Task_1

Public cryptographic system.

1. Discuss the system of cryptography based on private and public keys. Explain the idea of unsymmetrical encrypting, including mathematical algorithms.
2. Familiarize with the system gnuPG (http://www.gnupg.org).
3. Perform the exercise using gnuPG:
   - 3.1. Generate pair of keys, perform the measure of generating time (any method available). 1024 bit key password protected.
   - 3.2. Send the public key to the another user via email.
   - 3.3. Add public key you have just received (from the another user) to your container of public keys.
   - 3.4. Add identifier to your private key. Now you can use ID as your full key name.
   - 3.5. Sign public key you have received before using your private key.
   - 3.6. Examine content of your container of public keys to be sure that your previous commands have been performed correctly.
   - 3.7. Encrypt any binary file (e.g. graphic one) **FILE1** using public key you have received before and send both files (encrypted and original) by email. Delete both files.
   - 3.8. Decrypt using your private key files you have just received. Compare decrypted and original files, they should be identical.
   - 3.9. Sign text file **FILE2** using your private key, not encrypting itself (its contents should remain legible). Check the signature correctness and send that file to the another user.
   - 3.10. Check the signature correctness under the file (**FILE2)** you have just received from the another user.
   - 3.11. Revoke your key.
   - 3.12. Send the certificate of revocation to the another user (by email) to inform him that your key is ivalid.
   - 3.13. Add the certificate of revocation which you have just received from the another user to your container.
   - 3.14. Check what has been changed in your container of keys.
   - 3.15. Delete keys which have been revoked.
4. Every step of the exercise described above should be presented in your report (description, screen shots etc.)