CHAPTER - 7

ELECTRONIC MAIL SECURITY

7.1 PRETTY GOOD PRIVACY

- **KEY POINTS**
- PGP is an open-source, freely available software package for e-mail security.
- It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
- PGP incorporates tools for developing a public-key trust model and public-key certificate management.
- S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.
- DKIM is a specification used by e-mail providers for cryptographically signing e-mail messages on behalf of the source domain.

7.1 PRETTY GOOD PRIVACY

- PGP is the effort of a single person, Phil Zimmermann, PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
- In essence, Zimmermann has done the following:
  - Selected the best available cryptographic algorithms
  - Integrated these algorithms into a general-purpose application
  - Made the package and its documentation, including the source code, freely available
  - Entered into an agreement with a company to provide a fully compatible, low-cost commercial version of PGP

CONTINUE…

- PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth
  - It is available free worldwide and is used on all platforms. The commercial version comes with a vendor support.
  - It is based on algorithms that extremely secure and are public reviewed. Like RSA, DSS, Deffie-Hellman, etc for Public key encryption and CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.
  - It has a wide range of applicability from corporations to individuals wanting to communicate worldwide securly.
  - It was not developed by, nor is it controlled by, any governmental or standards organization
  - PGP is now on an Internet standards track (RFC 3156; *MIME Security with OpenPGP)*

CONTINUE…

Notation

- K= session key used in symmetric encryption scheme
- PRa= private key of user A, used in public-key encryption scheme
- PUb= public key of user A, used in public-key encryption scheme
- EP= public-key encryption
- DP= public-key decryption
- EC= symmetric encryption
- DC= symmetric decryption
- H= hash function
- ||= concatenation
- Z= compression using ZIP algorithm
- R64= conversion to radix 64 ASCII format

❑ OPERATIONAL DESCRIPTION

- PGP provide following services
  - Authentication
  - Confidentiality
  - Compression
  - e-mail compatibility

❑ Authentication

- The sequence is as follows.
  - 1. The sender creates a message.
  - 2. SHA-1 is used to generate a 160-bit hash code of the message.
  - 3. The hash code is encrypted with RSA using the sender’s private key, and the result is prepended to the message.
  - 4. The receiver uses RSA with the sender’s public key to decrypt and recover the hash code.
  - 5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic.

