Gnu Privacy Guard

(aka GnuPG)

(aka GPG)

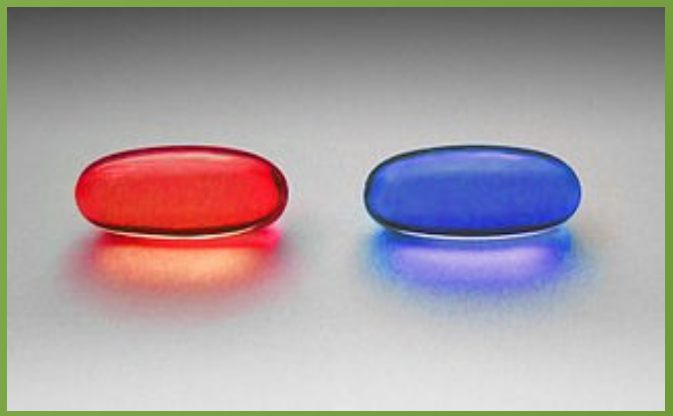
An Introduction

Stephen R Guglielmo (http://srg.io)

March 10th, 2015, Temple University

Who's This Guy?

- AS in CS from DCCC
- IS&T major at Temple University



- Just another tech geek that took the red pill
- Disclaimer: There's tinfoil under my hat

Overview

- History
- Protection
- How does it work? / Theory
- How does it work? / Practice
- Further Info / Credits

History

PGP → OpenPGP → GnuPG

1991 → 1997 → 1999

“PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.”

~Phil Zimmermann, 1995

Protection Against...

- Eavesdropping
- Modification of data in transit (MitM)
- Impersonation (well...maybe; see WoT)

No Protection Against...

- Coercion
- Incorrect use / Data leaks
- Metadata (including email subject)
- Loss of private key
- Moore's Law
- Quantum Computing

How Does GnuPG Work?

Data Encryption

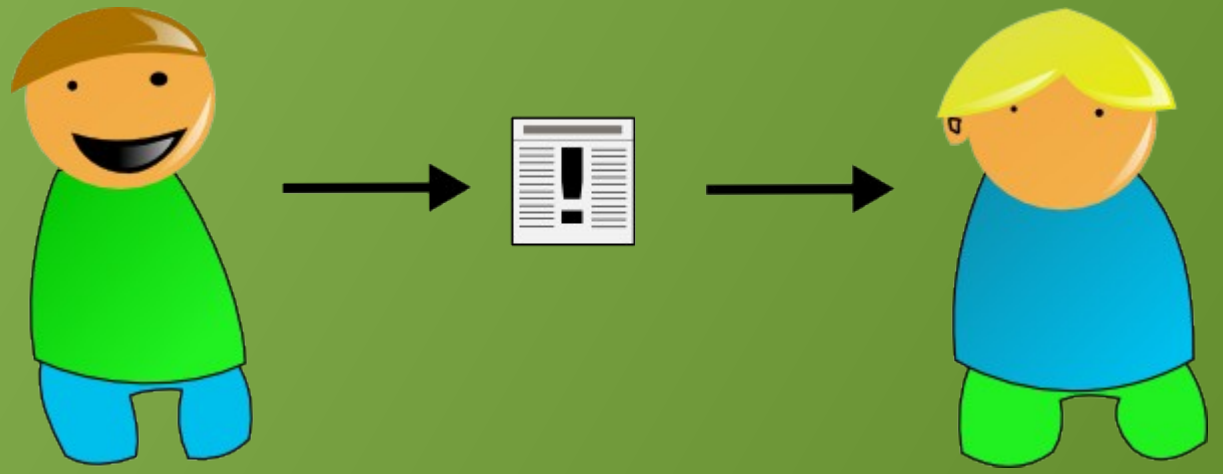
and

Data Authentication
(signing)

How Does GnuPG Work?
Theory

How does one communicate securely **without** first exchanging a secret?

How does one know who they **think** they're communicating with is who they **really are**?



