# Encryption of Data – assignment

- **Task 1:**
  - Create a new key pair usable for encryption and document signing
    - select maximum available key size
    - the key pair should expire 3 month after creation
    - Export your public key and exchange the exported keys with a colleague
    - Import colleague’s key into your key-chain
    - Verify the fingerprint of the imported key with the value from your colleague, sign the key
- **Task 2:**
  - Encrypt and sign a regular file using an asymmetric cipher.
    - Encrypt the file so that the contents can be read both by the colleague and you.
    - The message and the signature should be in the same file.
  - Exchange the encrypted file with your colleague whose key was used to encrypt it.
  - Decrypt the received file and verify its contents and signature.
- Number of points: 0,5 pt. per task.

# Encryption of Communication - assignment

- **Task:**
  - On your virtual machine, activate web console ‘cockpit’.
  - Create a tunnel that allows establishing a connection from outside network (e.g. from home) to the web server running on your machine (which is behind NAT and does not have a public IP address) via an accessible SSH server (e.g. ‘student.fiit.stuba.sk’).
- Example:
  - Connection to 'student.fiit.stuba.sk:9090' (or at least 'localhost:9090' on server 'student' ) will be forwarded to the port of the cockpit console on your virtual machine.
- Demonstrate correct functioning of the tunnel.
- Describe in detail the function and importance of this kind of forwarding.
- Number of points: 1 pt.

# References

- man gpg
- https://www.gnupg.org/gph/en/manual.html
- http://www.spywarewarrior.com/uiuc/gpg/gpg-com-4.htm
- https://futureboy.us/pgp.html
- man ssh
- man sshd
- man ssh_config
- https://cockpit-project.org/
- man curl, wget, lynx