Security - PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication.

- We can use PGP tools for protecting digital information
- PGP can be used as a library for other programming languages: https://www.openpgp.org/software/developer/

GPG Installation

GPG (GNU PGP) is the Open source implementation of PGP.

We can install PGP CLI programs using `brew` or `choco`:

```
brew install gnupg  # Mac
choco install gnupg # PC
```

🔑 Create a Public/Private Key Pair

Run the command:

```
gpg --gen-key
```

Then follow the prompts to enter your name, email, and passphrase.

Example output:

```
gpg: trustdb created
gpg: revocation certificate stored as '...rev'
public and secret key created and signed.

pub   ed25519 2022-03-15 [SC] [expires: 2024-03-14]
      F57AC82C7287D917A00C52AD951B59471C7CF6FE
uid   smcho <chos5@nku.edu>
sub   cv25519 2022-03-15 [E] [expires: 2024-03-14]
```

Encrypt a File

Jim can now encrypt a message for you using your key:

```
gpg --recipient smcho --encrypt myfile.txt
```

This creates myfile.txt.gpg, an encrypted file safe to send.

Decrypt a File

When you (smcho) receive myfile.txt.gpg, decrypt it with:

```
gpg -d myfile.txt.gpg
```

You’ll be asked to enter your passphrase.

Example output:

```
gpg: encrypted with cv25519 key, ID 46C764EADFBE878F
      "smcho <chos5@nku.edu>"
This is a secret message.
```