**Assignment Directions**

This assignment aims to train the use of a powerful cryptography application (GnuPG[[1]](#footnote-1)) in a set of different situations. The students will organize in a group (maximum of five) and realize all tasks suggested in this assignment.

Only one student submits this document with all answers and, if necessary, any complement files. It is required to fill the identification form.

**Identification Form**

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **E-mail** |
| **1** |  |  |
| **2** |  |  |
| **3** |  |  |
| **4** |  |  |
| **5** |  |  |

**PART I - Use of Cryptology Tools (100 points)**

1. Which kind of asymmetric algorithms does GnuPG support?
2. Comparing ElGamal and RSA, what is the main difference between both algorithms?

**For the following seven questions, the answer must type the command used to perform the task.**

1. Create at least 04 Elgamal key pairs using GnuPG and saved them into a file.
2. Check if there are any other keys locally installed.
3. Delete the key recently generated (question 3) and reimport them into the system.
4. GnuPG implements a set of different symmetric algorithms. Compare Blowfish and AES (Cite at least three differences between then and one case where Blowfish is a better idea when comparing it with AES.
5. Cipher a file (choose one) using AES-256, and then output is formatted in ASCII.
6. Cypher and signed a file using a symmetric algorithm and saved the output file using this name: 'cypher\_signed\_file.txt.' Verify the signature and decipher the file 'cypher\_signed\_file.txt.'
7. Using an asymmetric algorithm, encrypt/decrypt a file using one of the public keys generated previously.
8. Sign a message (file) after separate the signature file from the message file (detached) and verify the file using the signature.

**PART II – Challenge (+20 points)**

Using the classes server.py and client.py and the keys generated (Part I), Implement a client x server application in Python that performs the following process.

**Reference:** <https://docs.red-dove.com/python-gnupg/>



1. <https://gnupg.org/> [↑](#footnote-ref-1)