Chapter 5

Electronic mail security

Outline

- Pretty good privacy
- S/MIME
- Recommended web sites

Pretty Good Privacy

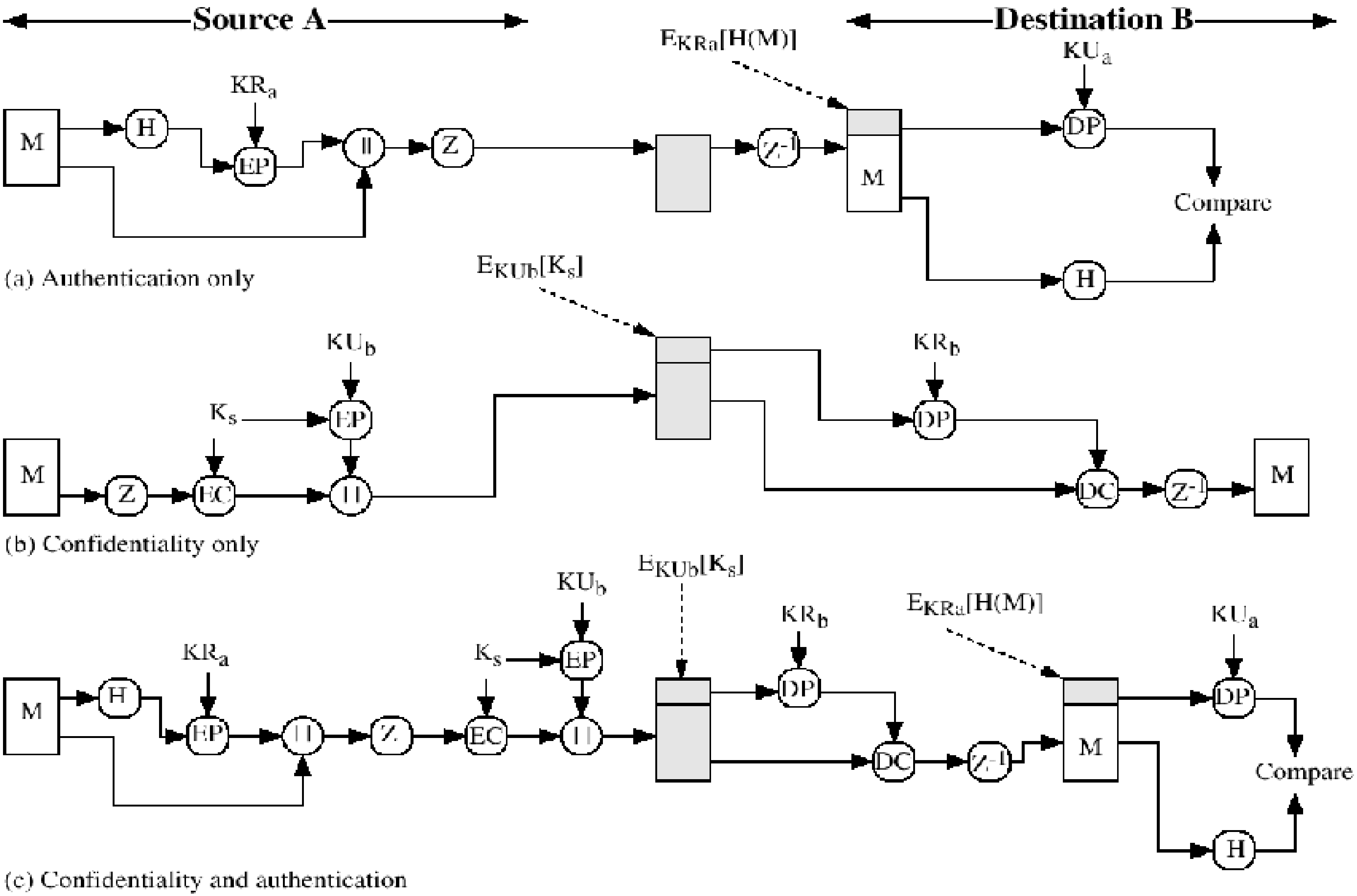
- Philip R. Zimmerman is the creator of PGP.
- PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