Authentication

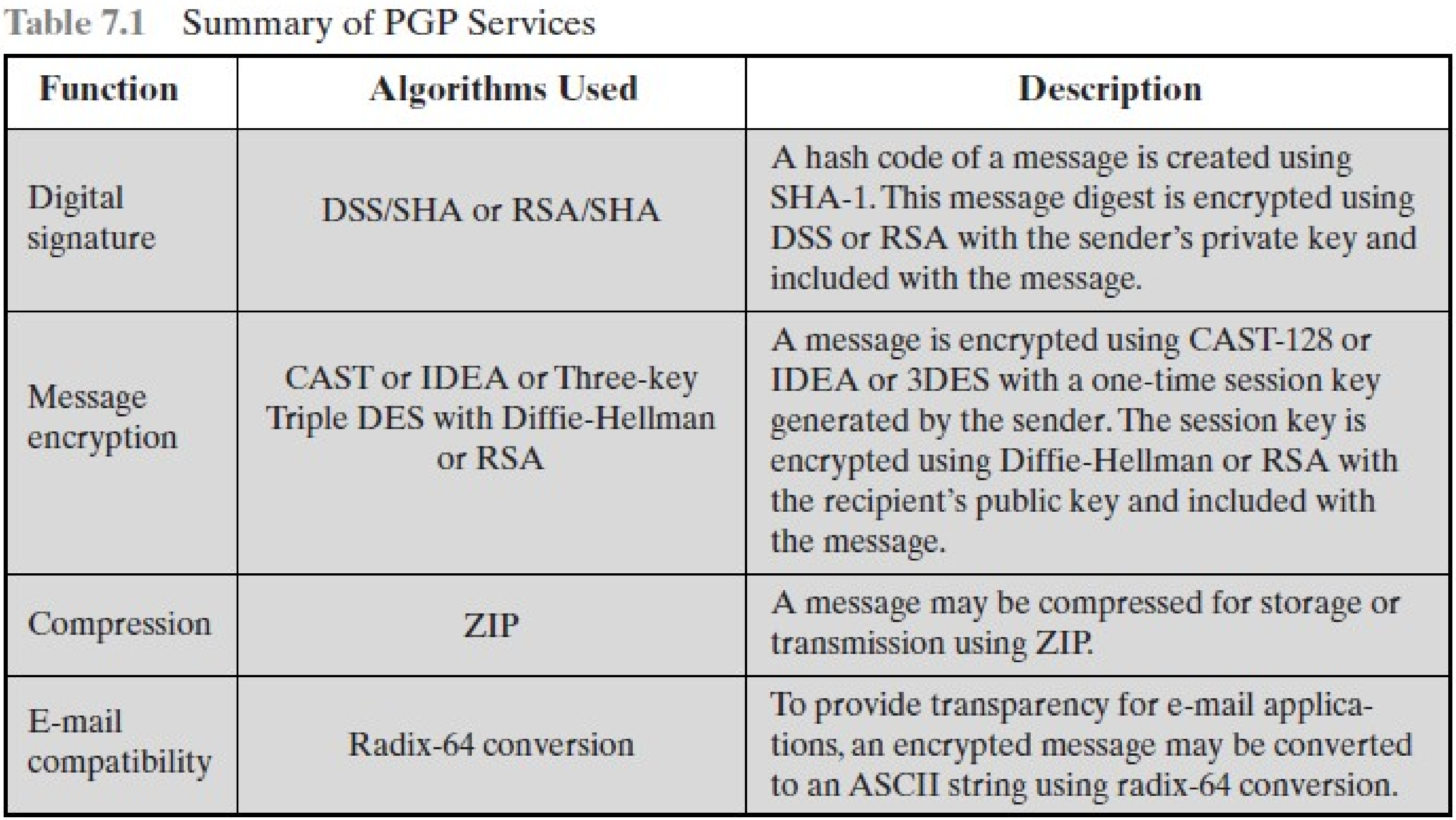


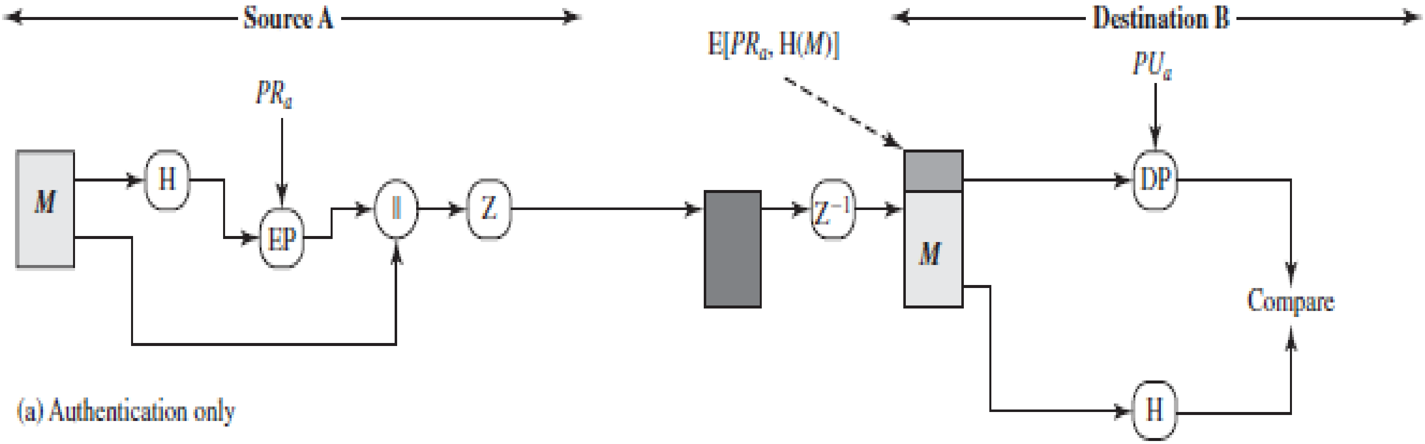
Table 7.1 Summary of PGP Services

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

❑Authentication

- The combination of SHA-1 and RSA provides an effective digital signature scheme.
- Because of the strength of RSA, the recipient is assured
  - that only the possessor of the matching private key can generate the signature.
  - And that, the recipient is assured that no one else could generate a new message that matches the hash code and, hence, the signature of the original message.
- As an alternative, signatures can be generated using DSS/SHA-1.
- Signature are appended with the messages in most of the cases but sometimes. E.g. when more than one parties need to sign a contract, a detached signature is made and trasnmitted separately.

