# Cryptography and Network Security Chapter 15

Fourth Edition
by William Stallings

Lecture slides by Lawrie Brown

# Chapter 15 – Electronic Mail Security

*Despite the refusal of VADM Poindexter and LtCol North to appear, the Board's access to other sources of information filled much of this gap. The FBI provided documents taken from the files of the National Security Advisor and relevant NSC staff members, including messages from the PROF system between VADM Poindexter and LtCol North. The PROF messages were conversations by computer, written at the time events occurred and presumed by the writers to be protected from disclosure. In this sense, they provide a first-hand, contemporaneous account of events.*

**—The Tower Commission Report to President Reagan on the Iran-Contra Affair, 1987**

# Email Security

- email is one of the most widely used and regarded network services

- currently message contents are not secure
  - may be inspected either in transit
  - or by suitably privileged users on destination system

# Email Security Enhancements

- confidentiality
  - protection from disclosure
- authentication
  - of sender of message
- message integrity
  - protection from modification
- non-repudiation of origin
  - protection from denial by sender
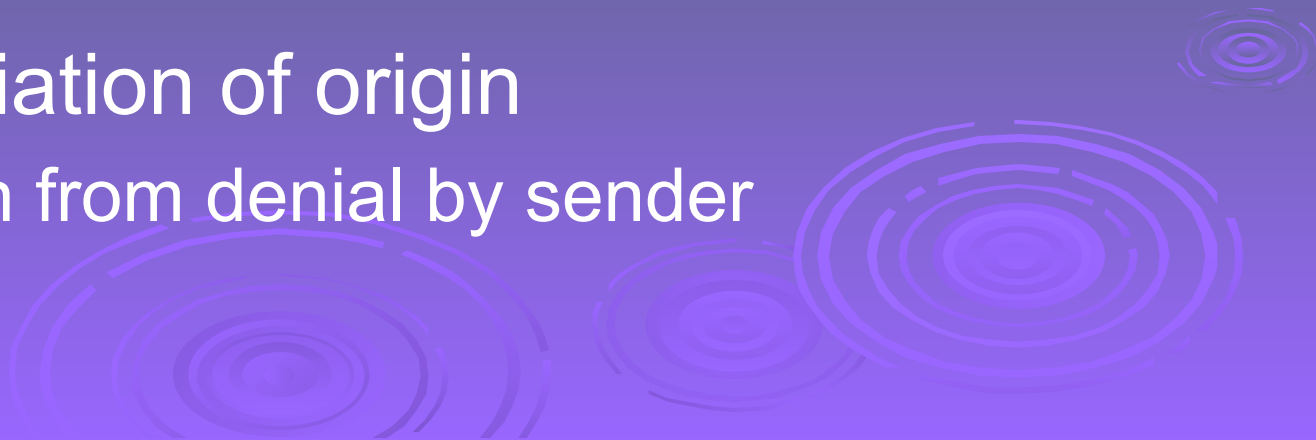
# Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- selected best available crypto algs to use
- integrated into a single program
- on Unix, PC, Macintosh and other systems
- originally free, now also have commercial versions available

# PGP Operation – Authentication

1. sender creates message
2. use SHA-1 to generate 160-bit hash of message
3. signed hash with RSA using sender's private key, and is attached to message
4. receiver uses RSA with sender's public key to decrypt and recover hash code
5. receiver verifies received message using hash of it and compares with decrypted hash code

# PGP Operation – Confidentiality

1. sender generates message and 128-bit random number as session key for it
2. encrypt message using CAST-128 / IDEA / 3DES in CBC mode with session key
3. session key encrypted using RSA with recipient's public key, & attached to msg
4. receiver uses RSA with private key to decrypt and recover session key
5. session key is used to decrypt message

# PGP Operation – Confidentiality & Authentication

 can use both services on same message
- create signature & attach to message
- encrypt both message & signature
- attach RSA/ElGamal encrypted session key

# PGP Operation – Compression

- by default PGP compresses message after signing but before encrypting
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic
- uses ZIP compression algorithm