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

Operational Description

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



(a) Authentication only

(b) Confidentiality only

(c) Confidentiality and authentication

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%

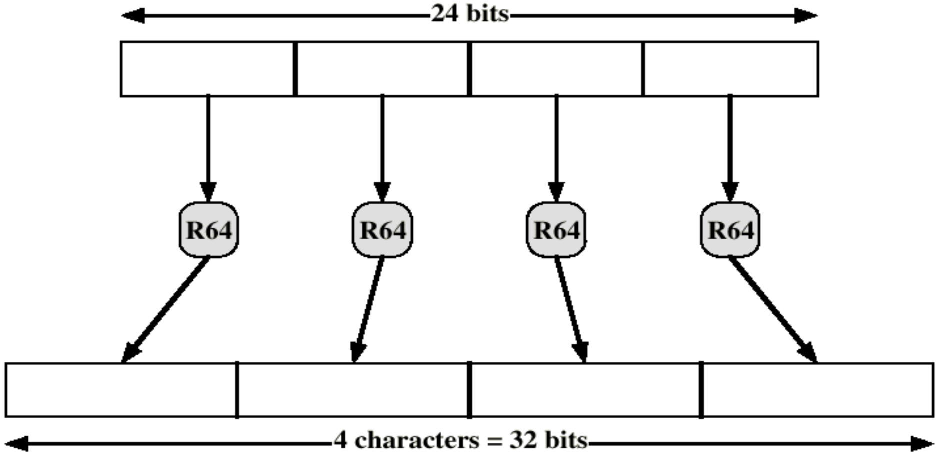


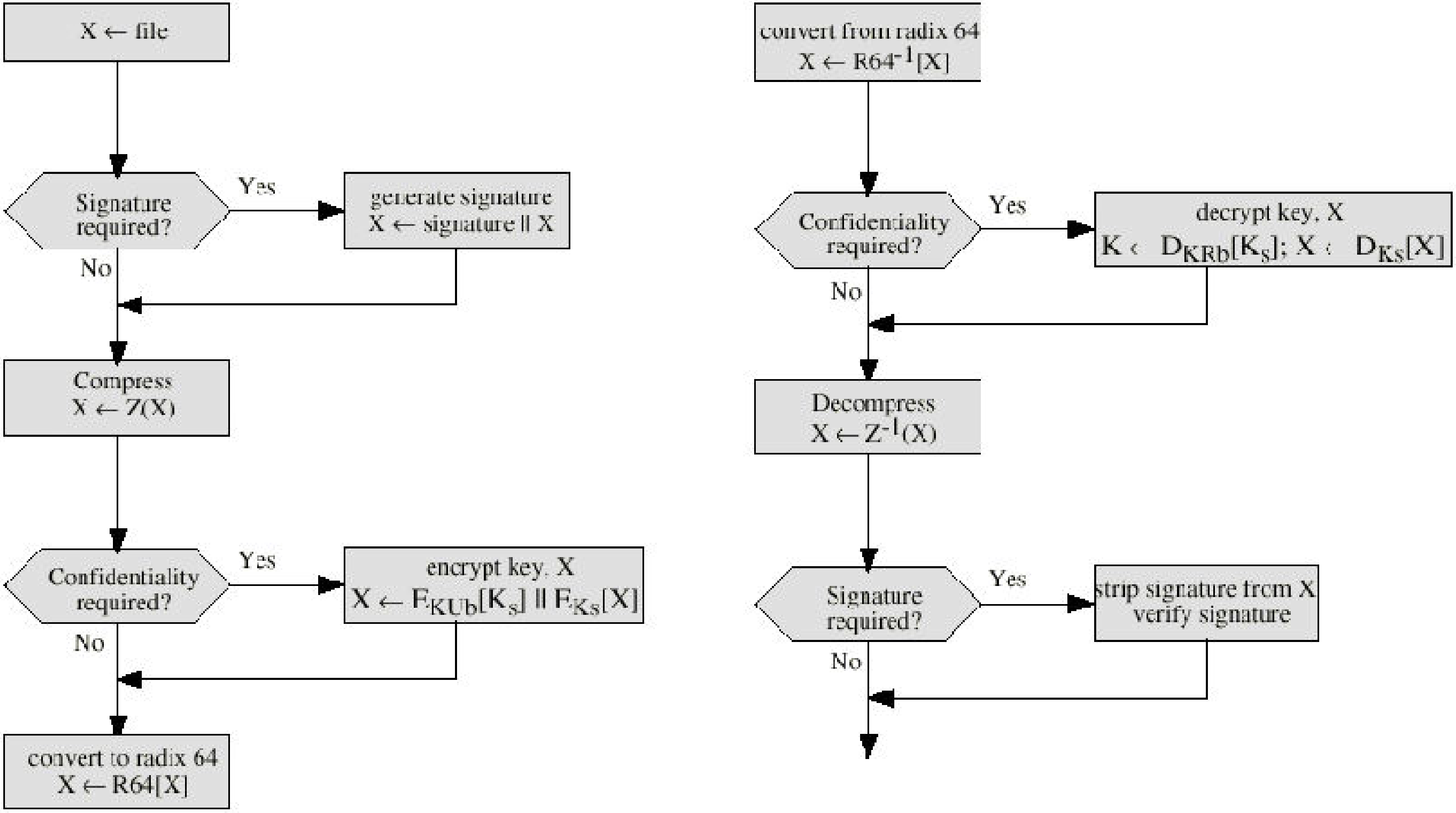
Figure 5.11 Printable Encoding of Binary Data into Radix-64 Format