❑ AUTHENTICATION



(a) Authentication only

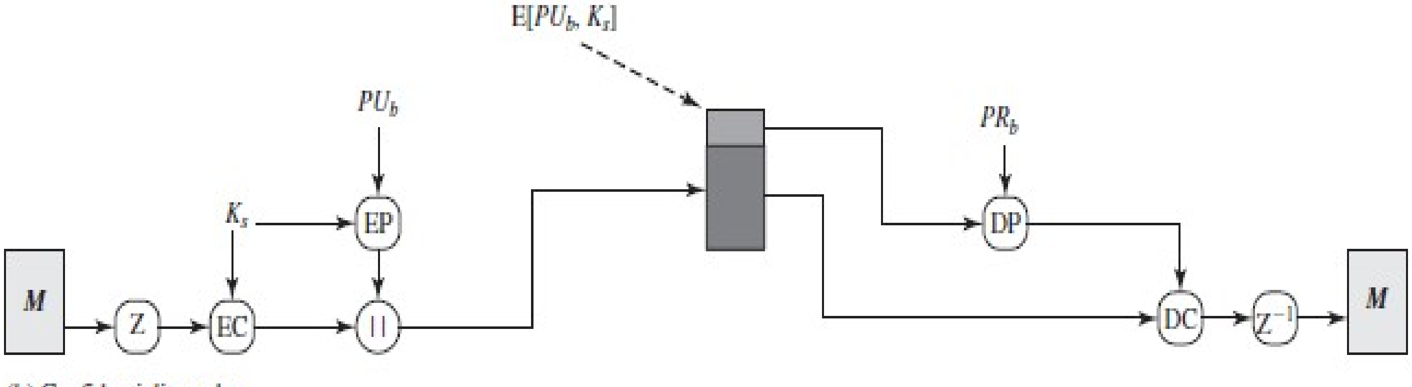
❑Confidentiality

- Confidentiality is provided by encrypting messages to be transmitted or to be stored locally as files.
- In both cases, the symmetric encryption algorithm CAST-128 may be used.
- Alternatively, IDEA or 3DES may be used. The 64-bit cipher feedback (CFB) mode is used.
- **Key Distribution**
- A new symmetric key is generated as a random 128-bit number for each message, also called session key or one-time key.
- Session key is bounded with the message and transmitted. Its secured by receiver’s public key.

❑Confidentiality

- Following figure illustrates the sequence, which can be described as follows.
- 1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
- 2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
- 3. The session key is encrypted with RSA using the recipient’s public key and is prepended to the message.
- 4. The receiver uses RSA with its private key to decrypt and recover the session key.
- 5. The session key is used to decrypt the message.
- As an alternative to the use of RSA for key encryption, PGP provides an option referred to as Diffie-Hellman.

❑ CONFIDENTIALITY

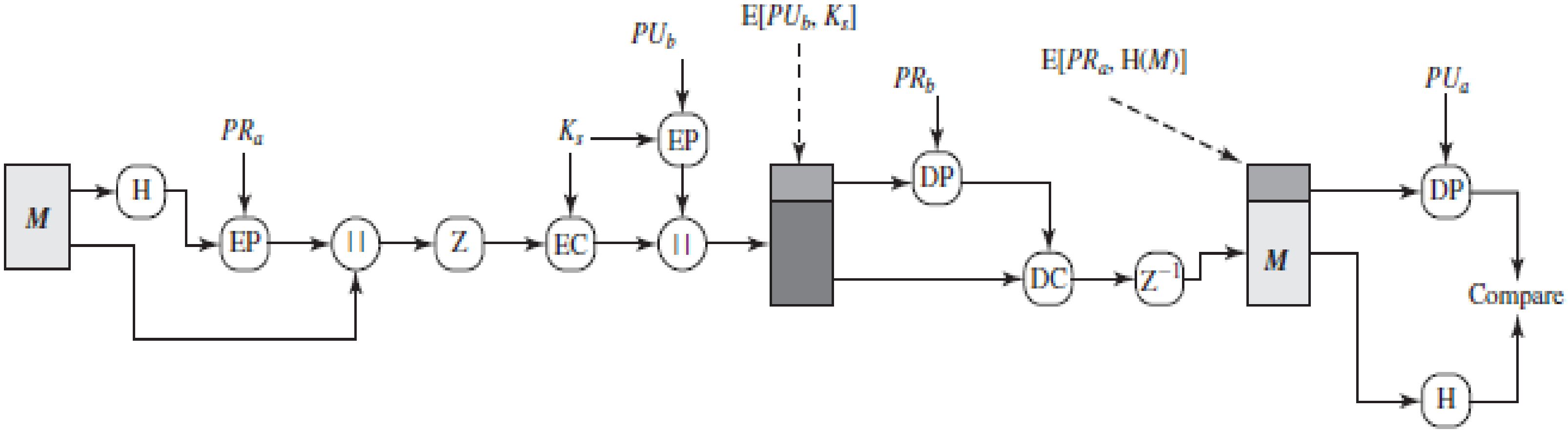


(b) Confidentiality only

❑Confidentiality and Authentication

- Both services may be used for the same message.
- First, a signature is generated for the plaintext message and prepended to the message.
- Then the plaintext message plus signature is encrypted using CAST-128 (or IDEA or 3DES), and the session key is encrypted using RSA (or ElGamal).
- Alternatively, the message can be encrypted first and then signature can be generated but note preferable if third party verification is to be done.

❑ CONFIDENTIALITY AND AUTHENTICATION



(c) Confidentiality and authentication