Unit IV

Electronic Mail Security- S/MIME

Noor Mohd
Graphic Era Deemed to be University Dehradun

Outline

- E-mail security
  - Pretty good privacy
  - S/MIME

Email Security

- Protocols:
- Simple Mail Transfer Protocol (SMTP):
  - Textbased commands for forwarding email between UAMSA (mail submission agent)
  - MSAMTA, MTAMTA, MTAMDA (mail delivery agent)
  - Message Transfer Agent: Node whereby mail is forwarded to another node
  - User Agent: the email client Node where mail is processed

- Internet Message Access Protocol (IMAP):
  - Allows UA to access mail stored by MDA.
  - Supports Several clients can be connected to the same mailbox
  - Separate retrieval of MIME parts of a message (e.g. attachment)
  - IMAP over SSL (IMAPS)
- Post Office Protocol:
  - Another popular mail retrieval protocol.
  - Client connects, gets email, deletes messages on server
  - One client can connect at a time
  - POP3 over SSL (POP3S)

Pretty Good Privacy

- PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

Why Is PGP Popular?

- It is availiable free on a variety of platforms.
- Based on well known algorithms.
- Wide range of applicability
- Not developed or controlled by governmental or standards organizations

five services

- Consist of five services:
  - Authentication
  - Confidentiality
  - Compression
  - E-mail compatibility
  - Segmentation

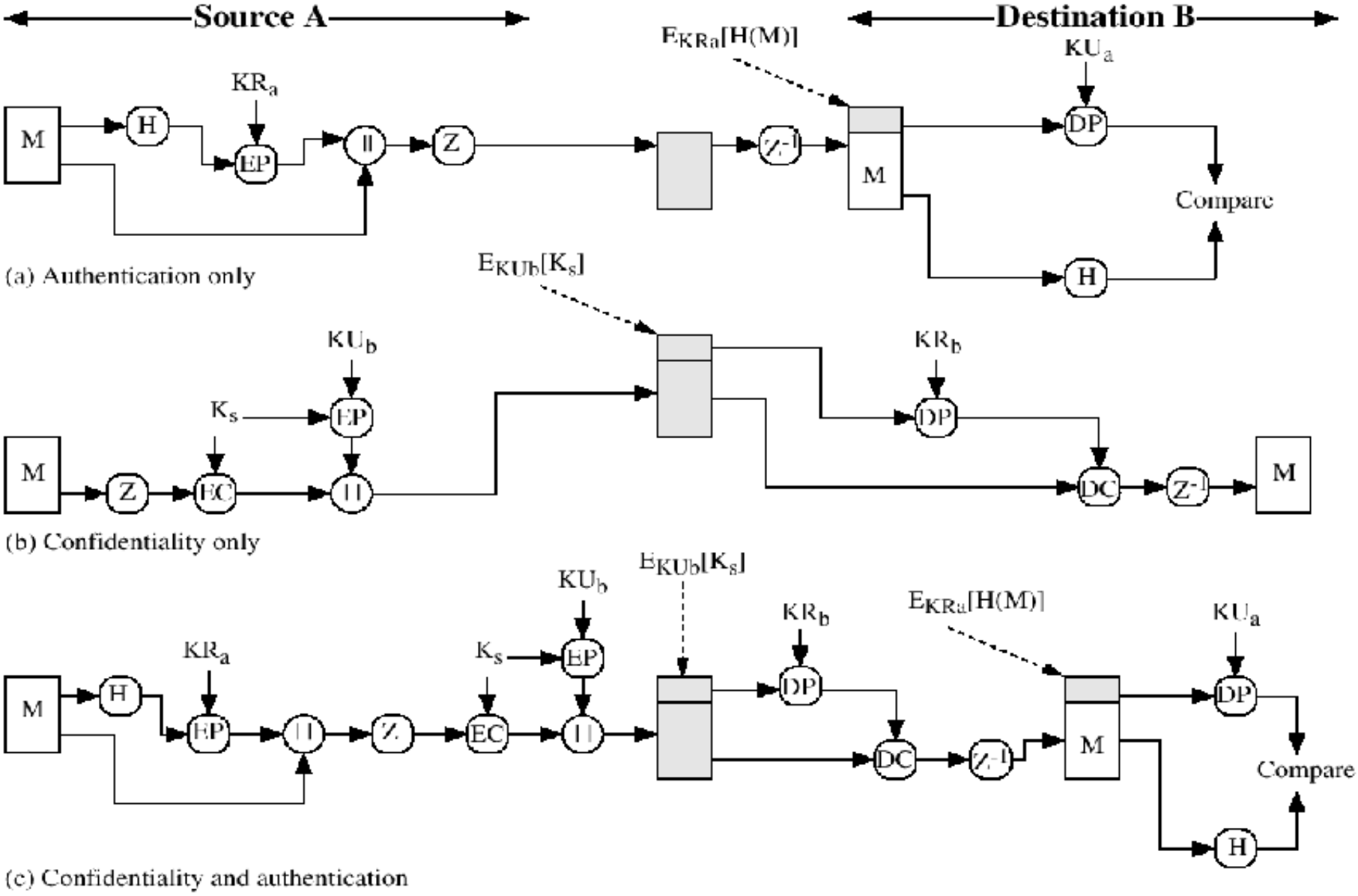

Figure 5.1 PGP Cryptographic Functions

Compression

- PGP compresses the message after applying the signature but before encryption
- The placement of the compression algorithm is critical.
- The compression algorithm used is ZIP (described in appendix 5A)

