Pretty Good Privacy

General Principles

Historical Overview

- Invented by Zimmermann as *guerrilla freeware*
- Commercially restricted by RSA patent and US Government export restrictions
- PGP Classic (V2.6) uses RSA and IDEA
- Patent free version uses DSS, Diffie-Hellman and 3DES
- IETF designed its own “Open PGP”

PGP Overview

- PGP works for mail and data files
- Based on public key cryptography
- PGP fingerprint is cryptographic hash of public key
- PGP allows an informal PKI on the anarchy model
- Certificates are an option in PGP PKI

PGP PKI

- PGP users may certify others
- Trust in a chain is at discretion of user
- PGP asks for a rating on
  - legitimacy of a particular key
  - degree of trust in owner when acting as an issuer of key certificates

Coding Efficiency PEM v PGP

- PEM encodes non text to prevent alteration by mail infrastructure – 33% expansion
- Further encoding (e.g. following encryption) adds another 33% (78% in total)
- PGP allows user to specify text or data
- PGP uses ZIP utility for compression

Certificates and Key Revocation

- Certificates may have expiry date but current practice in PGP is to omit expiry date
- Keys may be revoked as well as certificates
- All revocations distributed informally

Private Keys in PGP

- Required for generating signatures or for receiving encrypted mail
- PGP generates private keys on request
- Private key supplied encrypted under IDEA key also generated in registration process

Key Rings

- Key ring is a data structure containing public keys, information on holders and certificates
- PGP allows 3 levels of trust
  - complete, partial and none
- A “completely trusted” individual signs a “completely trusted” certificate
- PGP computes level of trust in keys from information supplied