

Electronic mail security

Dr KARTHIKEYAN A
Assistant Professor/ECE
SNS College of Technology

Why Is PGP Popular?

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

Operational Description

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

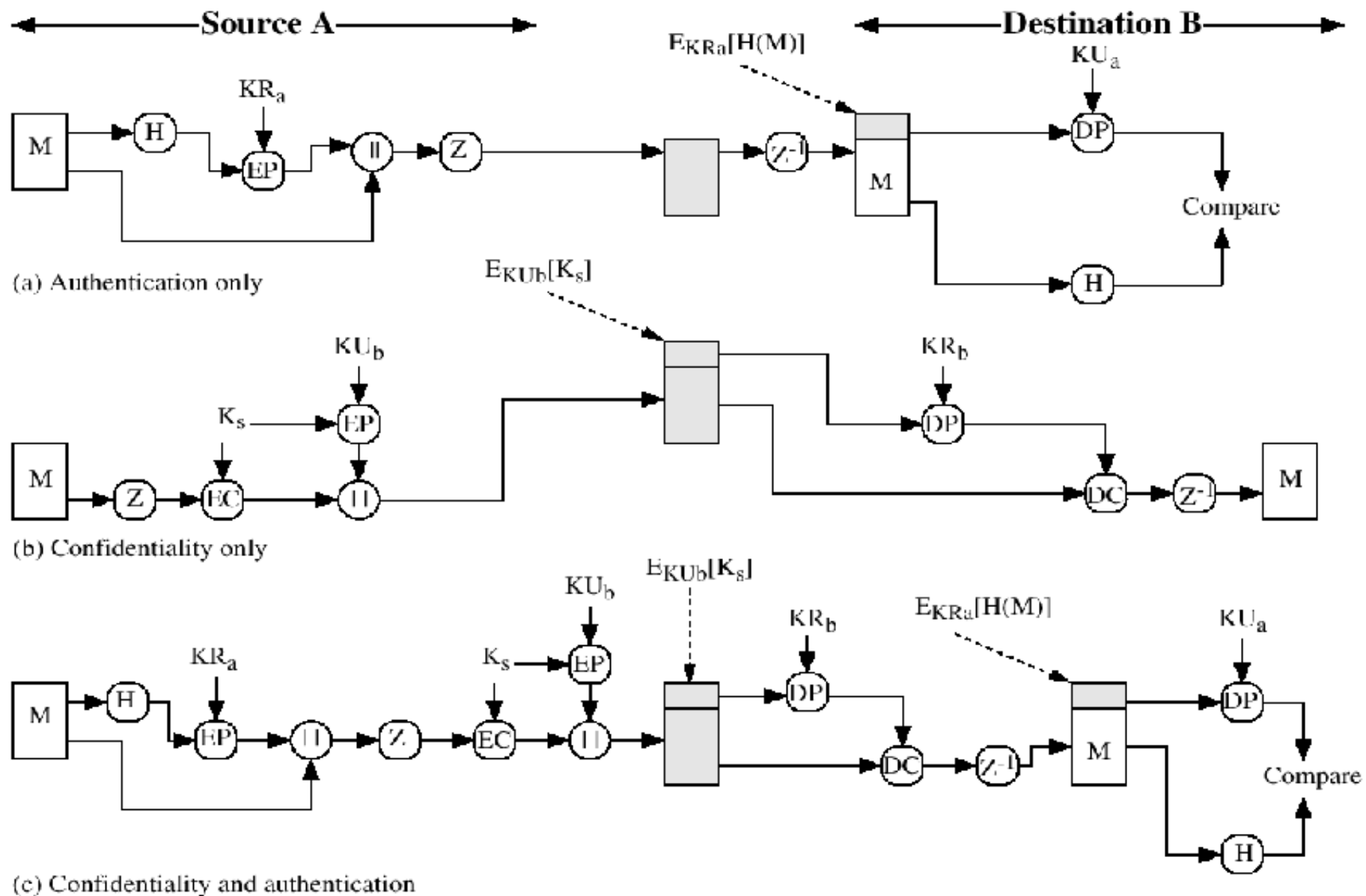


Figure 5.1 PGP Cryptographic Functions

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 (see appendix 5B).
- The use of radix-64 expands the message by 33%