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 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	

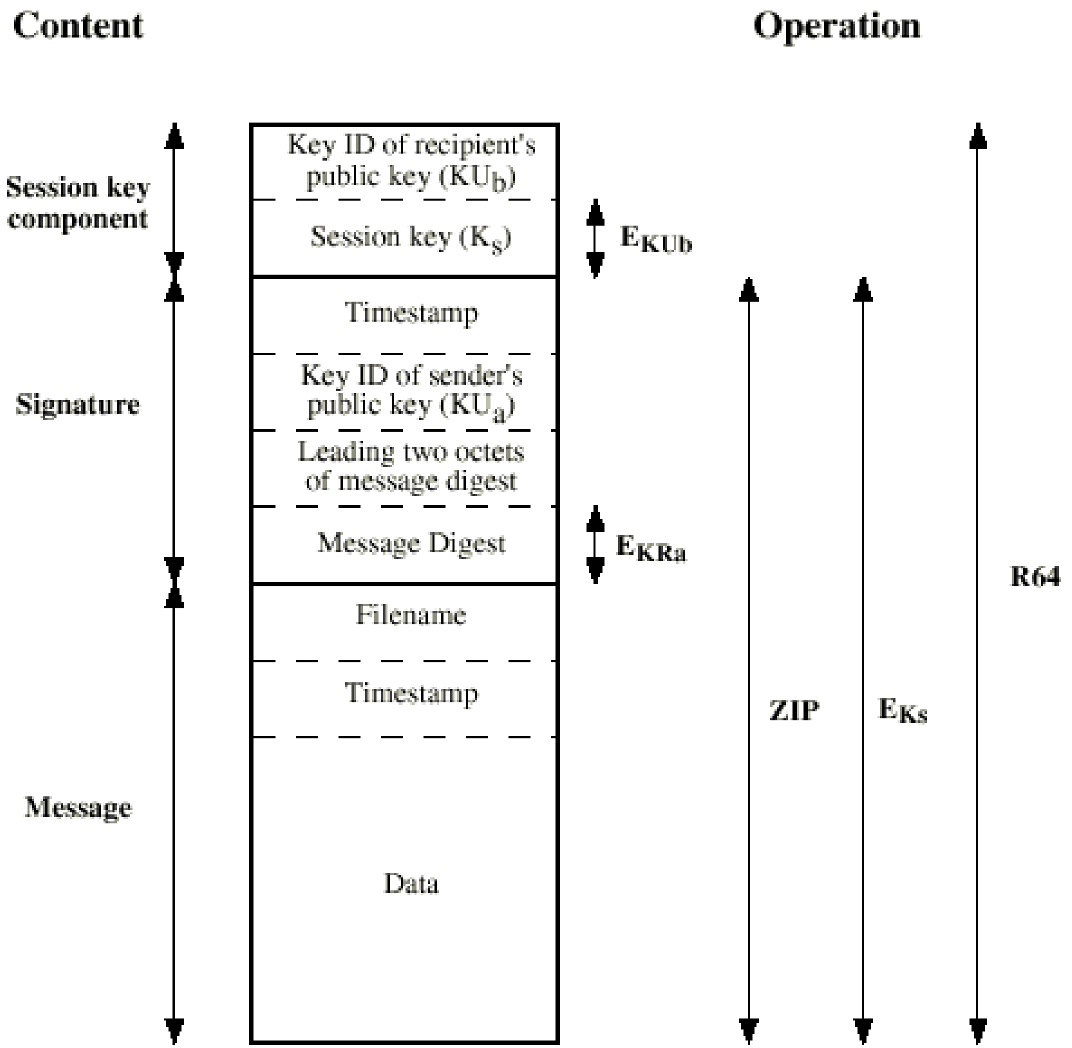


