Exercise
Algorithmic Cryptography
Sheet 1

- Write the name, group number and enrollment number of each group member on every sheet that you hand in.
- To achieve the permission for the exam you must earn 50% of the sum of all points and present one of your solutions at least once.
- You can earn 50% bonus points by presenting your solution. At the beginning of every exercise session, you can mark the exercises that you want to present.
- If a student is not able to present a correct solution although he/she marked the exercise as presentable, he/she will lose all of his/her points on the exercise sheet.

Exercise 1.1 (4 points)
Decrypt the following ciphertext and explain your approach.

ABCCD BEAFF GHIJK LGFJC MFJCF IKEGH IJKDK NGEFF KAIOC PIQCH KDBKQ DJIGP IKKHR GHSIK FHCPI JKAFI AHDLO HCPIJ RAGHL PAHTJ FKNKH IJEGR LKAFI FGDKF JCCIO PCRij KEKOI KQKCO IJKDK AIJFJ KADAL KKEGH KOPCR IJKIP KKIJP CSBIJ JKJFC IOGOI QOKKI CSIKD BAPAE EAHMC KIJKB CEDLS B

Hint: The text is in English and the letters appear with the following frequency:

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>15</td>
<td>7</td>
<td>18</td>
<td>10</td>
<td>9</td>
<td>16</td>
<td>11</td>
<td>14</td>
<td>27</td>
<td>20</td>
<td>36</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>2</td>
<td>8</td>
<td>11</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Exercise 1.2 (4 points)
Prove: If in DES each bit in the plaintext and in the key is replaced by its complement, then each bit in the ciphertext is also replaced by its complement.

Exercise 1.3 (4 points)
Consider the keys $K_1, K_2, \ldots, K_{16}$ used in DES in the function $f(R_{i-1}, K_i)$. Let $K'_1, K'_2, \ldots, K'_{16}$ be these keys in reverse order, i.e., $K'_1 = K_{16}, K'_2 = K_{15}, \ldots, K'_{16} = K_1$.
What happens if DES uses the keys $K'_i$ instead of the standard keys $K_i$ and what is the relation between the plain- and ciphertext of the standard and this modified DES?
Exercise 1.4

Compare encryption and decryption of DES if the key

11100000 11100000 11100000 11100000 11110001 11110001 11110001 11110001

is used.

Deadline: Thursday, October 26, 2017, 10:15 a.m.,
in the lecture or in the box in front of the i1.