ITSI PGP Aufgabe Jakob Franzel

Aufgabestellung:

Eine GPG-Software installieren und eine Verschlüsselte Mail mit Bild durch einen E-Mail-Client verschicken.

Aufgabenlösung:

Nach der Installation von Gpg4win kann ein Schlüsselpaar erstellt werden dies kann ebenfalls mit einem Passwort gesichert werden. Nach der Erstellung sollte der Schlüssel auf einem Keyserver hochgeladen werden damit andere Nutzer dieses finden können. Neuere E-Mail Softwares haben bereits durch die Installation von Gpg4win eine Integration für GPG bekommen. Nach dem Schreiben der E-Mail und anhängen des Bilds kann die Mail verschickt werden. Bevor diese an den Empfänger gesendet wird, können noch finale Einstellungen zu GPG gemacht werden, sowie mit welchem Schlüssel man die Nachricht verschlüsselt.

Die PGP Verschlüsselung verwendet User-Trusted Keys. Das heißt dass ein generierter Key von anderen Personen unterschrieben / signiert werden können und somit können andere einem von vielen verschiedenen Personen signiert ist kann man diesem ebenfalls trauen. Um Daten zu signieren und zu verschlüsseln, nutzt man seinen Private Key, der wie schon im Namen steht, privat bleiben sollte. Gesendete Daten kann man mit dem Public Key wieder entschlüsseln, um die Originale Daten zu bekommen. Eine Signierung eines Dokuments kann ebenfalls mit dem Public Key überprüft werden.