STI MEI/MIEBIOM 2022/2023

Practical Exercises #1

Email security using PGP (GnuPG)

1. Create a public and private key pair using GnuPG
2. Publish you PGP public key on http://pgp.dei.uc.pt
3. Add the public keys of other users to your PGP Keyring
4. Validate the public keys of other users on your PGP Keyring
5. Change the level of trust on another user on your Keyring
6. Use PGP to secure email:
    - Send an encrypted message
    - Decrypt a received message
    - Send a signed message
    - Verify the signature in a received message
    - Send a signed and encrypted message
    - Verify and decrypt a received message

Configuring PGP on your email client

Enigmail: https://www.enigmail.net/

GPGTools: https://gpgtools.org

Mailvelope: https://www.mailvelope.com

Goals

Secret and public-key cryptography

Email security with PGP (GnuPG)

Materials

- GnuPG, The GNU Privacy Guard: http://www.gnupg.org
- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, Capítulo 2: "Segurança em Correio Eletrónico"