

ELEC-C7420 Basic Principles in Networking Spring 2022

Assignment VI: PGP



Aalto University
School of Engineering

PSALTAKIS GEORGIOS

Goals of the experiment

This experiment is a quite simple implementation of PGP encryption in emails encrypting either plain text or even files . We also implement signature in emails.

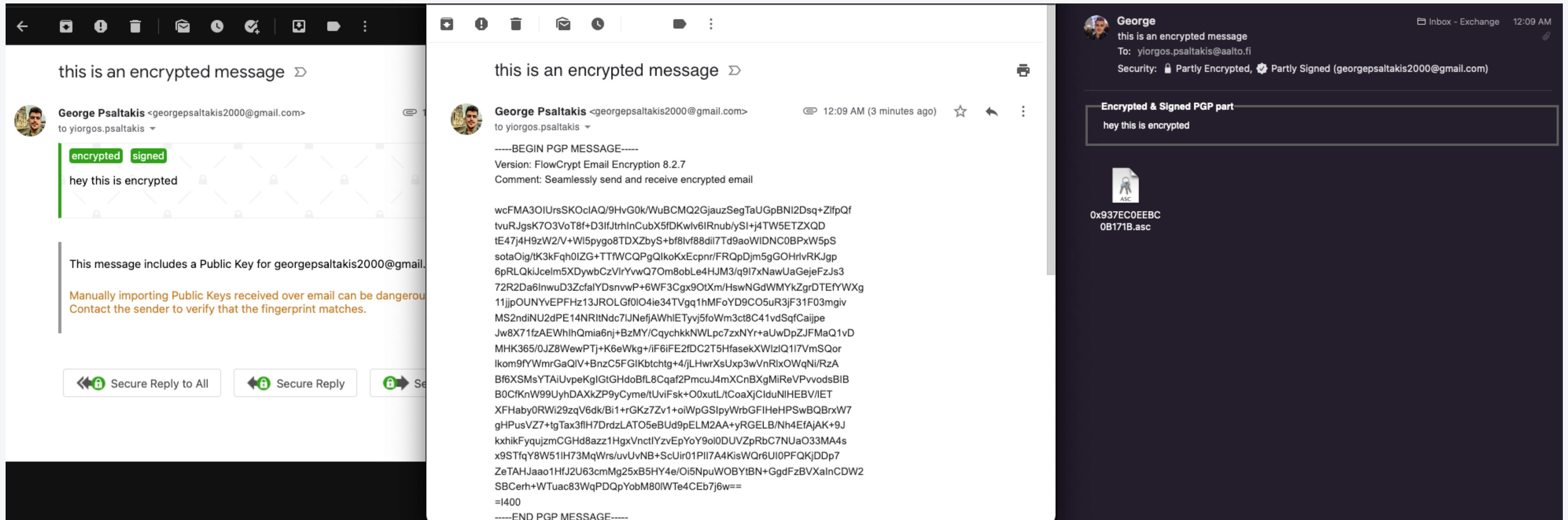
The goal is to better understand the reasoning behind the PGP encryption and to understand the use case scenarios as well as the ease of use to implement it.

Experimental Setup

The experimental setup is quite simple for this assignment. I used my personal gmail as well as my academic outlook email to sent emails back and forth. For gmail i used the secure compose and i created my private key and published exported the public key to share with my academic email account. In my academic email i used the GPG keychain app and included the addon in the email app of apple. I then also exported the public key for the private key i gave for my academic email and added it to secure compose on gmail.

