Report Exercise 1

https://www.rug.nl/society-business/centre-for-information-technology/security/aup/?lang=en

1. What (if any) are the differences between the responsibilities of 'ordinary' users and systems managers? Do systems managers have special privileges and responsibilities (if so, what are they)?

> Systems managers have the same rights and duties as other users of the university computer systems. However, the sensitive nature of their positions naturally leads to additional security related requirements.

Responsibilities of ordinary users:

> Users of the university computer systems should realize they are not > the only users of these computers. Many computers are multi-user > systems, and the users of these computers belong to a community. > Therefore, the ground-rule on which this AUP is based is similar to > the ground-rule on which traffic is based: the users of the > university computer systems may not endanger these systems, nor may > they hinder other users.
>
> Some implications of this ground-rule are that users are not allowed > to send unsolicited email or try to obtain or use other users' > passwords; neither occasionally, nor `for fun'.
>
> Privacy of accounts:
>
> Access to university computer systems is only granted to > individuals. Using other people's accounts or access-rights will > result in the discontinuation of one's account.
>
> Any unauthorized use of an account should be reported immediately to > the security manager of the Center of Information Technology.
>
> Copying software:
>
> Software made available on the university computer systems may be > used subject to applicable licenses and copyrights. Any software > stored on the university computer systems may not be copied for use > elsewhere, unless explicit and written permission was granted by > proper authorities. Conversely, using illegally obtained software is > not allowed on university computer systems.
>
> Using the university computer systems:
>
> Using the university computer systems, including hardware, software > and computer network facilities is only allowed in accordance with the > nature of the provided account. Any use of the university computer > systems is always restricted to research or education. Any > commercial use of the university computer systems is not allowed, > unless explicit and written permission was granted by proper > authorities.
>
> Access information security:

> By obtaining access information (e.g., usernames, passwords) third > parties may gain access to the university computer systems. Even in > this case the registered user of an account is liable for any access > or abuse of the university computer systems. In order to minimize > the probability that unauthorized parties obtain your password, adhere to the following rules of thumb:
>
> ```
> Keep your access information secret: don't hand this information >
> over to friends or acquaintances.
> Don't type your  password when somebody watches you type.
> Change your password every now and then. Opinions differ about > the
> optimal interval for password changes, but everyone working > in the
> field of security advocates to change passwords every > once in a
> while. Changing ones
> password very often isn't necessary, but a password should be >
> changed at least once a year.
> Do not use personal data about yourself, your friends or > relatives
> when constructing your password.
> Do not use existing words or abbreviations (like rcrug of ppsw).
> Use lower- as well as uppercase letters, use digits and > punctuation
> characters when constructing your password.
> Some examples of hard to guess, but easy to remember passwords >
> (well, up to now, as they are now listed in this document):
>            o  1irC&D `it is raining cats and dogs'.
>            o  6^twT.  `barking up the wrong > tree'.
> ```
>
> Report holes in security:
>
> All multi-user systems are vulnerable to security breaches. If you > find a flaw in a system's security setup you should report this to > the security manager. It is not allowed to exploit the discovered > weakness in the security setup of university computer systems. By > informing the security manager of any weakness you have found, you > effectively help to optimize the reliability of the university > computer systems, while preventing misunderstandings at the same > time (do you exhibit intellectual curiosity or are you purposely > exploiting a security hole?)
>
> Using games:
>
> On various university computer systems games were made available. > Enjoy them in a responsible way. If you notice that somebody is > waiting for your terminal it is very impolite to keep using your > terminal for playing games. Terminate your session without being > asked, and let others use your terminal. Prevent the situation that > the other person has to ask you to leave your terminal.

Summarized:

- Privacy of accounts: "Using other people's accounts or access-rights will result in the discontinuation of one's account."
- Copying software: You are not allowed to copy software from university computers elsewhere. Running illegally obtained software on the university computer system is also forbidden.
- Using the university computer systems: The university computer systems may only be used for research or education (unless explicit written permission has been granted).

- Access information security: Use strong passwords (no personal data, no common phrases or words, should be hard to guess). Don't share passwords with friends/acquaintances. Don't type the password when someone is watching. Change the password every now and then.
- Report holes in security: Security vulnerabilities must be reported to the security manager.
- Using games: While there are games on varios university computer systems, don't play use them while other people are waiting for the terminal.

