Cryptography, winter 2006

PROF. DR. WERNER SCHINDLER, DIPL.-INF. DANIEL LOEBENBERGER

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 φ function).

Let $p \in \mathbb{N}$ be a prime number and $m, n \in \mathbb{N}_{\geq 2}$. Euler's φ function is defined by

$$\varphi\colon \mathbb{N}_{\geq 2} \to \mathbb{N}, n \mapsto \#\{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}.$$

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 α, β are chosen from $\mathbb{Z}_{26}$ and the function ξ is the Caesar cipher defined in exercise 1.3:*

$$\xi^{(2)}_{\alpha,\beta}\colon \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto \xi_\beta(\xi_\alpha(x)).$$

(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

`ADISPLAYEDEQUATION`

was encrypted to give the ciphertext

`DSRMSIOPLXLJBZULLM`

Determine the key.

Exercise 2.4 (Homework: Linear Algebra). (2 points)

2 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). (8 points)

Let be $n \in \mathbb{N}$.

4 (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.

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

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

Exercise 2.6 (Homework: Substitution Cipher). (5 points)

5 The following table gives the frequency distribution of the 26 letters in typical English texts:

letter	probability	letter	probability
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.002
M	0.024	Z	0.001

Suppose you know that the plaintext of the following ciphertext, taken from "The Diary of Samuel Marchbanks" by. R. Davies and C. Irwin, was encrpyted using a substitution cipher (i.e. the improved variant of Caesar's cipher). You can find this text on the tutorial's webpage.

```
 EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
OIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
GFZCCMDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
       IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
```

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. 5