GPG

2018

Symmetric Cryptography

- One key
- Used for encryption **and** decryption

Asymmetric Cryptography

- Two keys
- A public one and a private one
- Whatever is encrypted with the public key can be decrypted **only** with the private key and vice verca
- GPG

Download GPG

- **Linux**: Already installed
- **Windows**: `https://www.gpg4win.org/`
- **Mac**: `https://gpgtools.org/`

Key Creation

- gpg –gen-key
- Real name and email
- 4096 bits
- Good password
- Cannot retrieve password if lost
- Reccomended expiration time: 1 year
- Renew with gpg –edit-key *identifier*

Key Servers

- Where we publish our keys
- e.g. pgp.mit.edu
- gpg –keyserver pgp.mit.edu –send-keys D1372AFA
- Publish the public key with identifier *D1372AFA* to the pgp.mit.edu key server
- gpg –keyserver pgp.mit.edu –recv-keys D1372AFA
- Download the public key with identifier *D1372AFA* from the pgp.mit.edu key server

Message Encryption

- Using the public key of the receiver of the message
- Have to download the public key first
- gpg -a –encrypt –recipient D1372AFA
- Encrypt a message with the public key of *D1372AFA*
- Type message and ctrl+d on Linux/Mac and ctrl+z on Windows

Ciphertext

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEMA3IZE7Agm8S5AQf/ZMfPl6TG+hMh+ehUnmL9U+2yIr6GBZyuCVXbHvi3JsJI
+ndyFZkFfD98m16wnaHhftSw134xESgQqeJCGkjnWaLt7bDjRYoN5s8pxAmne0D1
e6kPYQKMCC7/P8BWo0CKAfkf0nFpqycyKKSaQgJL8aA85URN4NsTh5IuXaHtRRUc
+l4U55e03p4nUvQDwzU+G6gbM0wEUHimsXW7unY9s6Sx+EF3zgw7l/H8NSx1pW4O
tjch5EhSnYuvMG8bQ9a5lG+DftX4EPIV/3p6tdvWivmXUDZYSB5z/MA5KLRWqoNP
9PMLtnzEfxzjf72OZTGsQ1hXT9PjzkcyK2bqWCDer9JBAf6Sh11SzZJakQM9/zLZ
YmaQ3jJe+1RP7aj5kLHYcC+npvo3ZWhoYddmEiHVNcLW7q/SPSwZ/9JFwmqf5+aM
8Sg=
=so3C
-----END PGP MESSAGE-----
```

Message Decryption

- gpg –decrypt
- Copy/Paste the ciphertext
- Message has to be encrypted with our public key

Message Signing

- gpg –clearsign
- Sign a message
- gpg –verify
- Verify that a message has a valid signature

Signature

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

I am the real Vitalis!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBCAAGBQJa6ufkAAoJEOiKrw/RNyr6p7QQALMh6RexfikBjkOKZd8IA+tg
0Ns9g7G12gPu6vyCrw2TwL4x6JK7KLg3EPFvWSdpC1S6j4lItYF2M7/E3LbavzM1
bzfq0V1m2/PCXHYPrL5LLBM+oDSvRRPCDDxs/kRKR03r54dx2iTqKRZNFNBufYto
ITvd4jbne+eYpTxqBPNv73wXkIsLzp3o0cOJ9nQodbo67tv5ME9OCGx7KLJDdYHH
LmY9C2Leri2Xc2B0BgJV49yROn+LCoDK8qrhiyi8UvHcTdqyHqmMq+7WUceoH8pv
XbWvvCPcec0Z3q6gGT8P1QKWVeEd6FQTbR9SZWTM1JfyrwKG5o/XWyuaFzFXGYeP
NVnqD2GHogftwiEUNFX3Ss9zJimunQnM7WOJJyEQsrGO2jDp05nUzaLKGkKF9ITU
B382E+EkpP2jYWu8Z+ty8/o9VLd2g6pLTKQaWT2e3Ae/pEjFT9yxoWIUP+6xj2pg
YT974p6r/FXTB8NfJ87Mb3zfGok5Yza+vHS7hWV0SlBYRrsx2SCkyzpS0JRrdX4Q
3Ey1qdN9ykwhIqvjO9v7BtZXalSi6MND40+J3TOvtInNYAXx0Rh3vZ+O3yTnWd7H
z+h4xMcyfwmSUAM5N6BQNrdQViLGr6QoNkKHpU8eoyXDbCP/k9clUtO2Ok/kKfK6
7fyBv6qxOFDX3rFHJh0j
=qVbm
-----END PGP SIGNATURE-----
```

Trust Relationships

- Anyone can create a key with my name
- How can someone know that a public key actually belongs to me?
- Solution: **key signing**
- People that know me and have verified that a public key belongs to me upload a signature that states that a key belongs to me
- gpg –sign-key D1372AFA
- gpg –keyserver pgp.mit.edu –send-keys D1372AFA

Cheat Sheet

- **Create**: gpg –gen-key
- **Publish**: gpg –keyserver pgp.mit.edu –sendkeys D1372AFA
- **Retrieve**: gpg –keyserver pgp.mit.edu –recvkeys D1372AFA
- **Show**: gpg –list-keys
- **Encrypt**: gpg -a –encrypt –recipient D1372AFA
- **Decrypt**: gpg –decrypt
- **Sign Message**: gpg –clearsign
- **Verify Signature**: gpg –verify
- **Sign Key**: gpg –sign-key D1372AFA