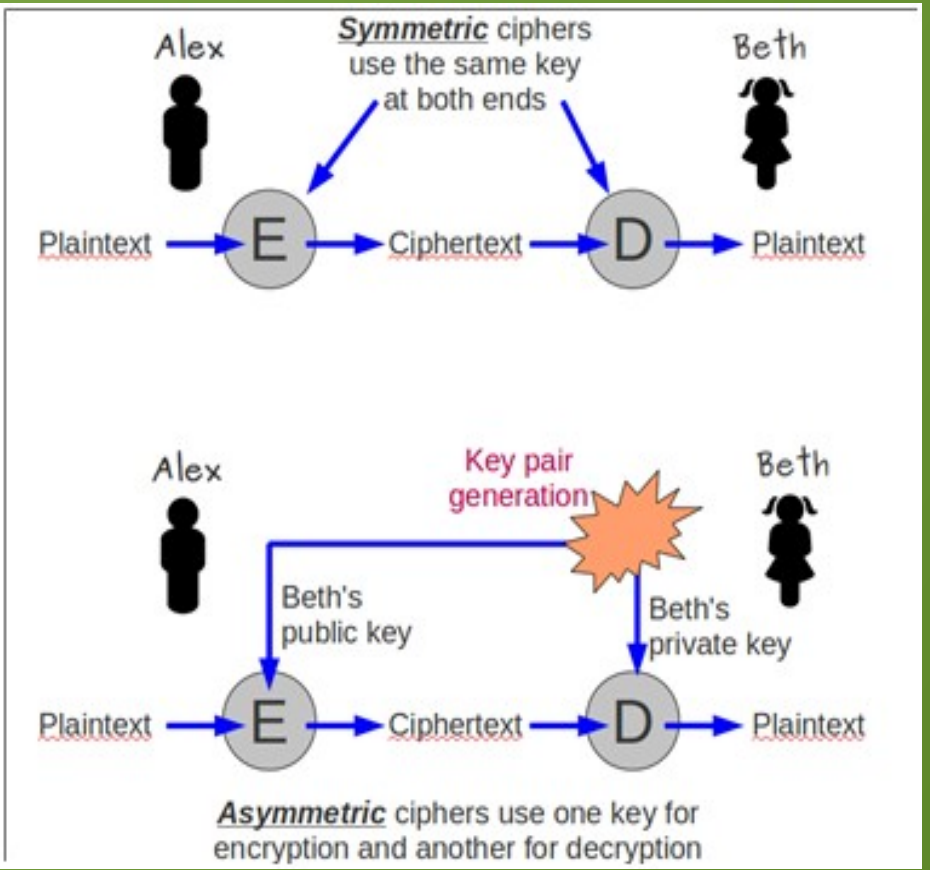
How Does GnuPG Work?
Theory

Public Key Cryptography

(Asymmetric Cryptography)

Symmetric
- Same key to encrypt and decrypt

Asymmetric
- Separate (but mathematically connected) keys to encrypt and decrypt



How Does GnuPG Work? Theory

Public Key Cryptography

(Asymmetric Cryptography)