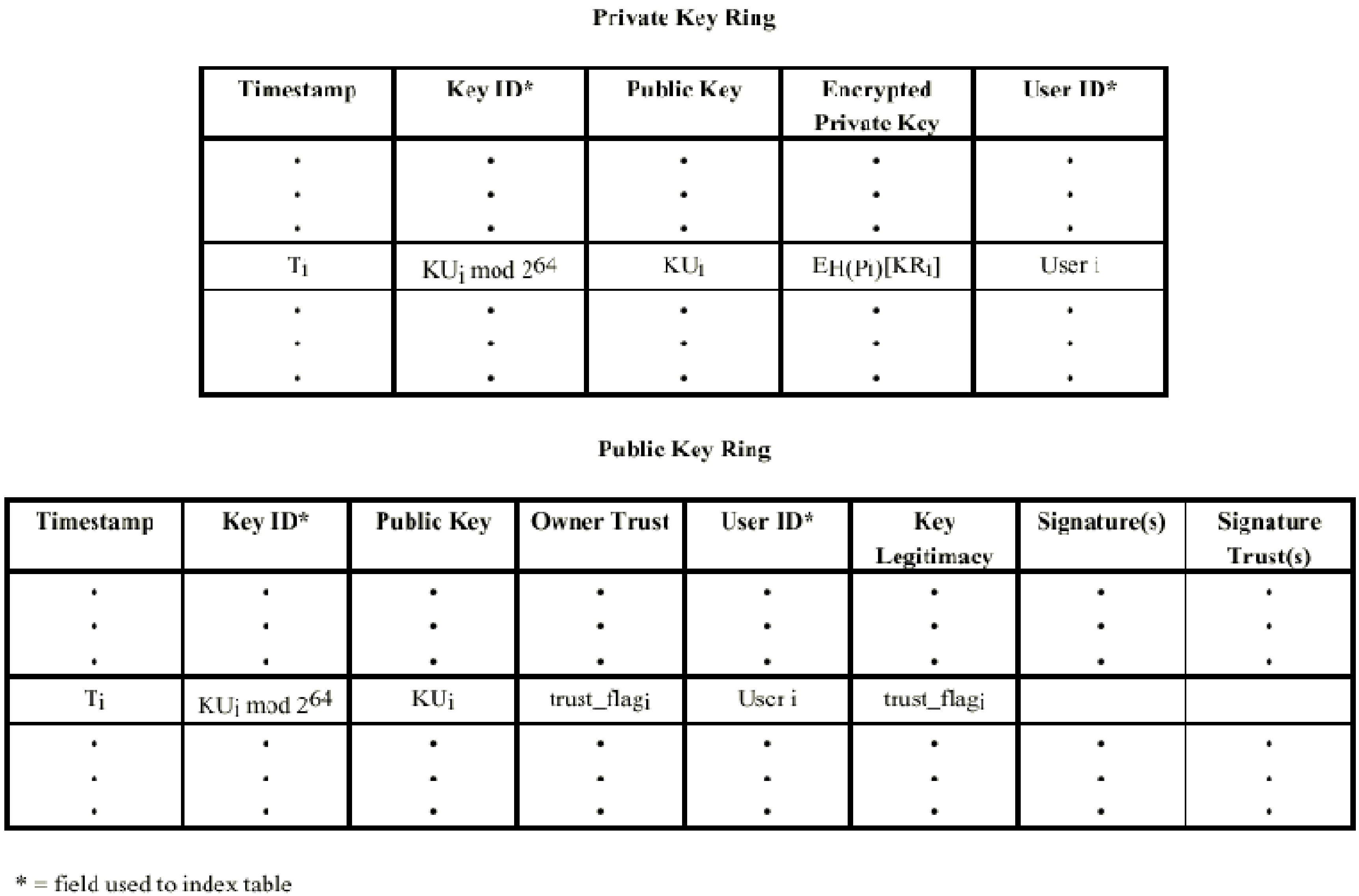
(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Figure 5.2 Transmission and Reception of PGP Messages

