GPG *Gnu Privacy Guard or GnuPGP)

- GPG
  - Free cryptographic software originally developed by Werner Koch.
  - It supports important major cryptographic algorithms, which are known to be secure.
  - Has been continuously updated.
  - A crucial tool for privacy protection – Known to be used by Edward Snowden to prevent his communications from being eavesdropped.

GPG

- Symmetric encryption
  - To encrypt: `gpg -c test.txt`
    - ✓ The ciphertext `test.txt.gpg` will be created.
    - ✓ To save your ciphertext in ascii format use: `gpg -c --armor test.txt` (Note that without the armor option, the default format of the ciphertext (encrypted text) is binary, which cannot be displayed correctly. *Try: `cat test.txt.gpg` and `cat test.txt.asc` and compare the result.
    - ✓ Note that "AES" is a default symmetric encryption algorithm.
  - To decrypt: `gpg test.txt.gpg`

GPG

- Public key encryption
  - To generate key: `gpg --gen-key`
    - ✓Default is RSA2048
    - ✓It may take some time depending on platforms
    - ✓Important to use correct uid (email address)
  - To export a public key: `gpg --armor –-export uid > mypubkey.gpg.asc`
    - ✓You can send your public key to your friend.
  - To list the public keys you have in the current system: `gpg –-list-keys`
  - To import a public key: `gpg --armor –-import pubkey.gpg.asc`

GPG

- Public key encryption
  - To encrypt: `gpg --encrypt -r <recipient_uid> --armor filename`
  - To decrypt: `gpg filename`

GPG

- Task: Assume that you are Alice on Kali VM. Your friend is Bob on Ubuntu VM.
  1. GPG is also installed on Ubuntu. On Ubuntu VM, generate a Bob's public key, export it as asc (ascii), and send it to Alice on Kali VM (via email). [See page 3]
  2. On Kali VM, import the received (Bob's) public key and encrypt any message using it (Bob's public key). Send the ciphertext to Bob the Ubuntu VM (via email). [See pages 3 and 4]
  3. Bob decrypt the received ciphertext with his private key. [See page 4]