**PGP Self-study Notes**

Available flavors

* GPG – Open source PGP, x-platform

Key Generation

* Information needed:
  + Kind of key (algorithm)
    - RSA, DSA, etc.
  + Key size
    - 1024, 2048, etc.
  + Key Validity
    - 1day, 1month, 1year, etc.
  + Identity information
    - Name
    - Email address
    - Comment (optional)k
  + Passphrase (optional)
    - This is additional security on top of private key – just in case private key is compromised
* Entropy: This is a random number generation. This takes time, and if the host is doing other compute, that helps. Question: How to make the host work on other compute?
* Revocation certificate
  + Post to public servers if secret key is compromised
  + So that others are aware this key is not to be trusted
  + Can be created even after the key is compromised (more appropriate)

GNUPGP

* Installation by downloading platform installable from gnupg.org
* Pulled up the command line and typed gpg



* + This creates an empty secret ring and public ring
  + Secring holds all private keys
  + Pubring holds all public keys
* Creation of private/public key
  + Command gpg --gen-key
  + After taking you through multiple prompts, it generate public/private key – there is substantial delay in creation of the key
* Exporting public key
  + gpg --armor --export uid > [output file.asc]
    - armor exports in ascii format