E-mail Compatibility

- The scheme used is radix-64 conversion.
- The use of radix-64 expands the message by 33%.

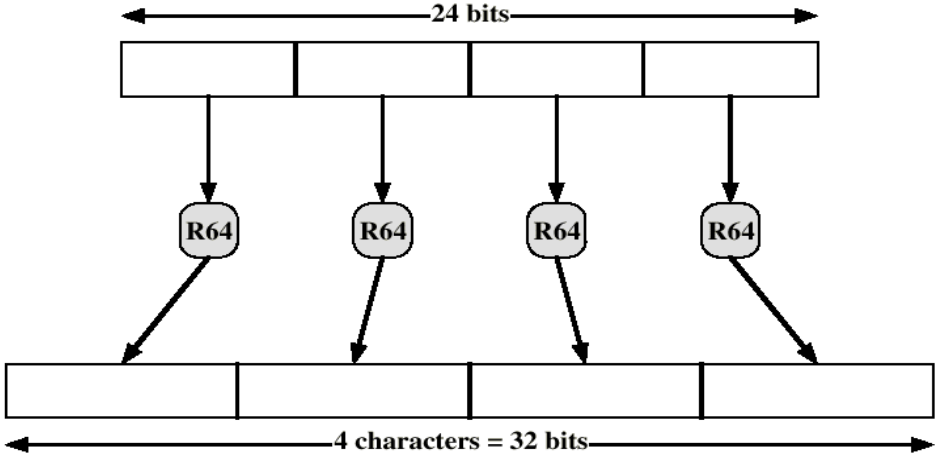

Figure 5.11 Printable Encoding of Binary Data into Radix-64 Format

Segmentation and Reassembly

- Often restricted to a maximum message length of 50,000 octets.
- Longer messages must be broken up into segments.
- PGP automatically subdivides a message that is to large.
- The receiver strip of all e-mail headers and reassemble the block.

Sumary of PGP Services

Function	Algorithm Used
Digital Signature	DSS/SHA or RSA/SHA
Message Encryption	CAST or IDEA or three-key triple DES with Diffie-Hellman or RSA
Compression	ZIP
E-mail Compatibility	Radix-64 conversion
Segmentation	

S/MIME

- Secure/Multipurpose Internet Mail Extension
- S/MIME will probably emerge as the industry standard.
- PGP for personal e-mail security

Simple Mail Transfer Protocol (SMTP, RFC 822)

- RFC 822 defines a format for text messages that are sent using electronic mail.
- **SMTP Limitations - Can not transmit, or has a problem with:**
  - executable files, or other binary files (jpeg image)
  - “national language” characters (non-ASCII)
  - messages over a certain size
  - ASCII to EBCDIC translation problems
  - lines longer than a certain length (72 to 254 characters)

Header fields in MIME

- **MIME-Version:** Must be “1.0” -> RFC 2045, RFC 2046
- **Content-Type:** More types being added by developers (application/word)
- **Content-Transfer-Encoding:** How message has been encoded (radix-64)
- **Content-ID:** Unique identifying character string.
- **Content Description:** Needed when content is not readable text (e.g.,mpeg)

S/MIME Functions

- **Enveloped Data:** Encrypted content and encrypted session keys for recipients.
- **Signed Data:** Message Digest encrypted with private key of "signer."
- **Clear-Signed Data:** Signed but not encrypted.
- **Signed and Enveloped Data:** Various orderings for encrypting and signing.

Algorithms Used

- **Message Digesting:** SHA-1 and MDS
- **Digital Signatures:** DSS
- **Secret-Key Encryption:** Triple-DES, RC2/40 (exportable)
- **Public-Private Key Encryption:** RSA with key sizes of 512 and 1024 bits, and Diffie-Hellman (for session keys).

User Agent Role

- S/MIME uses Public-Key Certificates - X.509 version 3 signed by Certification Authority
- Functions:
  - **Key Generation** - Diffie-Hellman, DSS, and RSA key-pairs.
  - **Registration** - Public keys must be registered with X.509 CA.
  - **Certificate Storage** - Local (as in browser application) for different services.
  - **Signed and Enveloped Data** - Various orderings for encrypting and signing.