Cryptography, winter 2006

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

1. Exercise sheet (08.11.2006)
Hand in solutions to the homework exercises on Wednesday, November 22nd, in the lecture.

During this exercise sheet will identify the 26 letters A, B,..., Z with elements in $\mathbb{Z}_{26}$, namely 0 (for A), 1 (for B), through 25 (for Z).

Exercise 1.1 (Repetition: Properties of the gcd).

Show that the following two statements are equivalent for $a, b, d \in \mathbb{Z}$:

(i) *There exist $s, t \in \mathbb{Z}$ so that holds: $as + bt = d$.*

(ii) *d is divisible by* $\gcd(a, b)$.

Exercise 1.2 (Repetition: Modular Arithmetic).

Recall that for $n \in \mathbb{N}$ the ring $\mathbb{Z}_n$ is the set $\{0, \ldots, n-1\}$ equipped with addition and multiplication mod n.

(i) *Compute* $1024 \bmod 26$, $-1024 \bmod 26$, $26 \bmod 1024$ *and* $-26 \bmod 1024$.

(ii) *Compute* $18 \cdot 17 \bmod 19$ *and* $5 \cdot 23 \cdot 20 \bmod 21$.

(iii) *Let $0 \neq a \in \mathbb{Z}_n$. Show that there exists $0 \neq b \in \mathbb{Z}_n$ such that $a \cdot b = 1 \pmod{n}$ if and only if* $\gcd(a, n) = 1$.

Exercise 1.3 (Caesar cipher).

A Caesar cipher *is given by the following encryption function, where α is chosen from $\mathbb{Z}_{26}$:*

$$\xi_\alpha : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto x + \alpha \bmod 26.$$

(i) *Encrypt the message "THEANSWERISFORTYTWO" using the Caesar cipher ξ_7.*

(ii) *Define the decryption function of the Caesar cipher. Decrypt the message "ROXAPXCCQNZDNBCRXW".*

(iii) *If an encryption function using a key α is identical to the decryption function, then the key α is called an* involutory key. *Find all involutory keys of the Caesar cipher over $\mathbb{Z}_{26}$.*

Exercise 1.4 (Homework: Cryptool). (5 points)

Suppose you want to encrypt the following message, taken from "The War of the Worlds" by H. G. Wells, using the Caesar cipher ξ_5 defined in Exercise 1.3. Blanks and special characters are not encrypted.

```
No one would have believed in the last years of the
nineteenth century that this world was being watched
keenly and closely by intelligences greater than man's
and yet as mortal as his own; that as men busied
themselves about their various concerns they were
scrutinised and studied, perhaps almost as narrowly as a
man with a microscope might scrutinise the transient
creatures that swarm and multiply in a drop of water.
With infinite complacency men went to and fro over this
globe about their little affairs, serene in their
assurance of their empire over matter.
```

3 (i) Download cryptool from `http://www.cryptool.de/` and install it on your computer.
Find the MD5 sum of the file `SetupCrypTool_1_4_00_en.exe`. Hand in this hash-value.

2 (ii) Perform the encryption using cryptool. You can find the above plaintext on the tutorials webpage. Hand in the encrypted text.

Exercise 1.5 (Homework: Vigenère Cipher). (7 points)

An improvement of the Caesar cipher is the so called *Vigenère cipher*. Here you use a *keyword* $K := (k_0, \ldots, k_\ell) \in \mathbb{Z}_{26}^\ell$ to encrypt a message $M := (m_0, \ldots, m_\ell) \in \mathbb{Z}_{26}^\ell$ in the following way:

$$\nu : \mathbb{Z}_{26}^\ell \to \mathbb{Z}_{26}^\ell, (m_0, \ldots, m_\ell) \mapsto (m_0 + k_0 \bmod 26, \ldots, m_\ell + k_\ell \bmod 26)$$

We give an example: Suppose $\ell = 6$ and the keyword is `CIPHER`. This corresponds to the numerical equivalent $K = (2, 8, 15, 7, 4, 17)$. Suppose the plaintext is the string

`CRYPTOSYSTEMS`

We convert the plaintext elements to residues modulo 26, write them in groups of six, and the "add" the keyword modulo 26, as follows

2	17	24	15	19	14	18	24	18	19	4	12	18
2	8	15	7	4	17	2	8	15	7	4	17	2
4	25	13	22	23	5	20	6	7	0	8	3	20

The alphabetic ciphertext would thus be `EZNWXFUGHAIDU`.