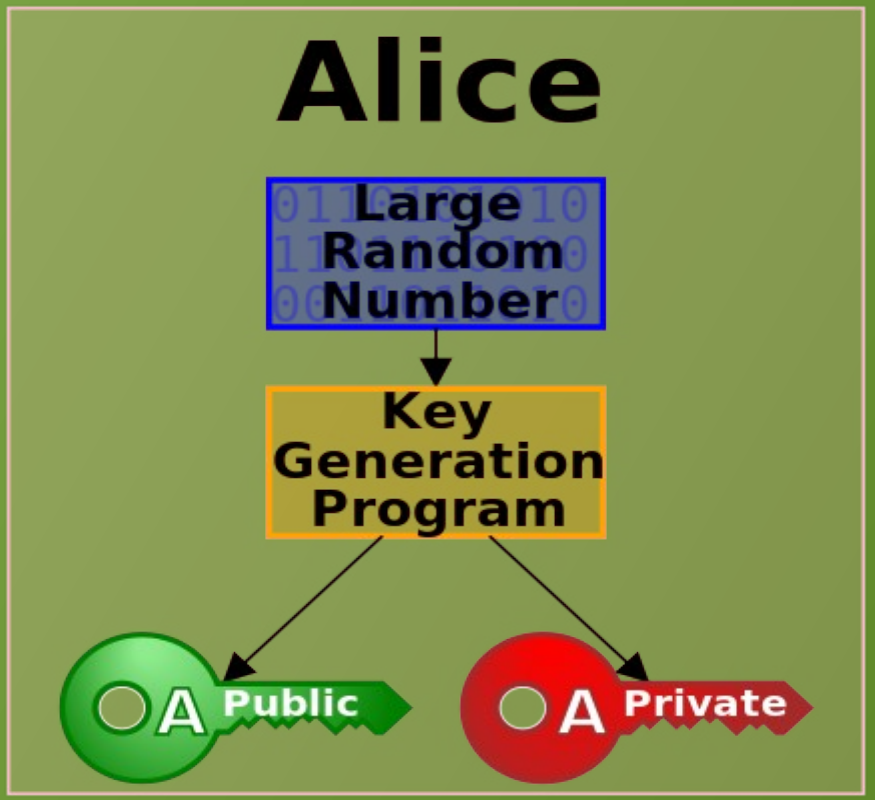
- Math problems w/ no efficient solution
  - Factorization of very large prime numbers
  - Discreet logarithms
  - Elliptic curves