# PGP Operation – Email Compatibility

☐ when using PGP will have binary data to send (encrypted message etc)

☐ however email was designed only for text

☐ hence PGP must encode raw binary data into printable ASCII characters

☐ uses radix-64 algorithm

  • maps 3 bytes to 4 printable chars

  • also appends a CRC

☐ PGP also segments messages if too big

# PGP Operation – Summary
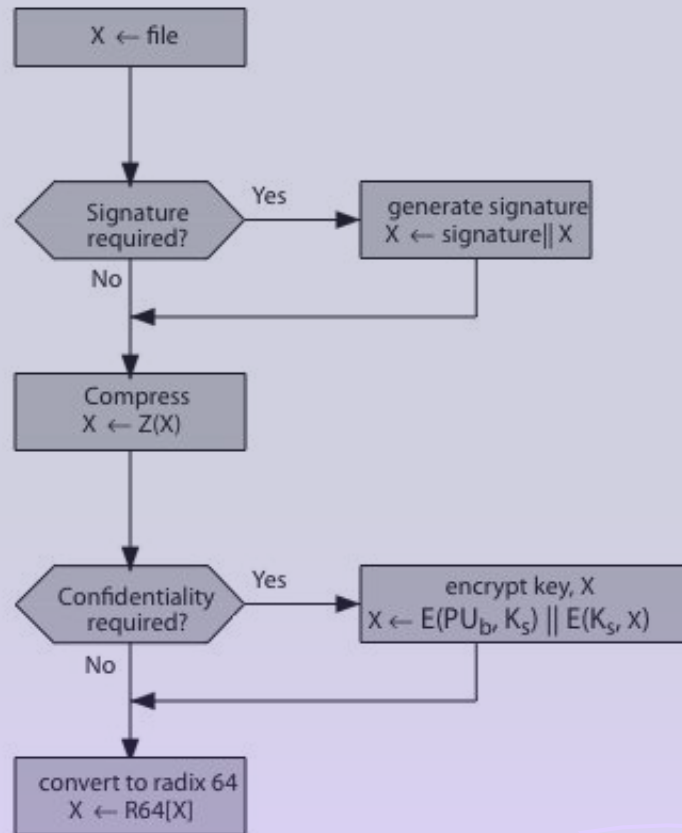


(a) Generic Transmission Diagram (from A)
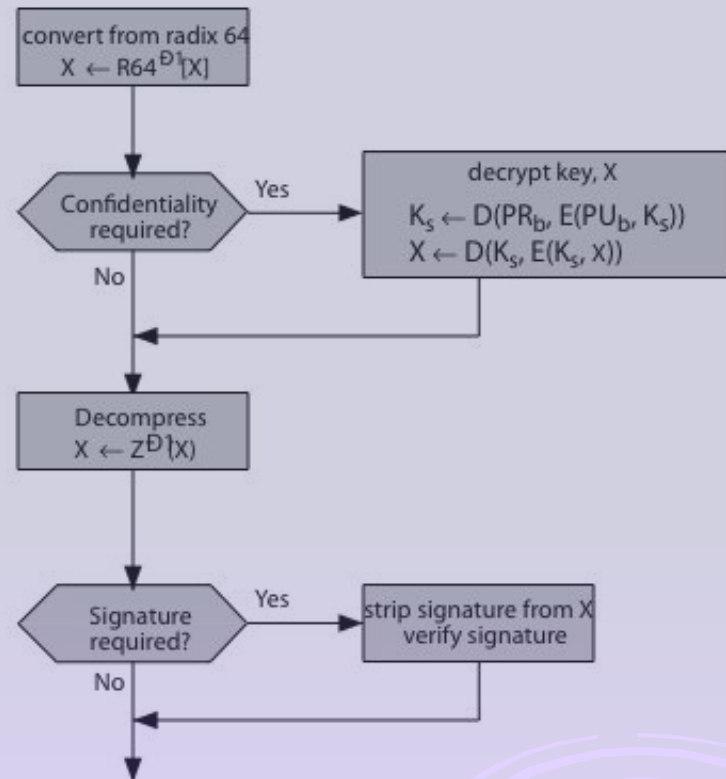
(b) Generic Reception Diagram (to B)