(i) Suppose now you know that the following text, taken from "The Hitchhiker's Guide to the Galaxy" by D. Adams, was encrypted using a Vigenère cipher, where blanks and special characters were not encrypted. You can find this text on the tutorials webpage. Use cryptool to find the plaintext. [2]

```
Lizg lghlhh zbm esue br Exnpxv.  "Cbiw my cb?" dwqyl
Dvzbcu.  "Xny Plxibplokl'a Jyoxm ws zbm Jerufb.  Mz'm
 i vsxn wi irykwvuhqf fuis.  Lx zytow eic hzklgwloho
  bsa hmhh zi sqsc ujryz uvbxncvj.  Xnub'v mzm rrf."
   Glbkyx ncurkx qw sbyz qixpwxwrs qq lom pdrjm.  "Q
   omqy bki iidhv," ny admj.  "Xwq'x Vuvlg.  On'a wlk
zquwz bmotlot rv ohbhprcolfry bkmta iqchilb'w yuqg xu
gm dpr xib." "M'rf aksc swx luq qw aulsv," wgcl Isxx.
 Ph wtubflkx qw jxiu Dvzbcu ani edw ynqop nitgmta qw
 ey cn lx cua d xci-ehiq-xmdh ruzn etx xxpryl lx uob
  rj ona fsbyz.  "Bsa jzhwy nplw hobwst bmui eic vik
   uvg xny afvkyv ommbbv yv aqymta gry zbm lrjyf." D
     wilmhr, gvwxx zbzhi ohkkiy vg isal, tlx aj iqh
ibiueinmuw hyodr zi nomiemu eilwvw zbm vyxzifi.  "Eic
 zetn br otie dfuob Ysmivv, wu C mqxkl bkez hipi yi."
  Plw lcvjixm bdtvyl vssy urvk embw.  "Ghl wlklm zi
  glm." Wlk qwuhy Pwjst Wwqwzlcfxul Noikna ipglmg mt
  azhit ukusym bki ywzhit.  Zwuh vlmvwkx i oexam uij
vcwxuh iw xny jrxziu rj zbm vgxymq etx ervjm jhkgh br
ytxcoezy ifvuma lx.  Gn bki yuuh xogm, wlk vwro hyodr
 zi asige bki khbuc gm ehpr cv d wzcto uacmw qkuaxvkx
          drmiy.  Bkmy ca zlgn bki hiwn wgcl.?
```

(ii) Describe how cryptool managed to decrypt the text. [5]

Exercise 1.6 (Homework: Affine Codes). (8 points)

An *affine Code* (also called substitution cipher) is given by the following encryption function, where α, β are chosen from $\mathbb{Z}_{26}$:

$$\varphi_{\alpha,\beta}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto \alpha x + \beta \bmod 26.$$

(i) Encrypt the (plaintext) word CRYPTOGRAPHY using the affine code $\varphi_{3,5}$. Name the decryption function corresponding to $\varphi_{3,5}$ and decrypt the (cipher text) word XRHLAFUUK. [2]

(ii) A central rule of cryptography states that "the plaintext must be computable from the key and the cipher text!" Explain why $\varphi_{2,3}$ violates this rule. Show that the function $\varphi_{\alpha,\beta}$ satisfies the rule if and only if $\gcd(\alpha, 26) = 1$ holds, i.e. if α and 26 have no common divisor. [4]

(iii) In the following we consider only functions $\varphi_{\alpha,\beta}$ with $\gcd(\alpha, 26) = 1$. Show that all affine codes with $\beta = 0$ map the letter A to A and the letter N to N. [2]