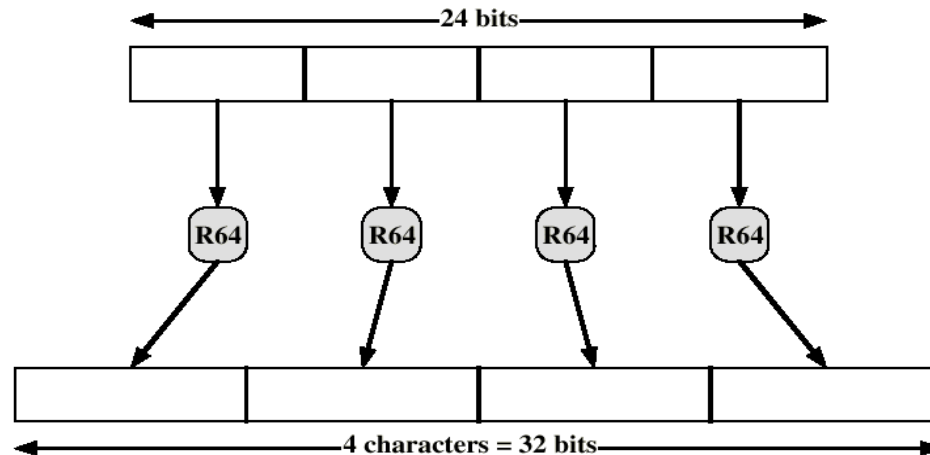


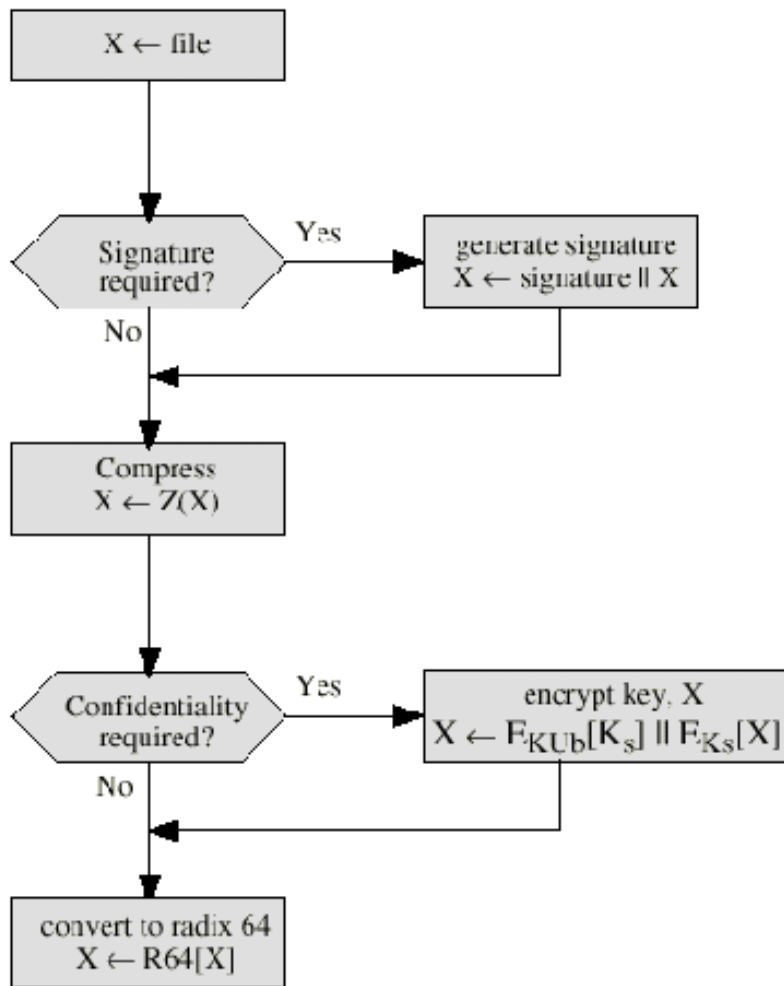
Figure 5.11 Printable Encoding of Binary Data into Radix-64 Format