How Does GnuPG Work? Theory

Public Key Cryptography

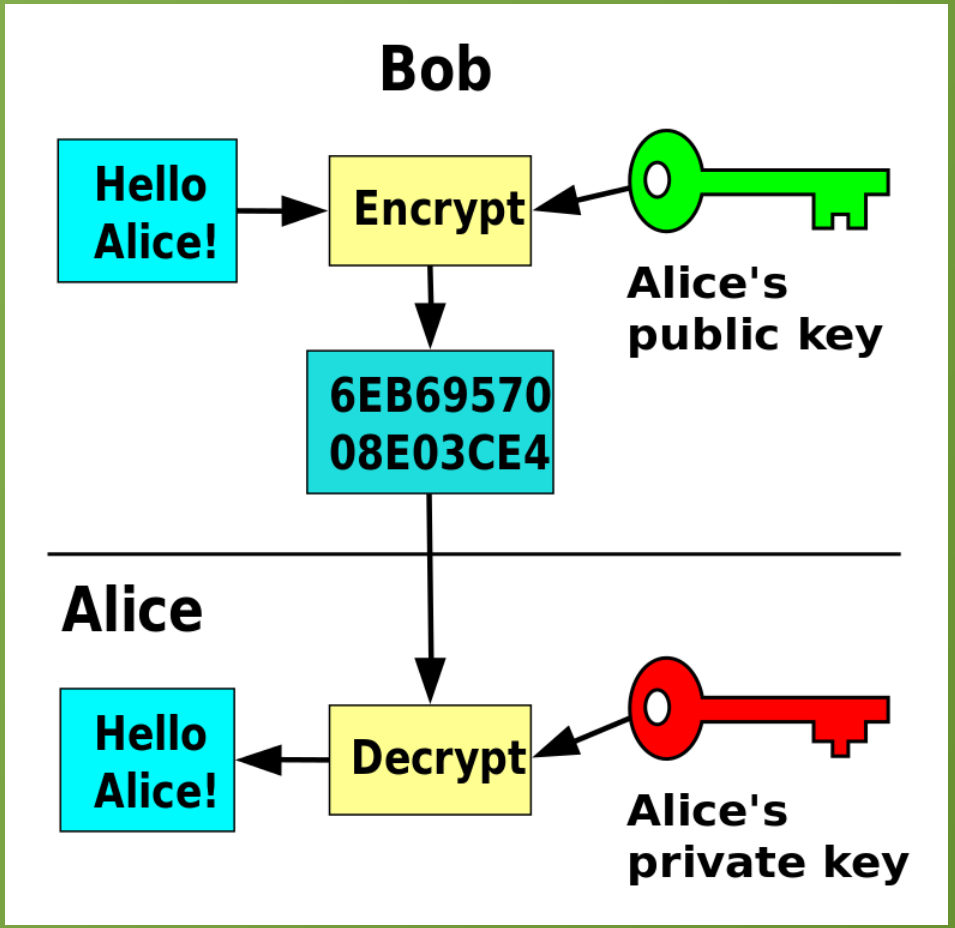
<u>Keypair</u>

- Public Key
- Private Key



How Does GnuPG Work? Theory

Bob sends a message to Alice

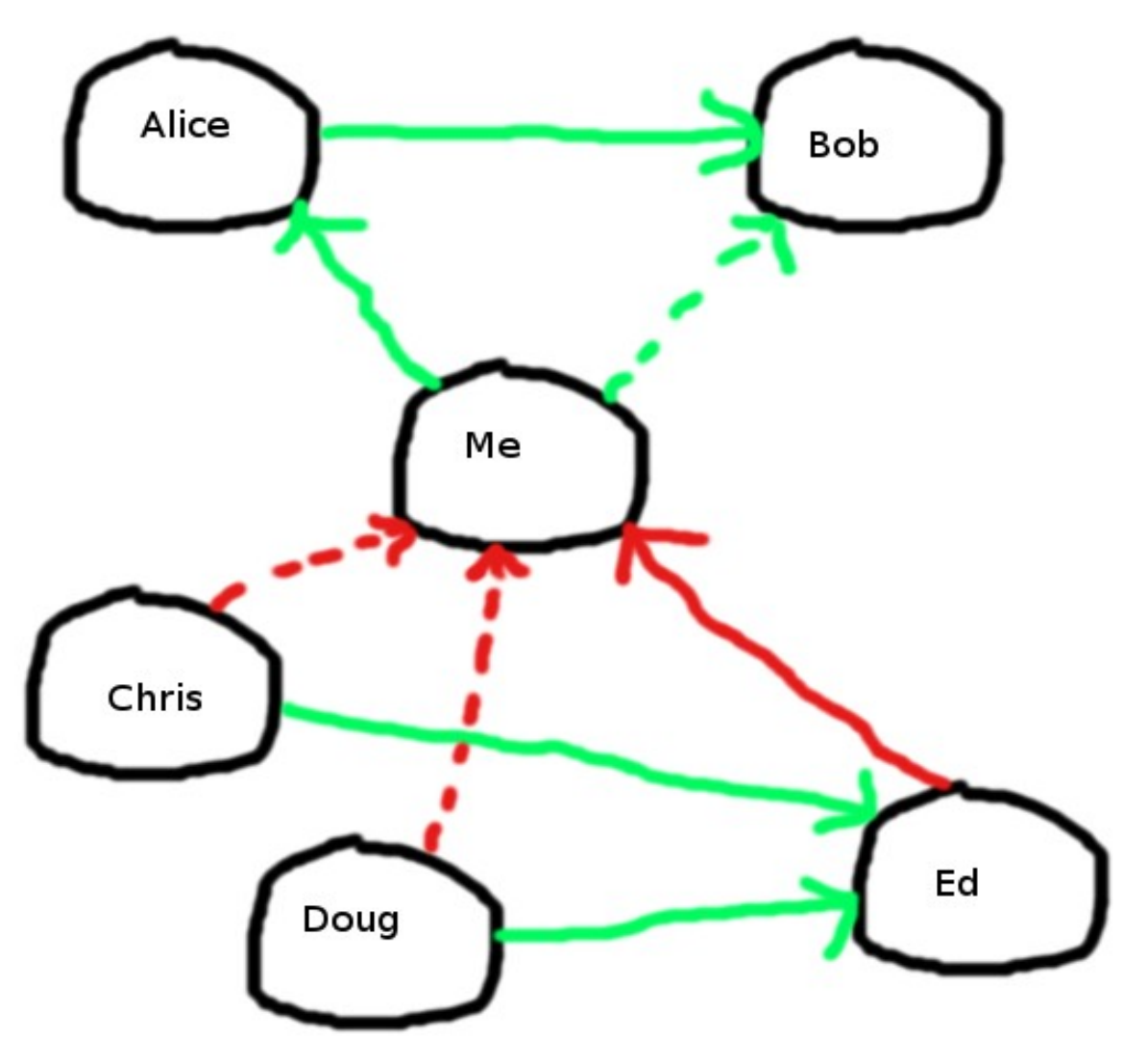


How Does GnuPG Work? Theory

Web of Trust

- Sign another users **public key** with your **private key**
- Verifies: Specific public key → Specific human
- How far until trust is satisfied?
- Four levels
  - Unknown / Don't trust / Trust marginally / Trust fully

