2. Exercise sheet (15.11.2006)
Hand in solutions to the homework exercises
on Wednesday, November 29th, in the tutorial/the lecture.

Exercise 2.1 (Repetition: Euler’s \( \varphi \) function).

Let \( p \in \mathbb{N} \) be a prime number and \( m, n \in \mathbb{N}_{\geq 2} \). Euler’s \( \varphi \) function is defined by
\[
\varphi : \mathbb{N}_{\geq 2} \to \mathbb{N}, n \mapsto \# \{ k \in \mathbb{Z}_n \mid \gcd(k, n) = 1 \}.
\]
Give proofs for the following formulae:

(i) \( \varphi(p) = p - 1 \),
(ii) \( \varphi(p^e) = p^{e-1}(p - 1) \) for all \( e \in \mathbb{N}_{\geq 1} \),
(iii) \( \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \), if \( \gcd(m, n) = 1 \).

Exercise 2.2 (Combining encryption algorithms).

Assume you define the Doubled Caesar cipher by the following encryption function, where \( \alpha, \beta \) are chosen from \( \mathbb{Z}_{26} \) and the function \( \xi \) is the Caesar cipher defined in exercise 1.3:
\[
\xi^{(2)}_{\alpha,\beta} : \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto \xi_{\beta}(\xi_{\alpha}(x)).
\]

(i) Show that this cipher is as (in)secure as the Caesar cipher.
(ii) Discuss the reasons why the combination of these two ciphers doesn’t give you more security.

Hint: The set \( \{ \xi_{\alpha} \mid \alpha \in \mathbb{Z}_{26} \} \) forms a group with respect to composition!

Exercise 2.3 (Affine Codes in higher dimensions).

Consider the affine cipher over \( \mathbb{Z}_{26} \) with \( m = 3 \). Suppose you know that the plaintext

\[
\text{ADISPLAYEDEQUATION}
\]

was encrypted to give the ciphertext

\[
\text{DSRMSIOPXLJBZULLM}
\]

Determine the key.
Exercise 2.4 (Homework: Linear Algebra).  
Compute the determinant and the inverse of the following matrix $A$ over $\mathbb{Z}_{26}$.

**Hint:** We are computer scientists...

$$ A := \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix} $$

Exercise 2.5 (Homework: Combinatorics).  
Let be $n \in \mathbb{N}$.

(i) Determine the number of permutations of a set $M$ with $n$ elements. Show that the set $S(M)$ of all permutations of $M$ forms a group with respect to composition.

(ii) Determine the number of possible bitstrings of length $n$.

(iii) Determine the number of strings of length $n$ over an alphabet $\Sigma$ that do not change if they are reversed.

Exercise 2.6 (Homework: Substitution Cipher).  
The following table gives the frequency distribution of the 26 letters in typical English texts:

<table>
<thead>
<tr>
<th>letter</th>
<th>probability</th>
<th>letter</th>
<th>probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.082</td>
<td>N</td>
<td>0.067</td>
</tr>
<tr>
<td>B</td>
<td>0.015</td>
<td>O</td>
<td>0.075</td>
</tr>
<tr>
<td>C</td>
<td>0.028</td>
<td>P</td>
<td>0.019</td>
</tr>
<tr>
<td>D</td>
<td>0.043</td>
<td>Q</td>
<td>0.001</td>
</tr>
<tr>
<td>E</td>
<td>0.127</td>
<td>R</td>
<td>0.060</td>
</tr>
<tr>
<td>F</td>
<td>0.022</td>
<td>S</td>
<td>0.063</td>
</tr>
<tr>
<td>G</td>
<td>0.020</td>
<td>T</td>
<td>0.091</td>
</tr>
<tr>
<td>H</td>
<td>0.061</td>
<td>U</td>
<td>0.028</td>
</tr>
<tr>
<td>I</td>
<td>0.070</td>
<td>V</td>
<td>0.010</td>
</tr>
<tr>
<td>J</td>
<td>0.002</td>
<td>W</td>
<td>0.023</td>
</tr>
<tr>
<td>K</td>
<td>0.008</td>
<td>X</td>
<td>0.001</td>
</tr>
<tr>
<td>L</td>
<td>0.040</td>
<td>Y</td>
<td>0.002</td>
</tr>
<tr>
<td>M</td>
<td>0.024</td>
<td>Z</td>
<td>0.001</td>
</tr>
</tbody>
</table>
Suppose you know that the plaintext of the following ciphertext, taken from “The Diary of Samuel Marchbanks” by R. Davies and C. Irwin, was encrypted using a substitution cipher (i.e. the improved variant of Caesar’s cipher). You can find this text on the tutorial’s webpage.

EMGLOSUDCGNDNCUSWYSFHNSFCTKDPUMWLWGYICOXYSIPJCK
QPKUGKMOLICGACKSNIAKCYKZSCXECJCKSHYXSCGOIDPKZCNKSHICGIWYGKGGOLDSILKG0US1USIGLEDSPWZUGFZCMDGYYSFUSZCNE0JNCGYEOUEUPXE2GACGFGLKNSACIG0IYCKXCJUCIUZCFZCCNGYYSFEUKEKUZCSOCF2ZCCNCIACZEJNCSFZEJ2EGMXCYHCJUMGKUCY

Find the plaintext!
**Hint:** F decrypts to W.

**Exercise 2.7** (Homework: Combining encryption algorithms). (5 points)

Assume you encrypt a text using first the Vigenère cipher followed by an application of the Caesar cipher. Discuss whether the resulting encryption algorithm is more secure than the Caesar/the Vigenère cipher.