Sample problems

1. (Playfair cipher) Decrypt the ciphertext

   OPNBNMDFLYNBDLCDXIWENMCRYDNIONP

   if the keyword is DECRYPTION.

   Solution.

   The 5x5 matrix has the following view:

   \[
   \begin{array}{ccccc}
   D & E & C & R & Y \\
   P & T & I/J & O & N \\
   A & B & F & G & H \\
   K & L & M & Q & S \\
   U & V & W & X & Z \\
   \end{array}
   \]

   Repeatedly applying the three rules the given ciphertext can be decrypted in the following way:

   Ciphertext:  OPNBNMDFLYNBDLCDXIWENMCRYDNIONP
   Plaintext:  inthiscasethekeywordisdecryption

2. (Hill cipher) Encrypt the plaintext PLAINTEXT with the key

   \[
   K = \begin{pmatrix}
   5 & 1 & 6 \\
   4 & 9 & 8 \\
   3 & 10 & 12 \\
   \end{pmatrix}
   \]

   Solution.

   \[
   \begin{align*}
   C_1 &= (5p_1 + 1p_2 + 6p_3) \mod 26 \\
   C_2 &= (4p_1 + 9p_2 + 8p_3) \mod 26 \\
   C_3 &= (3p_1 + 10p_2 + 12p_3) \mod 26
   \end{align*}
   \]

   By substituting \( p_1=15, \ p_2=11, \ p_3=0, \ p_4=8, \ p_5=13, \ p_6=p_7=19, \ p_8=4, \) and \( p_9=23, \) we obtain

   \[
   \begin{pmatrix}
   C_1 \\
   C_2 \\
   C_3 \\
   \end{pmatrix} = \begin{pmatrix}
   5 & 1 & 6 & \mid & 15 \\
   4 & 9 & 8 & \mid & 11 \\
   3 & 10 & 12 & \mid & 0 \\
   \end{pmatrix}
   \]

   Thus,
$C_1= 5 \times 15 + 1 \times 11 + 6 \times 0 = 75 + 11 + 0 = 86 \mod 26 = 8 = I,$
$C_2= 4 \times 15 + 9 \times 11 + 8 \times 0 = 60 + 99 + 0 = 159 \mod 26 = 3 = D,$
$C_3= 3 \times 15 + 10 \times 11 + 12 \times 0 = 45 + 110 + 0 = 155 \mod 26 = 25 = Z.$

Similarly,

\[
\begin{pmatrix}
C_4 \\
C_5 \\
C_6
\end{pmatrix} = \begin{pmatrix}
5 & 1 & 6 \\
4 & 9 & 8 \\
3 & 10 & 12
\end{pmatrix}
\begin{pmatrix}
8 \\
13 \\
19
\end{pmatrix}
\]

or

$C_4= 5 \times 8 + 1 \times 13 + 6 \times 19 = 40 + 13 + 114 = 167 \mod 26 = 5 = F,$
$C_5= 4 \times 8 + 9 \times 13 + 8 \times 19 = 48 + 117 + 162 = 327 \mod 26 = 15 = P,$
$C_6= 3 \times 8 + 10 \times 13 + 12 \times 19 = 24 + 130 + 228 = 382 \mod 26 = 18 = S.$

Finally,

\[
\begin{pmatrix}
C_7 \\
C_8 \\
C_9
\end{pmatrix} = \begin{pmatrix}
5 & 1 & 6 \\
4 & 9 & 8 \\
3 & 10 & 12
\end{pmatrix}
\begin{pmatrix}
4 \\
23 \\
19
\end{pmatrix}
\]

or

$C_7= 5 \times 4 + 1 \times 23 + 6 \times 19 = 20 + 23 + 114 = 157 \mod 26 = 20 = U,$
$C_8= 4 \times 4 + 9 \times 23 + 8 \times 19 = 16 + 207 + 162 = 385 \mod 26 = 25 = Z,$
$C_9= 3 \times 4 + 10 \times 23 + 12 \times 19 = 12 + 230 + 228 = 470 \mod 26 = 18 = C.$

The plaintext encrypted results IDZFPSUZC.

3. Suppose that we are using a Vigenere scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the given message. Given the ciphertext
find the key that yields the following plaintext:

MR MUSTARD WITH THE CANDLESTICK IN THE HALL

Solution.

As we know the key letter and plaintext letter identify the row, and the column, respectively. Hence, if the ciphertext and plaintext letters are given, the key letter can be found easily. As it follows from the above table the key used to encrypt the plaintext

MR MUSTARD WITH THE CANDLESTICK IN THE HALL

is

MISS SCARLET WITH THE KNIFE IN THE SHOWROOM

4. (Rail fence technique) Use rail fence technique to decrypt the following message

ESENEIERNANUIATRMDTRAENNVRIY

Solution.