How Does GnuPG Work?
Theory
Web of Trust



How Does GnuPG Work? Theory

Web of Trust

How Does GnuPG Work? Practice

- Install GnuPG
- Generate your keypair (optionally publish pubkey)
- Setup your email client
  - Typically can't just paste into webmail

```
srg@lapsdeb:~$ gpg --version
gpg (GnuPG) 2.0.26
libgcrypt 1.6.2
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, RSA, RSA, ELG, DSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
srg@lapsdeb:~$
```

How Does GnuPG Work? Practice

Install GnuPG

- Debian

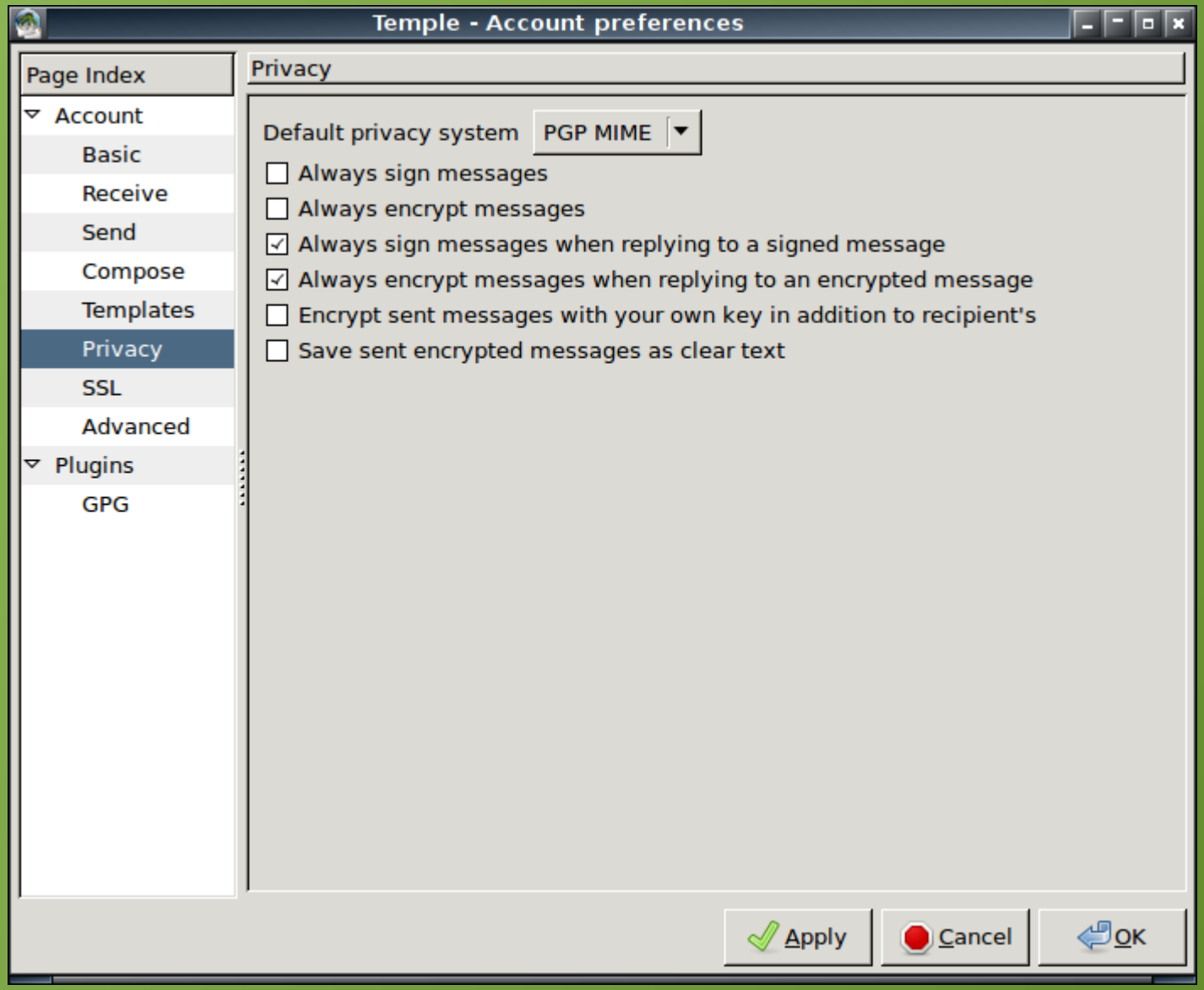
sudo apt-get install gnupg2 claws-mail claws-mail-pgpinline claws-mail-pgpmime