Special privileges and responsibilities of systems managers (in addition to the normal user responsibilities):

> Systems managers have the same rights and duties as other users of the university computer systems. However, the sensitive nature of their positions naturally leads to additional security related requirements.
>
> - Systems managers should ensure that the users of their systems have access to the software and hardware they require for their normal work at the university. Requests for the installation of software should always be considered conditional to the assigned nature of the particular university computer systems. E.g., a systems manager of a computer not intended to serve up webpages cannot rightfully be asked to install a webserver on that particular computer.
> - The systems manager is responsible for the security of the system > itself, and will take care of, in cooperation with the security > manager, the installation and maintenance of the required and > available software.
> - In order to uphold and maintain the integrity of `RUGnet' in- and > outbound traffic is constantly monitored. All information about this > traffic is using automatic means.
> - All information collected to analyze in- and outbound traffic is > destroyed after at most six months except in cases where a legal > obligation exists to retain the information for a longer period. In > those cases the University of Groningen applies the legally > acceptable minimum storage period.
> - All information obtained about in- and outboud traffic is also > analyzed using automated means and is aimed at the analysis of > malware like viruses, trojan horses and worms.
> - Except for the exceptional situation described below (abuse of an > account) systems managers will not perform any content-analysis of > the information within RUGnet.
> - The systems manager will consider any information about the > system, as well as any information stored in the system as > confidential.
> - In special situations the systems manager can be required to > submit specific information (data, software) for further > investigation, in order to solve any problems that were encountered > while using the data or software. These requirements may involve > security scans. Such scans are only performed subsequent to an > authenticated request made by the relevant department or user of the > system(s) involved.

Summarized:

- SM (system managers) must ensure that users have access to necessary software and hardware.
- Installation of software should align with the system's intended purpose
- SM are responsible for system security and software installation. Inbound and outbound traffic on 'RUGnet' is monitored and retained for a maximum of 6 months.
- Collected traffic information is analyzed for malware like viruses, trojans, and worms.
- Content analysis within 'RUGnet' is not performed by SM except in cases of abuse.

- Any information about the system, as well as any information stored in the system is considered confidential.
- Systems managers can be required to submit specific information (data, software) for further investigation, to solve problems that were encountered related to the data or software.
- Content inspection is only allowed with clear indications of account abuse and authenticated orders (written or signed letter, or electronic message bearing a verifiable signature) from the Juridical Department and the Center of Information Technology.

2. What is the ground-rule upon which the RUG's AUP is based;

> Therefore, the ground-rule on which this AUP is based is similar to the ground-rule on which traffic is based: the users of the university computer systems may not endanger these systems, nor may they hinder other users.
>
> Some implications of this ground-rule are that users are not allowed to send unsolicited email or try to obtain or use other users' passwords; neither occasionally, nor `for fun'.

Summarized: Users of the university computer systems must not endanger these systems or hinder other users.

3. Mention four advices for users of 'RuGnet';

- Keep Access Information Secret: Don't share passwords
- Change Passwords Regularly: Change passwords regularly. Improves the security of the system.
- Report Security Holes: Report vulnerabilities and contribute to optimizing the system reliability.
- Only use the university computer systems for research and education.

4. Describe four actions that are prohibited by the RUG's AUP;

> Abuse of facilities and privileges is illustrated by, but not restricted to, the following examples. Users of the university computer systems are expected to prevent and fight any abuse of the university computer systems in the spirit of this AUP. The examples provided below should be interpreted as illustrations, not as an exhaustive list.
>
> It is not allowed:
>
> ```
> To modify or to remove hard- or software without having obtained
> prior permission from proper authorities;
> To use university computer systems, or to use any software or stored
> data without having obtained prior permission from proper
> authorities;
> To send any email using other people's names and/or addresses, or to
> read or distribute other people's mail without having obtained their
> consent in advance;
> To alter IP-addresses or other identifying data of university
> computer systems (e.g., by using spoofing);
> To violate software and/or copyright licenses that are applicable to
> the software and/or data that are stored on the university computer
> systems;
> ```