Segmentation and Reassembly

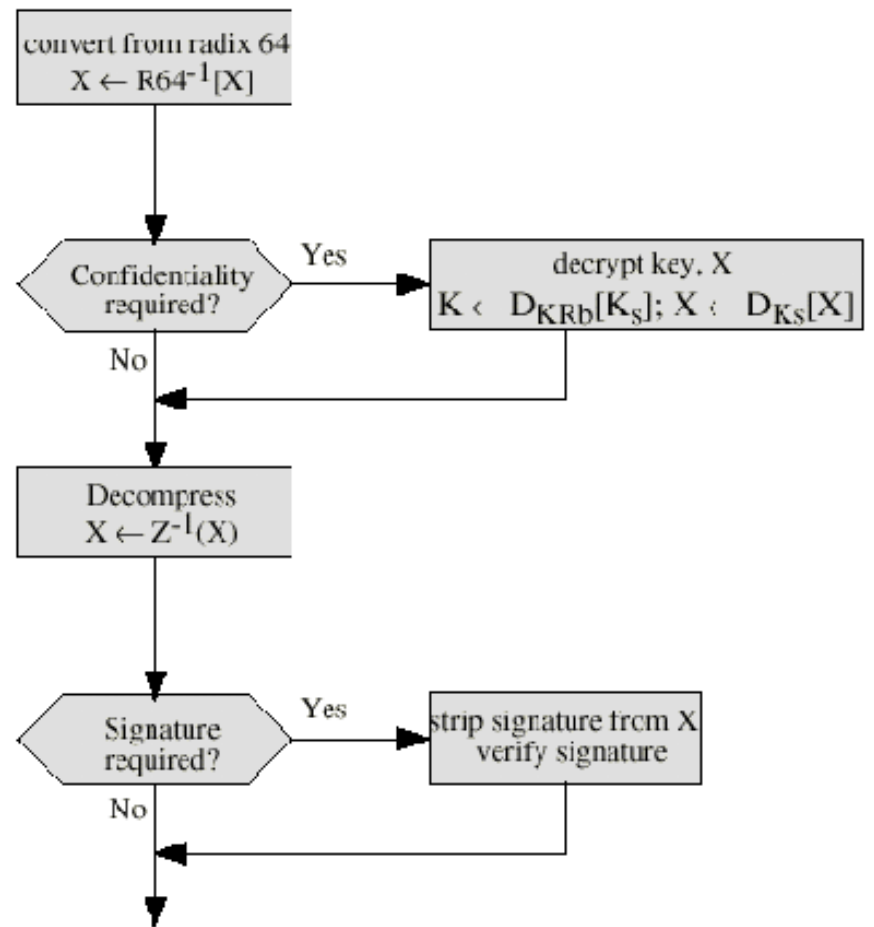
- Often restricted to a maximum message length of 50,000 octets.
- Longer messages must be broken up into segments.
- PGP automatically subdivides a message that is too large.
- The receiver strips off all e-mail headers and reassembles the block.

