, \ldots, 16 \), one now selects 48 key bits as in the above table PC2 on the right to obtain \( K_n \).

In the following, a particular pair of keys for DES is considered\(^1\):

\[ K_0 = (\text{01FE 01FE 01FE 01FE}), \quad \hat{K}_0 = (\text{FE01 FE01 FE01 FE01}) \]

\(^1\)The keys are shown in hexadecimal representation.
b) Determine \((C_0, D_0)\) and \((C_1, D_1)\) from \(K_0\), and \((\tilde{C}_0, \tilde{D}_0)\) and \((\tilde{C}_1, \tilde{D}_1)\) from \(\tilde{K}_0\).

c) Which of the generated subkeys \(K_1, K_2, ..., K_{16}\) are identical when \(K_0\) is used?

d) Show that \(\text{DES}_{K_0}(\text{DES}_{K_0}(M)) = M\) holds for all \(M \in \mathcal{M}\).

**Problem 2.** (DES Complementation property) Let \(M\) be a block of bits of length 64 and let \(K\) be a block of bits of length 56. Let \(\text{DES}(M, K)\) denote the encryption of \(M\) with key \(K\) using the DES cryptosystem. \(\overline{x}\) denotes the bitwise complement of a block \(x\).

a) Show that the complementation property holds:

\[
\text{DES}(M, K) = \overline{\text{DES}(\overline{M}, \overline{K})}
\]

b) How does the complementation property help to attack DES?

**Problem 3.** (weak DES keys) There are four so called weak DES keys. One of those keys is

\[
K = 00011111 \ 00011111 \ 00011111 \ 00011111 \ 00001110 \ 00001110 \ 00001110 \ 00001110.
\]

a) What happens if you use this key?

b) Can you find the other three weak keys?