> ```
> To harass or hinder other users of the university computer systems;
> To gain access to, or to distribute any information stored in the
> university computer systems without having obtained prior permission
> of the owner of such software or data;
> To hamper or to deny access to the university computer systems by
> sending extremely large bodies of email, either to local destinations
> or to destinations outside of the university. Analogously, it is not
> allowed to abuse university computer systems by, e.g., submitting
> extremely large print-jobs, storing extremely large amounts of data,
> or executing programs using grossly inefficient algorithms or
> requiring excessively large resources;
> To distribute or to make available any information, irrespective of
> its form, owned by the university, without having obtained written
> permission by the owner in advance;
> To distribute or to make available obscene, aggressive,
> discriminating or threatening information.
> ```
>
> When there are clear indications that an account is being abused, systems managers may be ordered to inspect the contents of information stored in, going to or leaving that account (cf. section `Responsibilities of systems managers', below).

Summarized:

- **Unauthorized Access**: Users are not allowed to use other people's accounts. Any unauthorized use of an account is prohibited, and users must report any such unauthorized use to the security manager immediately.
- **Unauthorized Software Copying**: Users are not allowed to copy software stored on the university computer systems for use elsewhere except with explicit and written permission.
- **Commercial Use**: The use of university computer systems (hardware, software and network) is restricted to research or education purposes. Any commercial use of these systems is not allowed unless explicit and written permission has been granted.
- **Inappropriate Content**: Users are not permitted to distribute or make available obscene, aggressive, discriminating, or threatening information through the university computer systems.

5. What sanctions can be applied to those who violate the AUP?

> Abusing university computer systems may result in disciplinary action.
>
> If there are strong indications that university computer systems are or have been abused, and if the abuse can be traced down to a person who is associated with the university (the suspect), then at least one of the following steps should be taken to ensure the safety and integrity if the university computer systems:
>
> ```
> The board of the faculty or department responsible for the suspect is
> informed of the situation;
> The access rights of the suspect may be restricted or suspended,
> awaiting the results of the investigation. The suspect may file an
> objection to this restriction or suspension with the chair of his/her
> ```

```
department;
  o  Data files and media of the suspect are investigated;
  o  The board of the University and the board of the applicable
faculty or the director of the department responsible for the suspect
is informed about the (suspected) abuse.
```

Summarized:

- Violation may result in disciplinary action
- Restriction or Suspension of Access Rights

6. If a sanction is applied to you, where can you go to challenge that sanction?

An objection to the restriction or suspension may be filed with the chair of his/her department

Report Exercise 3

Purpose of this exercise: understand the properties of the substitution cipher.

In the report, provide your answers to the following questions:

1.

How many possible alphabets could be used in a substitution cipher that uses shifting?

A substitution cipher that uses shifting is known as the caesar cipher. Assuming we only have lowercase characters, then we have 26 different alphabets.

What about the number of possible alphabets in a substitution cipher that uses a mixed alphabet?

26!

2. Does applying a significant number of consecutive simple substitution cipher encryptions/decryptions with a mixed or shifted alphabet make it harder to break the original plaintext? Justify your answer.

No.

- Shift is a relatively weak cipher
- Shift value can be found using frequency analysis
- Chaining multiple shifts has no effect, because these operations can be merged. The attacker still only needs to the shift value for the merged operations which is easy with freququency analysis.
- Consecutive simple substitution cipher encryptions/decryptions performs one-to-one mapping so it wont be harder to break, consider mapping: abcd -> bcda ->dbac, it is actully abcd -> dbac.

3. Can the encryption function of the substitution cipher also be used for decryption? If so, how?

Shift: Yes. We have to shift by `26 - key`. See the code:

```
def encrypt_shift(text: str, shift: int) -> str:
    encrypted = ""
    for ch in text:
        if ch.isalpha():
            if ch.isupper():
                encrypted += chr((ord(ch) + shift - ord("A")) % 26 +
ord("A"))
            else:
                encrypted += chr((ord(ch) + shift - ord("a")) % 26 +
ord("a"))
        else:
            encrypted += ch

    return encrypted


def decrypt_shift(text: str, shift: int) -> str:
    return encrypt_shift(text, 26 - shift)
```

Yes Mapping works too.

Encryption function of the substitution cipher is an one to one mapping fuction,so the decryption function is just the encryption function
for example: the mapping abcde->deacb
E(bbc)->eea
E(eea)=E(E(bbc))=bbc