Information Security
Assignment 1

Jeewon Heo (s3766861) & Lubar Budaj (s4167376) & Matteo Wohlrapp (s4974921)

September 27, 2021

Exercise 1

In this exercise we familiarize with the acceptable use policy of the University of Groningen which can be found here.

0.0.1. Responsibilities

In general, system managers and 'ordinary' users have the same rights and duties. However, due to the system managers status, they need to fulfill additional security requirements. These include the following:

- Responsibility for the system itself, including accountability for installation and maintenance of software.
- System managers do not analyze content on RUGnet, because they are considered confidential and only have authority to do so in situations of abuse.
- Particular circumstances require the system manager to forward information for security scans or solving software issues.

0.0.2. Ground-rule

Since the computers are shared facilities with many of them being multi user systems, the most important ground-rule can be expressed as: "the users of the university computer systems may not endanger these systems, nor may they hinder other users."

0.0.3. Advice for 'RUGnet' users

To guarantee a trouble-free usage of the facilities, obtaining the following advice concerning access information security is crucial:

- Do not login with your password when you are observed.
- Do not share login information with other users.
- Choose a secure password which contains upper- and lowercase letters as well as special characters and numbers.
- Change your password from time to time.

0.0.4. Prohibited Actions

Examples for prohibited actions:

- Removing hard- or software or modifying them in any way.
- Violating copyright licenses by, e.g. copying software.
- Accessing and distributing content on the network without permission and sharing it.
- Sharing discriminating, violent, aggressive and threatening information or messages over the network.

0.0.5. Sanctions

If the suspect can be identified, the following sanctions can be pronounced. The board of the responsible faculty gets notified about the suspected abuse and furthermore the access rights of the suspect can be restricted or completely suspended.

0.0.6. Challenge sanctions

To challenge the situation, the individual can file an objection against the sanctions with the chair of the responsible faculty.

Exercise 3

0.1. 1

A substitution cipher that uses shifting has only 26 possibilities. Any number of shifts n, that is larger than 26, will result in same alphabet as moving $n\%26$ shifts. On the other hand, a substitution cipher that uses mixed alphabets, i.e. permuted alphabets, will have 26! keyspace, which is approximately 2^{88} possibilities.

0.2. 2

Applying a significant number of consecutive simple substitution cipher encryptions/decryptions with a mixed or shifted alphabet does not make it harder to break the original plaintext. The keyspace of substitution cipher using mixed alphabets contains the alphabet that can be obtained using any number of encryptions/decryptions using shifts and permutations. In other words, regardless of the number of consecutive encryptions/decryptions using mixed or shifted alphabets, the resulting alphabet (key) is one of the 26! possibilities that can be obtained by applying permutation just once.

0.3. 3

The encryption function of the substitution cipher also be used for decryption. Encryption and decryption shift the alphabet to the opposite directions. Other than this difference in direction, the rest of the algorithm remain the same for the both. We can consider decrypting with shift of n as encrypting with shift of $-n$. For instance, encrypting `a (at 0)` by shift of $n = 1$ gives us `b (at 1)`, while decrypting `a` by shift of 1 gives us `z (at 25 = -1 % 26)`. Thus, we can use the same function for encryption and decryption if we modify the shift parameter n, accordingly (pass in $-n$ for decryption).