ASSIGNMENT 2

PGP/GPG, S/MIME, Digital Signatures and Anonymity

Paolo Molinaro
pm222py@student.lnu.se

TOOLS AND REQUIREMENTS

- Small mail client with support for PGP/GPG: Try Thunderbird
- Supporting applications to work with certificates: OpenSSL
- PGP/GPG apps, additional add-ons… Figure out what you need!
- Two classmates for correspondence, key signing
- GNU/Linux - (WSL encouraged!)
- 9-page limit!

PRETTY GOOD PRIVACY / GNU PRIVACY GUARD

WHAT IS IT?

Created by Phil Zimmerman, it's a popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files.

OpenGPG standard -> Look in RFC 4880

- GNU Privacy Guard (as alternative)
- KGpg - tool if you want GUI instead

GPG

- You will work with different key-servers
- Old vs New generation
- When sending email to your instructor, make sure everything is in order! Send a test email to yourself first!

SECURE / MULTIPURPOSE INTERNET MAIL EXTENSIONS

- Defined by IETF
- You will need some kind of software to encrypt emails with this standard!

USEFUL LINKS

- GnuPG
- Thunderbird
- Enigmail
- Simple PGP Key Server
- PGP with key management