# PGP Session Keys

- need a session key for each message
  - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- generated using ANSI X12.17 mode
- uses random inputs taken from previous uses and from keystroke timing of user

# PGP Public & Private Keys

- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
  - could send full public-key with every message
  - but this is inefficient
- rather use a key identifier based on key
  - is least significant 64-bits of the key
  - will very likely be unique
- also use key ID in signatures

# PGP Message Format
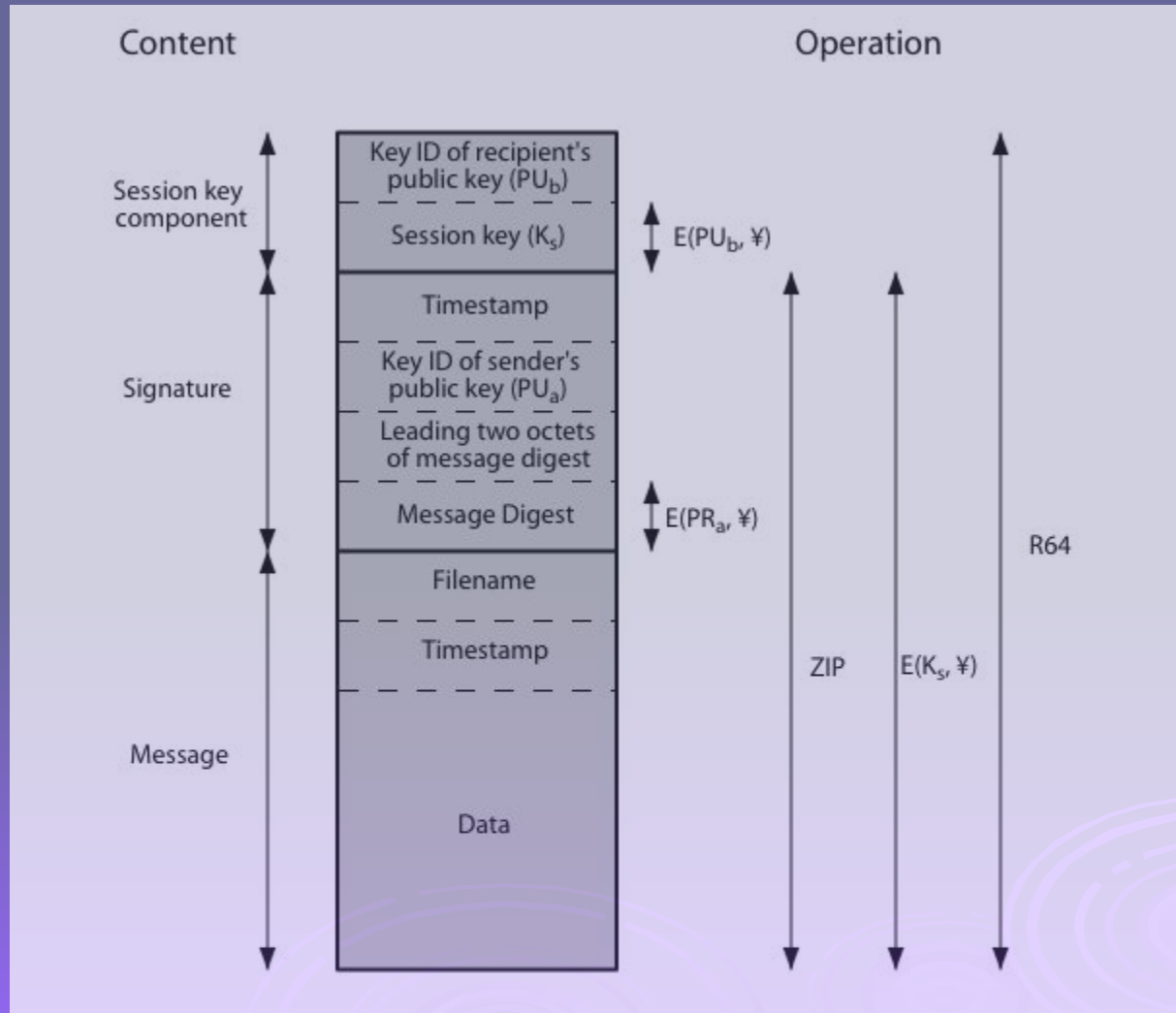
# PGP Key Rings

- each PGP user has a pair of keyrings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase
- security of private keys thus depends on the pass-phrase security

