Cryptographic Applications: PGP

maz@iij.ad.jp

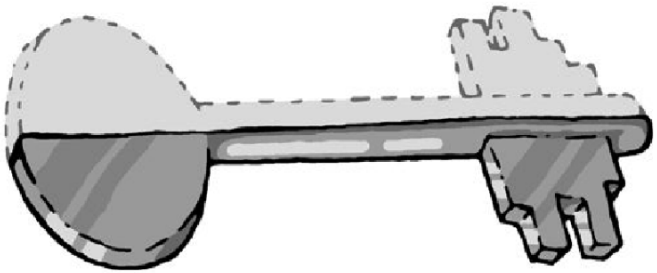
stole slides from

pokui@nsrc.org

Asymmetric encryption refresher:

- One key mathematically related to the other.
- Public key can be generated from private key. But NOT vice versa.
- If you **encrypt** data with the **public** key, you need to **private** key to **decrypt**

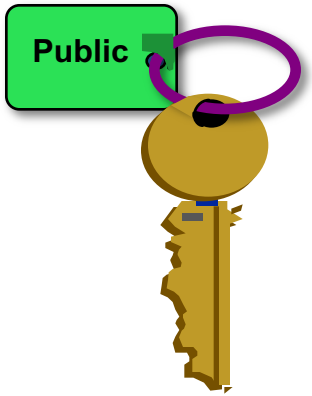
- You can **sign** data with the **private key** and **verify** the signature using the **public key**



keys

- Private key is kept SECRET.
- You **should** encrypt your private key with a **symmetric** passphrase.

- Public key is distributed.
- Anyone who needs to send you confidential data can use your public key



Signing & encrypting

- Data is encrypted with a public key to be decrypted with the corresponding private key.
- Data can be signed with the private key to be verified by anyone who has the corresponding public key.
- Since public keys are data they can be signed too.

use case

- email
  - encryption: to send confidential information
  - singing: to prove the message actually comes from you and is not modified during delivery
- file distribution
  - singing: to prove the contents is distributed by you and not modified since signed
  - you can generate separate signature file if needed
    - you have the original file and signature file for it

Installing GnuPG Software

- Core software either commercial from pgp or opensource from gnupg.
- https://www.gpg4win.org/ for windows
- https://www.gpgtools.org/ for OS X
- Your package manager for Linux/UNIX
- Source code from https://www.gnupg.org/
- we have hands-on later

Key management: generation

- Using graphical tools based on what you installed above:
  - GPG Keychain Access for OS X
  - Kleopatra or GPA for windows
- Using the command line:
  - `gpg --gen-key`
- Generate a key – use your email address. The comment field can be left blank.

Key management: distribution

- On printed media
  - published book or business cards:
- Digitally in email
- Online using the openpgp key servers.
  - https://pgp.mit.edu/
- Still does not tell you if you trust the key.

person and key(s)

- You don’t need to trust the person.
- What you need to check is the matching of the person and his/her public key(s)
  - You can ask passport and appropriate ID cards to confirm the person’s name which is usually included in the public key
  - And fingerprint of the key to check if the public key you have is actually the key which the person distributed

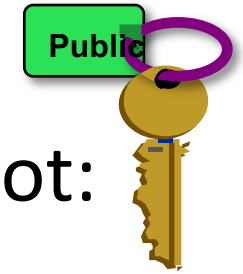
checking

Passport

JAPAN

finger-print: 8E 9C EC 04 87 6B ... 46 3B CB F7 72 CE

You got:

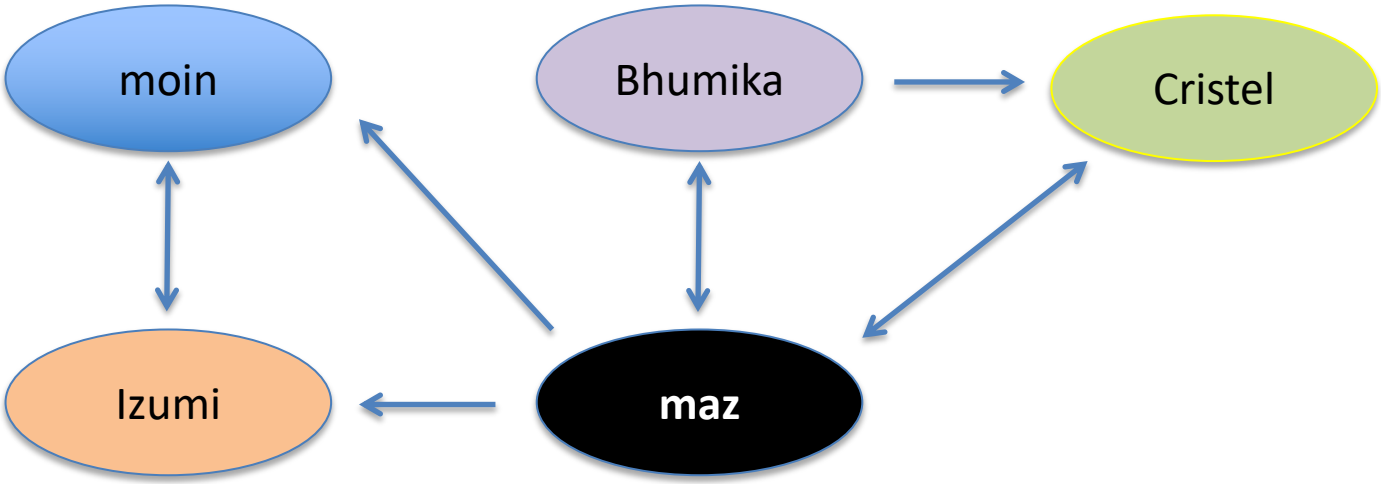


finger-print: 8E 9C EC 04 87 6B ... 46 3B CB F7 72 CE
uid: Matsuzaki Yoshinobu <maz@iij.ad.jp>

trust

- Centralized / hierarchal trust – where certain globally trusted bodies sign keys for every one else.
- Decentralized webs of trust – where you pick who you trust yourself, and decide if you trust who those people trust in turn.
- Which works better for what reasons?

Sample web of trust.



You can share your “trust information” by publishing others’ public keys with your pgp sign

Key management: rollover

- Expiry dates ensure that if your private key is compromised they can only be used till they expire.
- Can be changed after creating the key.
- Before expiry, you need to create a new key, sign it with the old one, send the signed new one to everyone in your web of trust asking them to sign your new key.

Key management: revocation

- Used to mark a key as invalid before its expiry date.
- Always generate a revocation certificate as soon as you create your key.
- Do not keep your revocation certificate with your private key.
  - `gpg --gen-revoke IDENTITY`

Key management: partying

- Key signing parties are ways to build webs of trust.
- Each participant carries identification, as well as a copy of their key fingerprint. (maybe some $ as well ☺)
- Each participant decides if they're going to sign another key based on their personal policy.
- Keys are easiest kept in a keyring on an openpgp keyserver in the aftermath of the party.

Interesting gpg commands

- Get help for gpg options
  - `gpg --help` AND `man gpg`
- Print the fingerprint of a particular key
  - `gpg --fingerprint IDENTITY`
- IDENTITY = email or PGP key ID
- Export a public key to an ASCII armored file.
  - `gpg -a --output my-public-key.asc --export IDENTIY`

Interesting gpg commands

- Import a key from a file into your keyring
  - `gpg --import  public.asc`
- Import a key from a keyserver
  - `gpg --recv-keys --keyserver hkp://keys.gnupg.net`
- Send your key to a keyserver
  - `gpg --send-keys --keyserver hkp://keys.gnupg.net`
- Sign a key
  - `gpg --sign-key IDENTITY`