Summary 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	-



(a) Generic Transmission Diagram (from A)



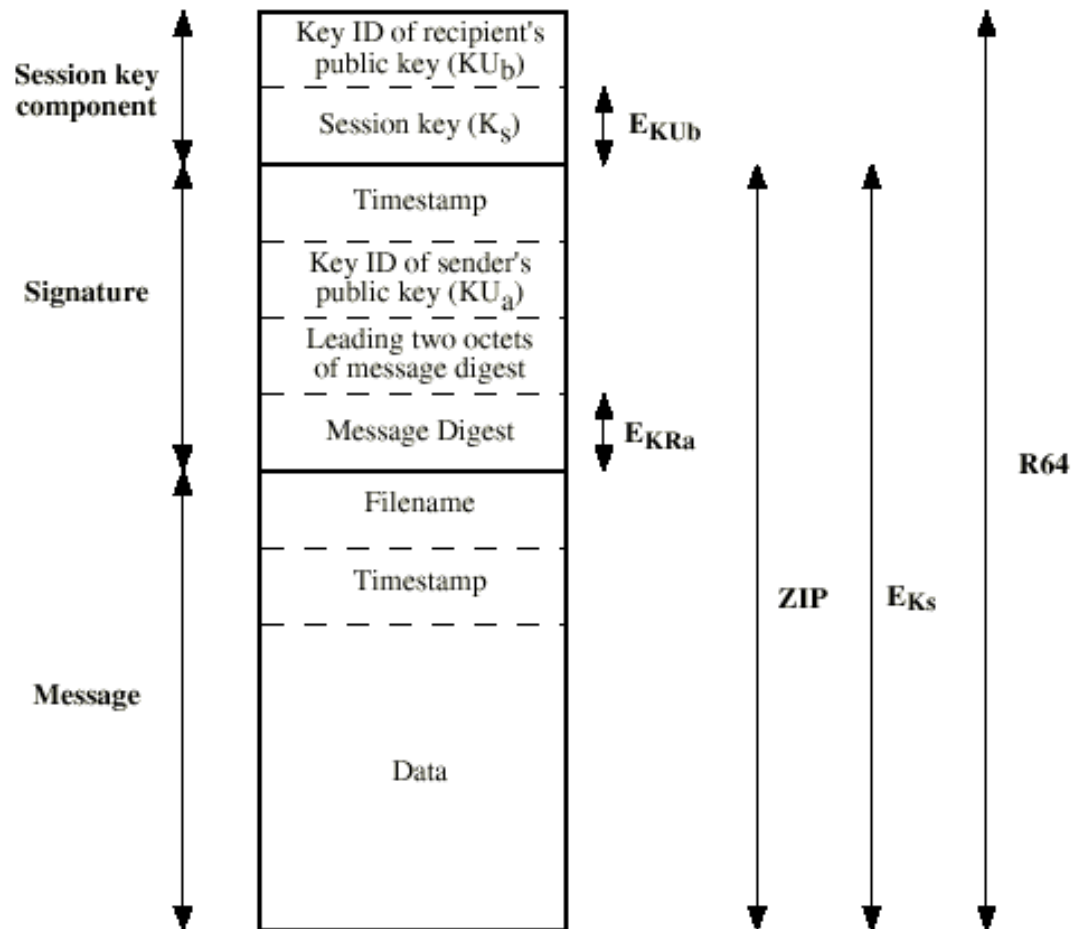
(b) Generic Reception Diagram (to B)

Figure 5.2 Transmission and Reception of PGP Messages

Format of PGP Message

Content

Operation



Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
.
.
.
T_i	$KU_j \bmod 2^{64}$	KU_i	$E_{H(P_i)}[KR_i]$	User i
.
.
.

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
.
.
.
T_i	$KU_j \bmod 2^{64}$	KU_i	trust_flagi	User i	trust_flagj		
.
.
.