# PGP Message Generation
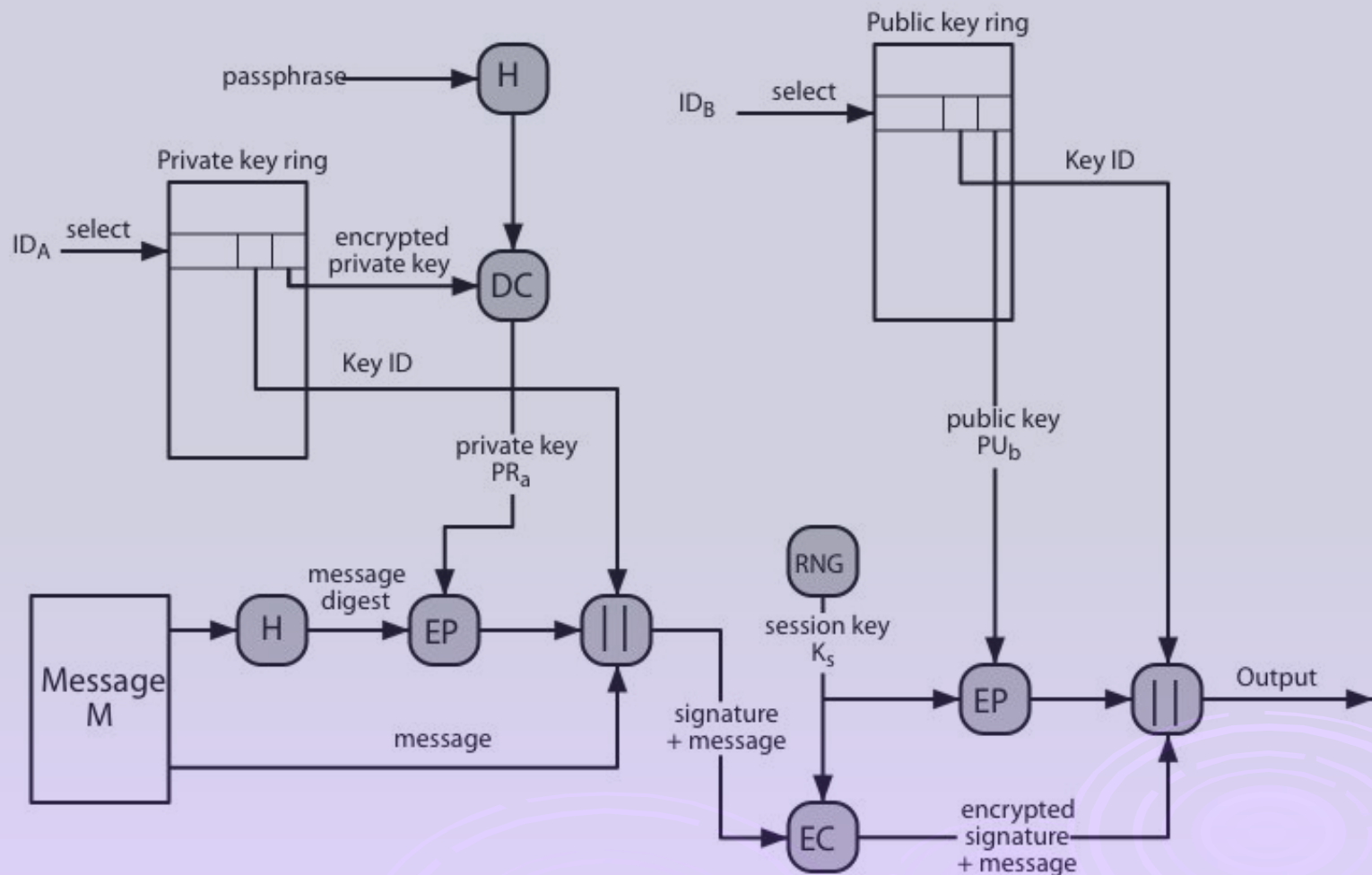
# PGP Message Reception
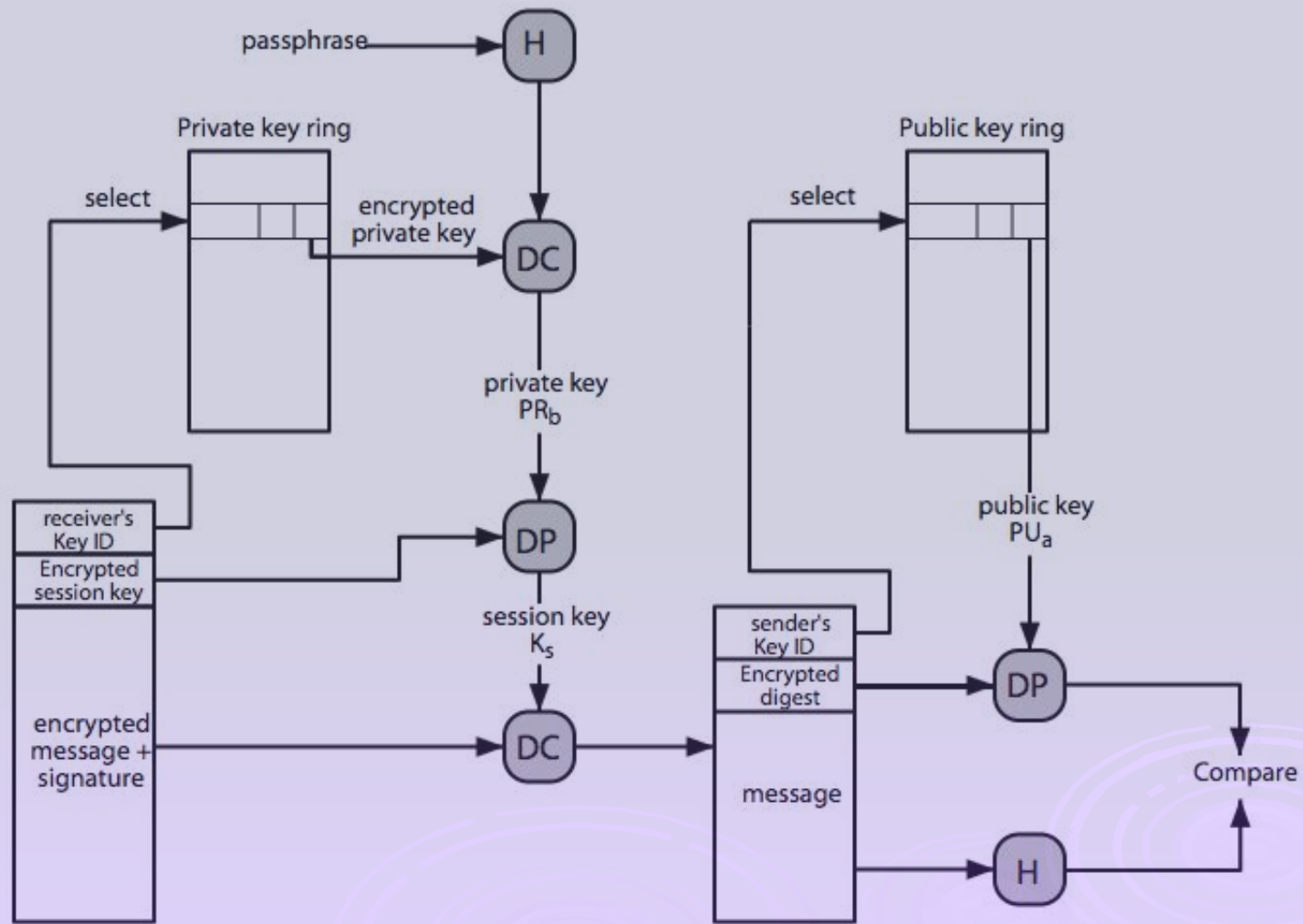
# PGP Key Management