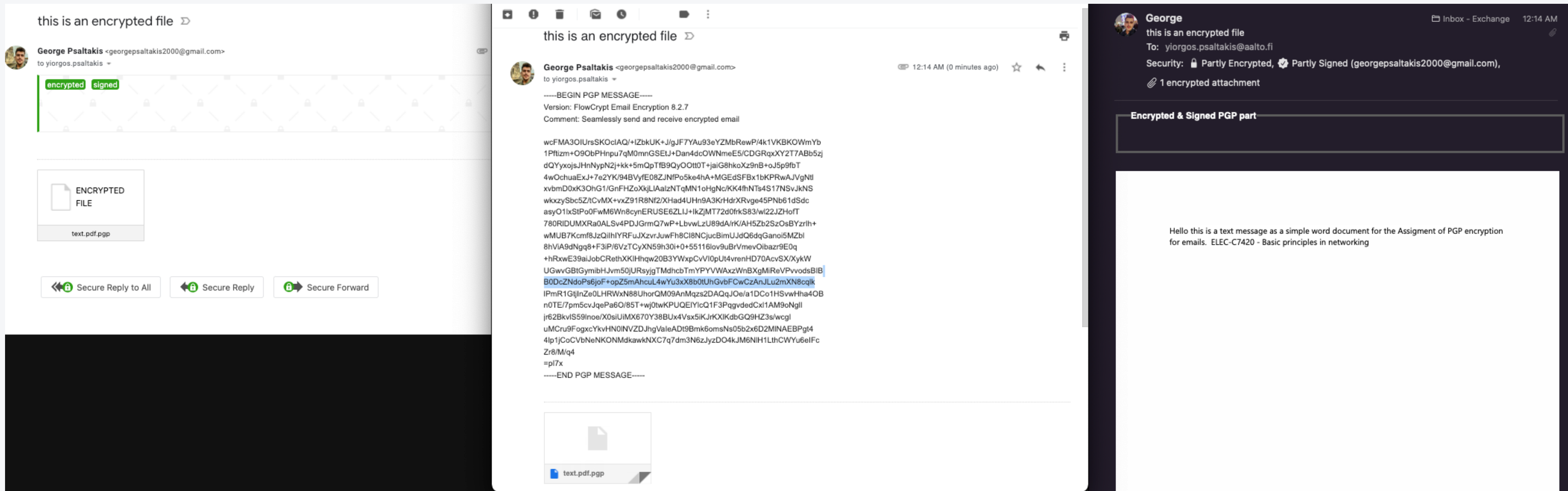
Results & Conclusion

Successful Plaintext Encryption/Decryption



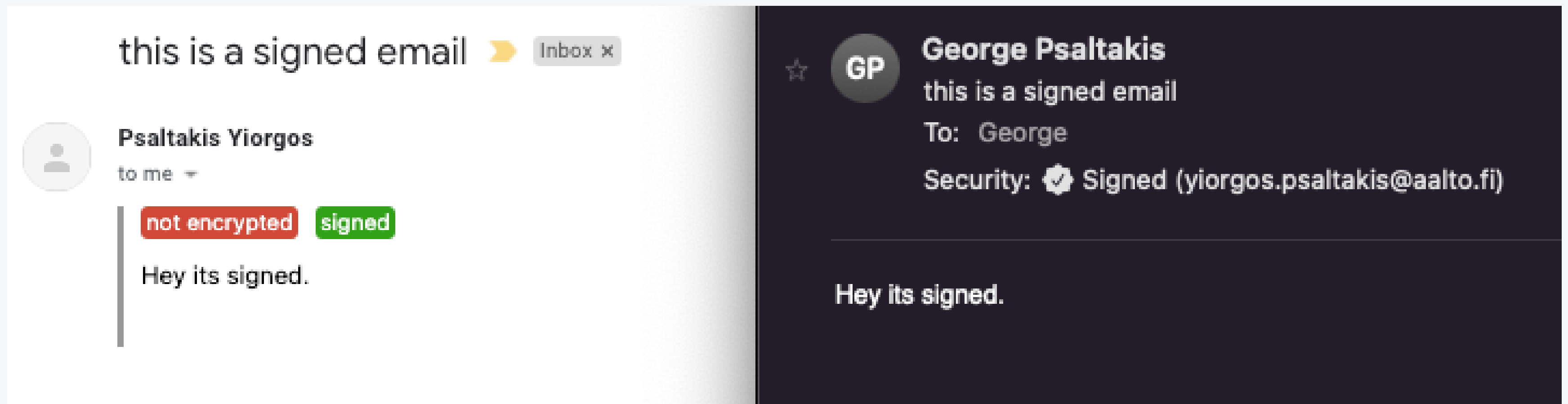
Here we can see the successful encryption and decryption of the email text between sender and receiver

Successful Attachment Encryption/Decryption



Here we can see the successful encryption and decryption of the attachment in the email between sender and receiver

Implement Digital Signature



Here we can see the successful implementation of the digital signature using the GPG keychain