- Windows: GPG4Win
  - http://gpg4win.org
  - A bundle with several programs, including Claws-Mail
- Mac OSX: GPGTools
  - https://gpgtools.org
- Android: K-9 Mail and APG
- iOS: iPGMail (Not FOSS!)

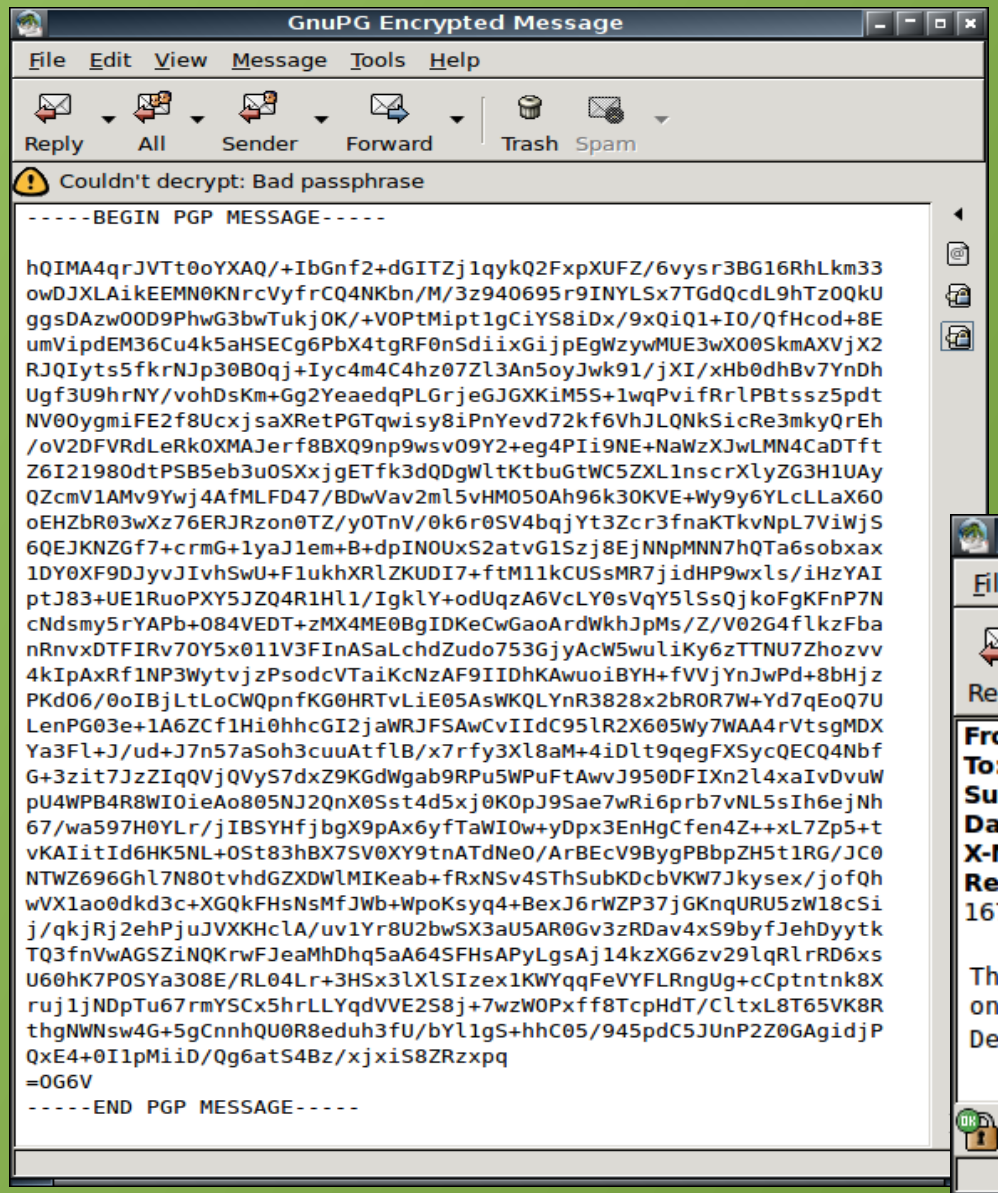
How Does GnuPG Work?