- rather than relying on certificate authorities
- in PGP every user is own CA
  - can sign keys for users they know directly
- forms a "web of trust"
  - trust keys have signed
  - can trust keys others have signed if have a chain of signatures to them
- key ring includes trust indicators
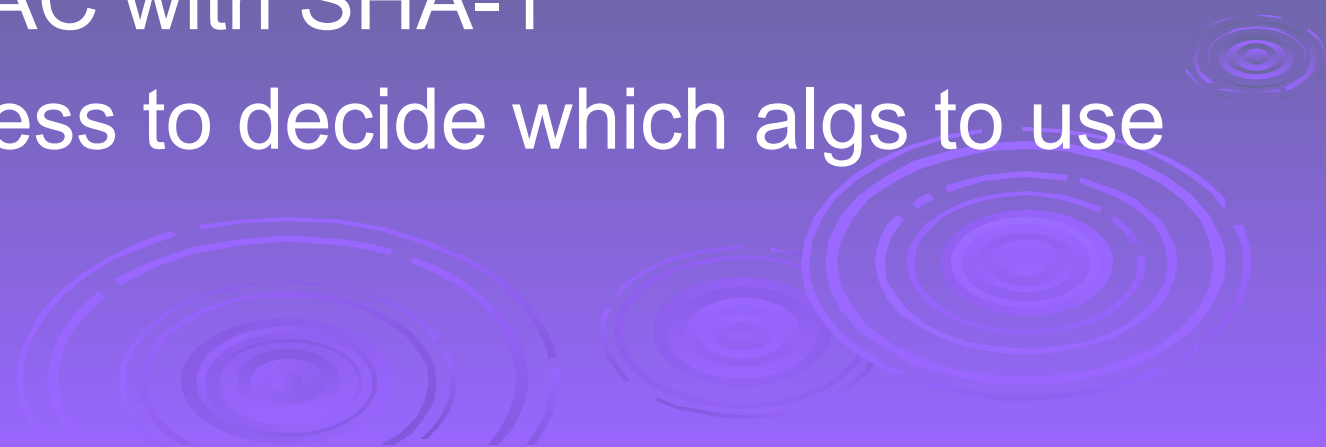- users can also revoke their keys