* = field used to index table

Figure 5.4 General Structure of Private and Public Key Rings

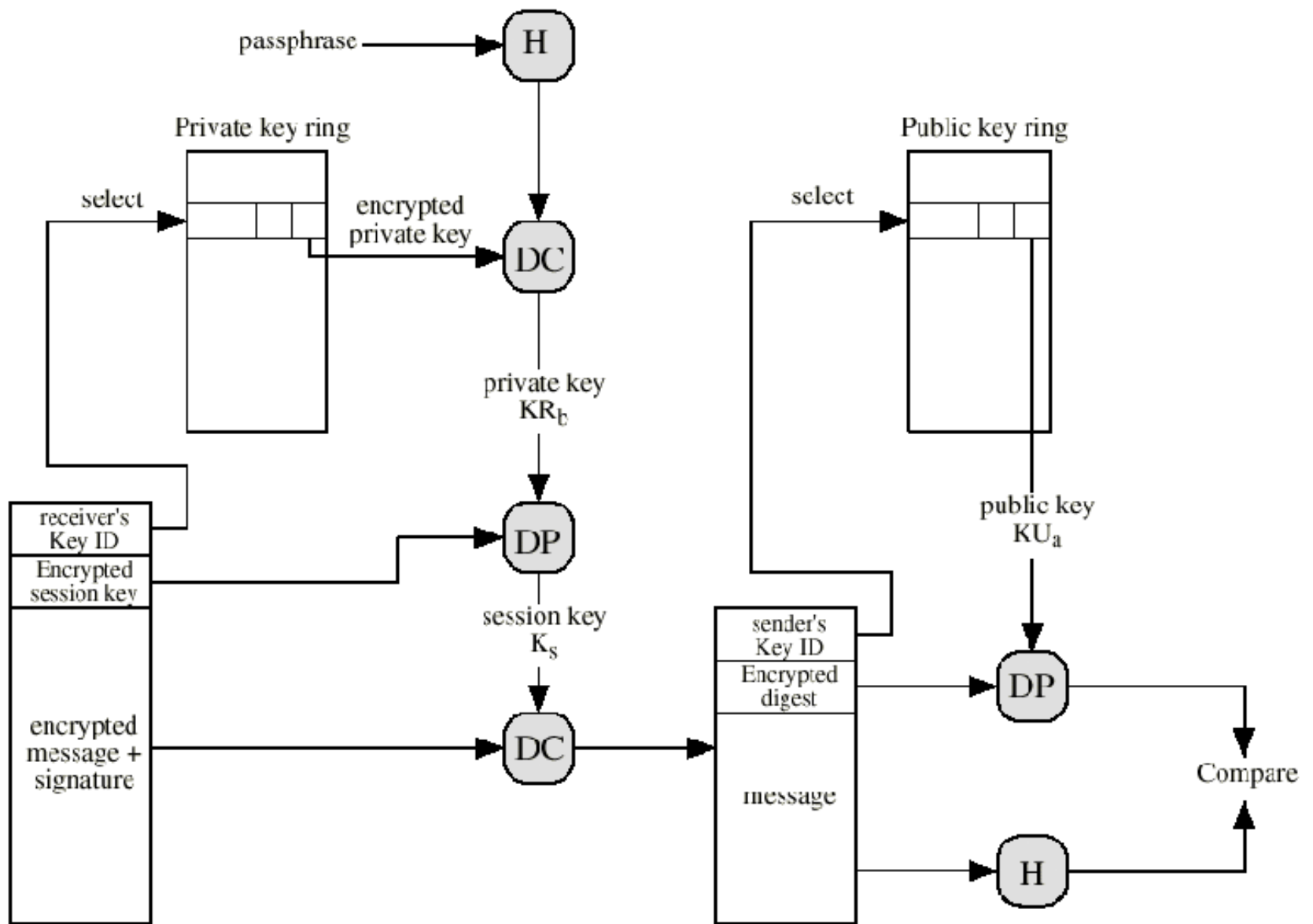
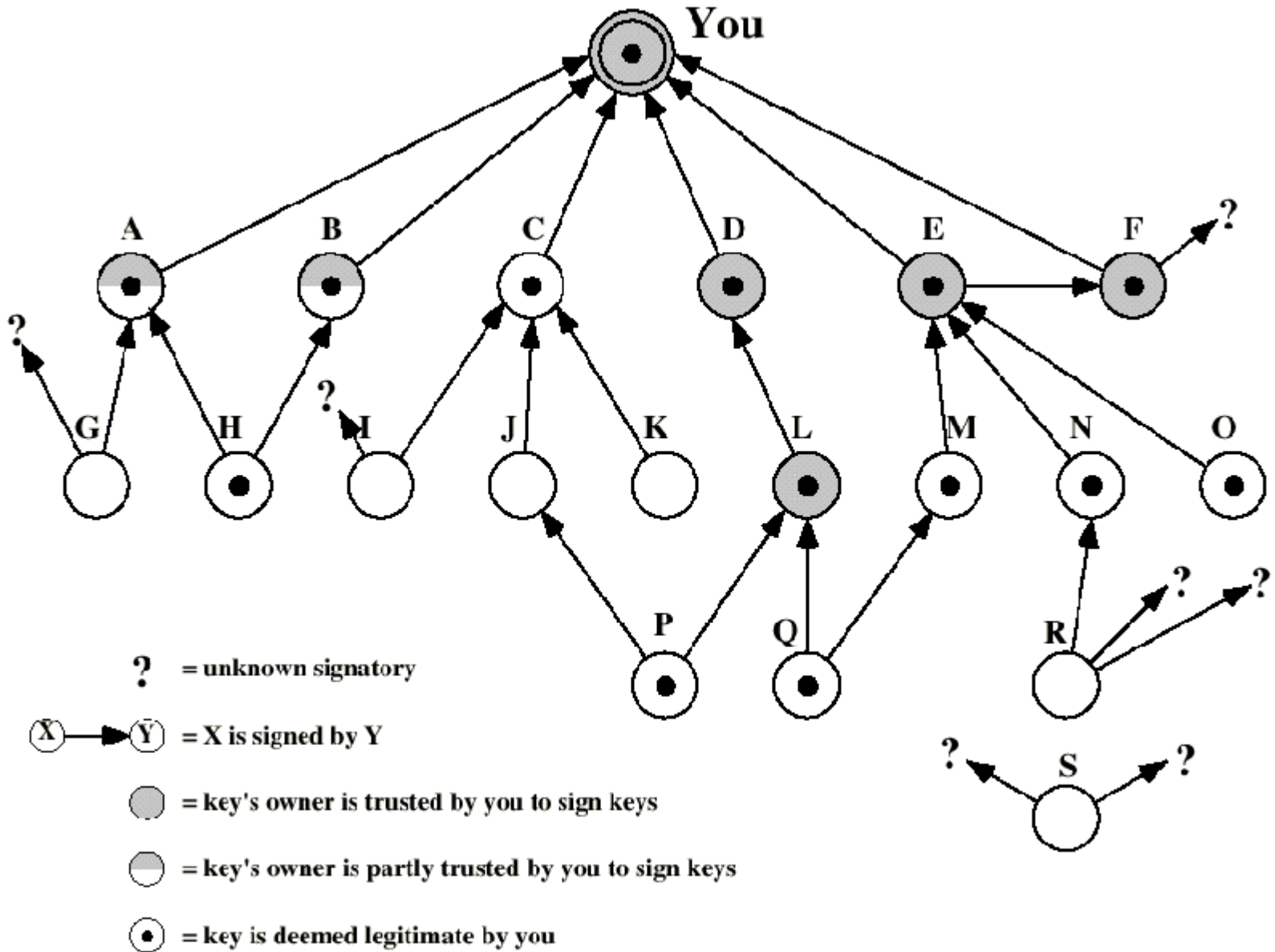


Figure 5.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)



Revoking Public Keys

- The owner issue a key revocation certificate.
- Normal signature certificate with a revoke indicator.
- Corresponding private key is used to sign the certificate.

Simple Mail Transfer Protocol (SMTP, RFC 822)

- **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)

User Agent Role

- **Example: Verisign (www.verisign.com)**
 - **Class-1:** Buyer's email address confirmed by emailing vital info.
 - **Class-2:** Postal address is confirmed as well, and data checked against directories.
 - **Class-3:** Buyer must appear in person, or send notarized documents.