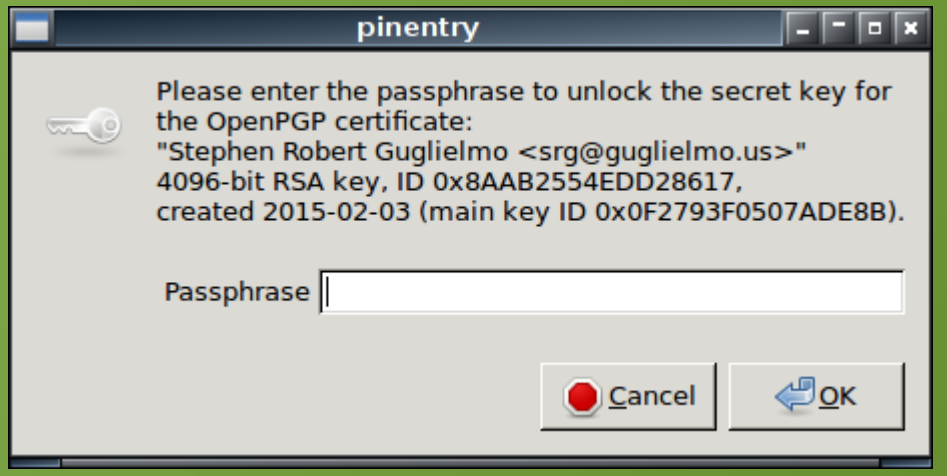
```
srg@lapsdeb:~$ gpg2 --gen-key
gpg (GnuPG) 2.0.26; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1y
Key expires at Wed 02 Mar 2016 07:32:55 PM EST
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Stephen R Guglielmo
Email address: srg@guglielmo.us
Comment:
You selected this USER-ID:
    "Stephen R Guglielmo <srg@guglielmo.us>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.
```

How Does GnuPG Work?



How Does GnuPG Work?





How Does GnuPG Work?

Beyond the scope of this presentation...

- Theory
  - Actually, 4 keys in each keypair
  - File encryption uses hybrid asymmetric/symmetric method
  - Different cipher, hashing, key algorithms and key lengths
- Practice
  - Keyservers
  - “Best practices” for security
  - Backing up private keys
  - Revocation
  - Subkeys/UIDs

More Information

- Slides and related text document available at http://srg.io
- Wikipedia
- Electronic Frontier Foundation (SSD)
- “Best Practices” guides on the internet (see text doc for links)
- Email me to test: srg@temple.edu

Image Credits

Unattributed images are licensed under the GPL or in the public domain

- Red/Blue pill by W.carter on commons.wikimedia.org
- Phil Zimmermann on http://www.mit.edu/~prz/EN/photos/
- Firewall by RRZEicons on commons.wikimedia.org
- Hammer by Shakespeare on en.wikipedia.org
- Root Lock by schill on Flickr
- Message Communication by Einar Faanes on commons.wikimedia.org
- Symmetric vs Asymmetric by ict@innovation on commons.wikimedia.org
- Signing Public Key Comic by Randall Munroe on xkcd.com