# S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
    - original Internet RFC822 email was text only
    - MIME provided support for varying content types and multi-part messages
    - with encoding of binary data to textual form
    - S/MIME added security enhancements
- have S/MIME support in many mail agents
    - eg MS Outlook, Mozilla, Mac Mail etc

# S/MIME Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

# S/MIME Cryptographic Algorithms

- digital signatures: DSS & RSA
- hash functions: SHA-1 & MD5
- session key encryption: ElGamal & RSA
- message encryption: AES, Triple-DES, RC2/40 and others
- MAC: HMAC with SHA-1
- have process to decide which algs to use

# S/MIME Messages

- S/MIME secures a MIME entity with a signature, encryption, or both
- forming a MIME wrapped PKCS object
- have a range of content-types:
  - enveloped data
  - signed data
  - clear-signed data
  - registration request
  - certificate only message

# S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's

# Certificate Authorities

- have several well-known CA's
- Verisign one of most widely used
- Verisign issues several types of Digital IDs
- increasing levels of checks & hence trust

| Class | Identity Checks | Usage |
|-------|-----------------|-------|
| 1 | name/email check | web browsing/email |
| 2 | + enroll/addr check | email, subs, s/w validate |
| 3 | + ID documents | e-banking/service access |

# Summary

* have considered:
  * secure email
  * PGP
  * S/MIME