In the rail fence technique, the plaintext is written down as a sequence of diagonals and then read off as a
sequence of rows. Implementing this technique to the given ciphertext will result

{EASTERNMEDITERRANEAN UNIVERSITY}

That is, the plaintext is EASTERNMEDITERRANEAN UNIVERSITY

5. Given ciphertext IYRMVLNSTLAEDTRSCCEEIGIYSANLSII and the key 3 6 1 2 5 4, use transposition technique based on writing the message in a rectangle, row by row, and reading the message off, column by column, with permuting the order of columns to decrypt it.

Solution.

We first split the given ciphertext in six blocks, then write the blocks column-wise according to the given key, then read the message in. As a result we obtain the following table.

<table>
<thead>
<tr>
<th>3 6 1 2 5 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A S I N G L</td>
</tr>
<tr>
<td>E C Y L I N</td>
</tr>
<tr>
<td>D E R S Y S</td>
</tr>
<tr>
<td>T E M I S T</td>
</tr>
<tr>
<td>R I V I A L</td>
</tr>
</tbody>
</table>

Hence, the message is ASINGLECYLINDERSYSTEMISTRIVIAL.

6. (S-DES) Using S-DES, decrypt the string 10100010 using the key 011111101 by hand. Show intermediate results after each function ($IP$, $F_k$, $SW$, $F_k$, $IP^{-1}$). Then decode the first 4 bits of the plaintext string and ciphertext string to a letters and the second 4 bits to another letters where we encode A through P in base 2 (i.e. A=0000, B=0001, ..., P=1111).

Solution.

<table>
<thead>
<tr>
<th>S-DES Key Generation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-bit key : 0111111101</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>P10</td>
<td>0111111101</td>
<td>1111110011</td>
</tr>
<tr>
<td>LS-1</td>
<td>11111 10011</td>
<td>11111 00111</td>
</tr>
<tr>
<td>P8</td>
<td>1111100111</td>
<td>01011111 (K₁)</td>
</tr>
</tbody>
</table>
S-DES Encryption

8-bit plaintext : 10100010 (KC)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>10100010</td>
<td>00110001</td>
</tr>
<tr>
<td>E/P</td>
<td>0001</td>
<td>10000010</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>10000010, K&lt;sub&gt;1&lt;/sub&gt;</td>
<td>11011101</td>
</tr>
<tr>
<td>S0</td>
<td>1101</td>
<td>11</td>
</tr>
<tr>
<td>S1</td>
<td>1101</td>
<td>00</td>
</tr>
<tr>
<td>P4</td>
<td>1100</td>
<td>1001</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>1001, 0011</td>
<td>1010</td>
</tr>
<tr>
<td>SW</td>
<td>10100001</td>
<td>00011001</td>
</tr>
<tr>
<td>E/P</td>
<td>1010</td>
<td>01010101</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>01010101, K&lt;sub&gt;2&lt;/sub&gt;</td>
<td>10101001</td>
</tr>
<tr>
<td>S0</td>
<td>1010</td>
<td>10</td>
</tr>
<tr>
<td>S1</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>P4</td>
<td>1010</td>
<td>0011</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>0001,0011</td>
<td>0010</td>
</tr>
<tr>
<td>IP&lt;sup&gt;-1&lt;/sup&gt;</td>
<td>00101010</td>
<td>00111000</td>
</tr>
</tbody>
</table>

8-bit ciphertext : 00111000

S-DES Decryption

8-bit ciphertext : 00111000 (DH)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>00111000</td>
<td>00101010</td>
</tr>
<tr>
<td>E/P</td>
<td>1010</td>
<td>01010101</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>01010101, K&lt;sub&gt;2&lt;/sub&gt;</td>
<td>10101001</td>
</tr>
<tr>
<td>S0</td>
<td>1010</td>
<td>10</td>
</tr>
<tr>
<td>S1</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>P4</td>
<td>1010</td>
<td>0011</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>0010,0011</td>
<td>0001</td>
</tr>
<tr>
<td>SW</td>
<td>00011010</td>
<td>10100001</td>
</tr>
<tr>
<td>E/P</td>
<td>0001</td>
<td>10000010</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>10000010, K&lt;sub&gt;1&lt;/sub&gt;</td>
<td>11011101</td>
</tr>
<tr>
<td>S0</td>
<td>1101</td>
<td>11</td>
</tr>
<tr>
<td>S1</td>
<td>1101</td>
<td>00</td>
</tr>
<tr>
<td>P4</td>
<td>1100</td>
<td>1001</td>
</tr>
<tr>
<td>Excusive-OR</td>
<td>1010,1001</td>
<td>0011</td>
</tr>
<tr>
<td>IP&lt;sup&gt;-1&lt;/sup&gt;</td>
<td>00110001</td>
<td>10100010</td>
</tr>
</tbody>
</table>

8-bit plaintext : 10100010