

## Summary for task x

### Applied cryptography Chapter 1:

- encrypting (E) means to hide a **message (M)**; plaintext (P) or cleartext, turning it into cyphertext (C)
  - It is any kind of binary data such as a stream of bit, text file, a stream of digitalized voice, image, video etc.
- decryption (D) is a process of turning cyphertext into the message
- cryptography: keeping messages secure
- letters create functions on how encryption flows to decryption
  - Encrypting:  $E(M)=C$
  - Decrypting:  $D(C)=M$
  - The full function of encrypting and then decrypting:  $D(E(M)) = M$
- In cryptography there are three vital components: authentication, integrity, nonrepudiation
  - authentication: there must be a possibility to verify as the receiver of the message
  - integrity: it can be proved by the receiver that the message has not been altered during transit
  - nonrepudiation: sender can't deny sending a message
- steganography: hides secret messages in another message
  - this can be in an image
- substitution cipher: characters are substituted by a different character
  - homophonic: plaintext characters can be several characters at the same time
  - polygram: blocks of characters encrypted in groups
  - polyalphabetic: many substitutions cipher used together to encrypt
    - Caesar cipher: characters replaced with the third character
- transposition cipher: order of characters has been changed
  - plaintext is written horizontally for example (simple columnar)
- rotor machines: created to automate encryption
- perfect encryption scheme is one-time pad
  - a large nonrepeating random set of key letters on paper glued together

- Most popular computer encryption algorithms DES
  - symmetric algorithm, same key used for encryption and decryption.
- RSA: popular public-key algorithm
- DSA: can't be used for encryption, just digital signatures

## PGP

- GNU: privacy guard for gpg, a popular encryption way and sign

```
safi@lightsaber-virtualbox:~$ sudo apt-get update
Hit:1 http://deb.debian.org/debian trixie InRelease
Get:2 http://security.debian.org/debian-security trixie-security InRelease [43,4
kB]
Get:3 http://deb.debian.org/debian trixie-updates InRelease [47,3 kB]
Get:4 http://deb.debian.org/debian trixie-backports InRelease [53,8 kB]
Get:5 http://security.debian.org/debian-security trixie-security/main Sources [5
0,3 kB]
Get:6 http://security.debian.org/debian-security trixie-security/main amd64 Pack
ages [45,7 kB]
Get:7 http://security.debian.org/debian-security trixie-security/main Translatio
n-en [30,8 kB]
Get:8 http://deb.debian.org/debian trixie-backports/main Sources.diff/Index [63,
3 kB]
Get:9 http://deb.debian.org/debian trixie-backports/main amd64 Packages.diff/Ind
ex [49,9 kB]
Get:10 http://deb.debian.org/debian trixie-backports/main Translation-en.diff/In
dex [33,0 kB]
Get:11 http://deb.debian.org/debian trixie-backports/main Sources T-2025-09-22-2
010.19-F-2025-09-14-2007.49.pdiff [11,6 kB]
Get:12 http://deb.debian.org/debian trixie-backports/main amd64 Packages T-2025-
09-22-2010.19-F-2025-09-14-2007.49.pdiff [15,9 kB]
Get:11 http://deb.debian.org/debian trixie-backports/main Sources T-2025-09-22-2
010.19-F-2025-09-14-2007.49.pdiff [11,6 kB]
```

```
safi@lightsaber-virtualbox:~$ gpg --gen-key
gpg (GnuPG) 2.4.7; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: lightsaber-laptop
Email address: rude.akili@yahoo.com
You selected this USER-ID:
"lightsaber-laptop <rude.akili@yahoo.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? 0
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/safi/.gnupg/trustdb.gpg: trustdb created
```

```
documents documents.pub music public templates
safi@lightsaber-virtualbox:~$ head -4 rude.pub
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEaNLpQxYJKwYBBAHARw8BAQdAGg6S8UMR0bJeVrjYXaBEI6wgvCin0nLU/0mb
JG990Zy0KGxpZ2h0c2FiZXItbGFwZG9wIDxydWRlLmFraWxpQHLhaG9vLmNvbT6I
safi@lightsaber-virtualbox:~$
```

```
key
safi@lightsaber-virtualbox:~/alice$ gpg --homedir . --fingerprint
/home/safi/alice/pubring.kbx
-----
pub   ed25519 2025-09-23 [SC] [expires: 2028-09-22]
       501F 6E01 43CF 6FAE 9B75  1EB7 6E49 9332 F768 A4FF
uid           [ultimate] Alice <alice@example.com.invalid>
sub   cv25519 2025-09-23 [E] [expires: 2028-09-22]

pub   ed25519 2025-09-23 [SC] [expires: 2028-09-22]
       1D5E C999 58C5 DD8D E75F  1EBB 5A44 FF6A 86DE 6D27
uid           [ unknown] lightsaber-laptop <rude.akili@yahoo.com>
sub   cv25519 2025-09-23 [E] [expires: 2028-09-22]

safi@lightsaber-virtualbox:~/alice$ gpg --homedir. --export --armor --output ali
e.pub
gpg: invalid option "--homedir."
safi@lightsaber-virtualbox:~/alice$ cp -v alice/alice.pub
cp: missing destination file operand after 'alice/alice.pub'
Try 'cp --help' for more information.
safi@lightsaber-virtualbox:~/alice$ cp -v alice/rude.pub
cp: missing destination file operand after 'alice/rude.pub'
Try 'cp --help' for more information.
```

I managed to create Alice in the linux but couldn't fix the issue with the files missing. Therefore I couldn't finish with encrypting and decrypting a message between the two.

```
safi@lightsaber-virtualbox:~$ sudo apt update
[sudo] password for safi:
Hit:1 http://deb.debian.org/debian trixie InRelease
Get:2 http://deb.debian.org/debian trixie-updates InRelease [47,3 kB]
Get:3 http://deb.debian.org/debian trixie-backports InRelease [53,8 kB]
Err:2 http://deb.debian.org/debian trixie-updates InRelease
  Sub-process /usr/bin/sqv returned an error code (1), error message is: Signatu
re by 4CB50190207B4758A3F73A796ED0E7B82643E131 was created after the --not-after
 date. Signature by B8E5F13176D2A7A75220028078DBA3BC47EF2265 was created after t
he --not-after date.
Err:3 http://deb.debian.org/debian trixie-backports InRelease
  Sub-process /usr/bin/sqv returned an error code (1), error message is: Signatu
re by 4CB50190207B4758A3F73A796ED0E7B82643E131 was created after the --not-after
 date. Signature by B8E5F13176D2A7A75220028078DBA3BC47EF2265 was created after t
he --not-after date.
Hit:4 http://security.debian.org/debian-security trixie-security InRelease
256 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: An error occurred during the signature verification. The repository is
not updated and the previous index files will be used. OpenPGP signature verific
ation failed: http://deb.debian.org/debian trixie-updates InRelease: Sub-process
 /usr/bin/sqv returned an error code (1), error message is: Signature by 4CB5019
0207B4758A3F73A796ED0E7B82643E131 was created after the --not-after date. Signat
ure by B8E5F13176D2A7A75220028078DBA3BC47EF2265 was created after the --not-afte
r date.
```

I've come across an issue when trying to update my VM to download the password manager.

Password managers are important because you can create more complicated passwords and protect against keyloggers. Keyloggers are logs that have been recorded from the used characters. This is a common way to steal someone's password.

It can manage ssh keys and keep it private and create backups.