Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

2. Exercise sheet
Hand in solutions until Monday, 10 November 2008.

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).

Reminders.

- Have you registered an account for the b-it?
- Exercise 1.2 cannot be completed without coming to the first tutorial.

Exercise 2.1 (SMTP and mail format). (10 points)

(i) Look up the RFCs for SMTP and ESMTP, and describe briefly the major differences. [4]

(ii) Consider the virus warning "`[SotI: <your name>] Virus warning`" that was sent to you on Tuesday, 4 November, at about 14:39 or 15:10. (You might have to retrieve it from your spam folder...)

(a) Find out how to display the source code and copy the first ten lines or so. [1]

(b) Which parts are suspicious, which are not? [2]

(c) Which actions are appropriate in reaction to such a mail? [1]

(d) How do you know whether the warning is true? [1]

(e) What is the damage caused by it? [1]

Exercise 2.2 (Repetition: Modular Arithmetic). (2 points)

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 $-26 \bmod 1024$. [1]

(ii) Compute $18 \cdot 17 \bmod 19$ and $5 \cdot 23 \cdot 20 \bmod 21$. [1]

Exercise 2.3 (Caesar cipher). (5 points)

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

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

[2] (i) Encrypt the message "THEANSWERISFORTYTWO" using the Caesar cipher ζ_7.

[2] (ii) Define the decryption function of the Caesar cipher. Decrypt the message "ROXAPXCCQNZDNBCRXW".

[1] (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 2.4 (Affine Codes). (8 points)

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

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

[2] (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.

[4] (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.

[2] (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.

Exercise 2.5 (Cryptool). (4 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 2.3. 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.
```

(i) Download cryptool from `http://www.cryptool.de/` and install it on your computer.

(ii) Perform the encryption using cryptool. You can find the above plaintext on the tutorials webpage. Hand in the encrypted text. 4