Format of PGP Message





Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	$KU_i \bmod 2^{64}$	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	$KU_i \bmod 2^{64}$	KU_i	trust_flag$_i$	User i	trust_flag$_i$		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

* = field used to index table

Figure 5.4 General Structure of Private and Public Key Rings

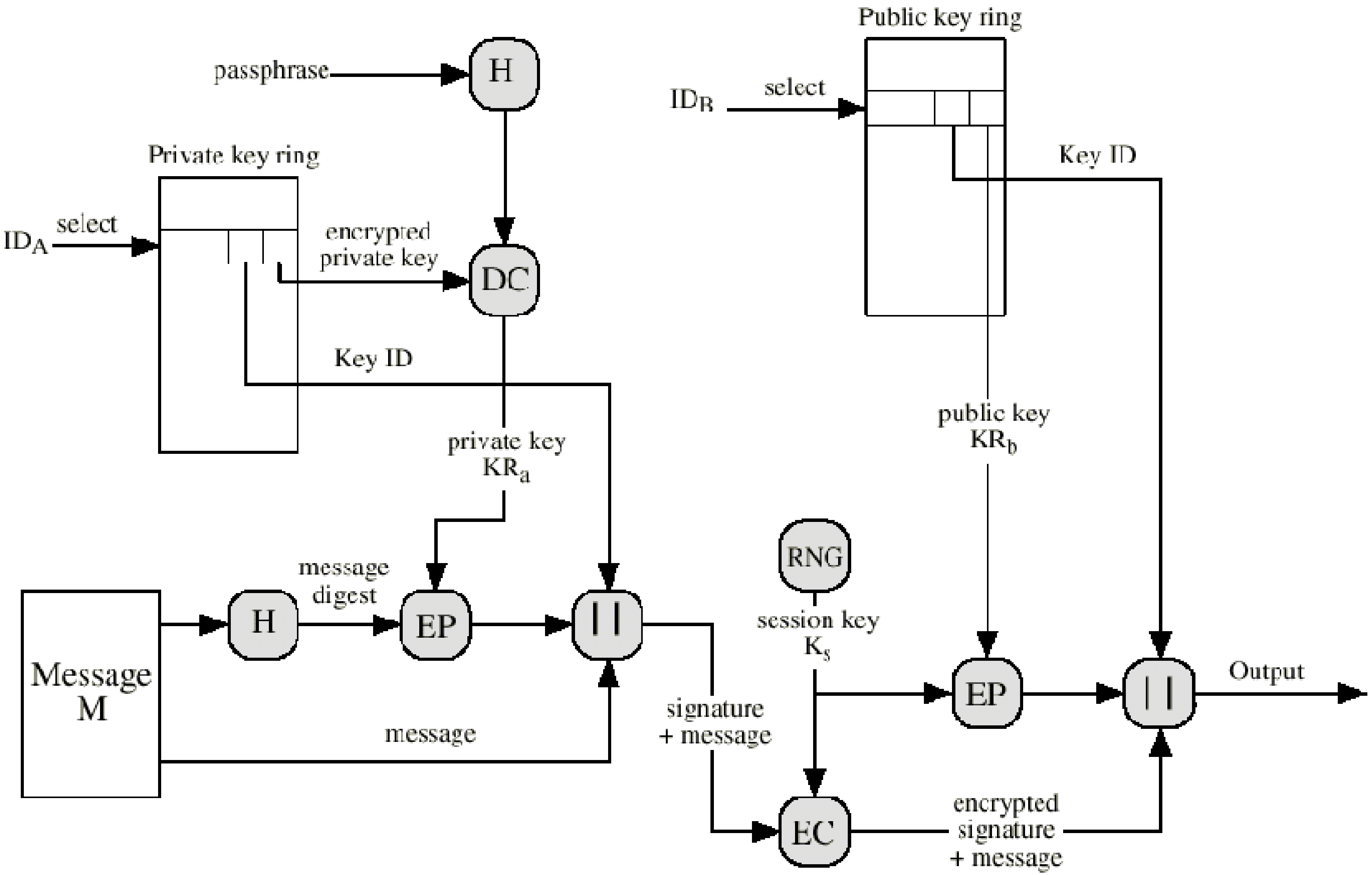


Figure 5.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

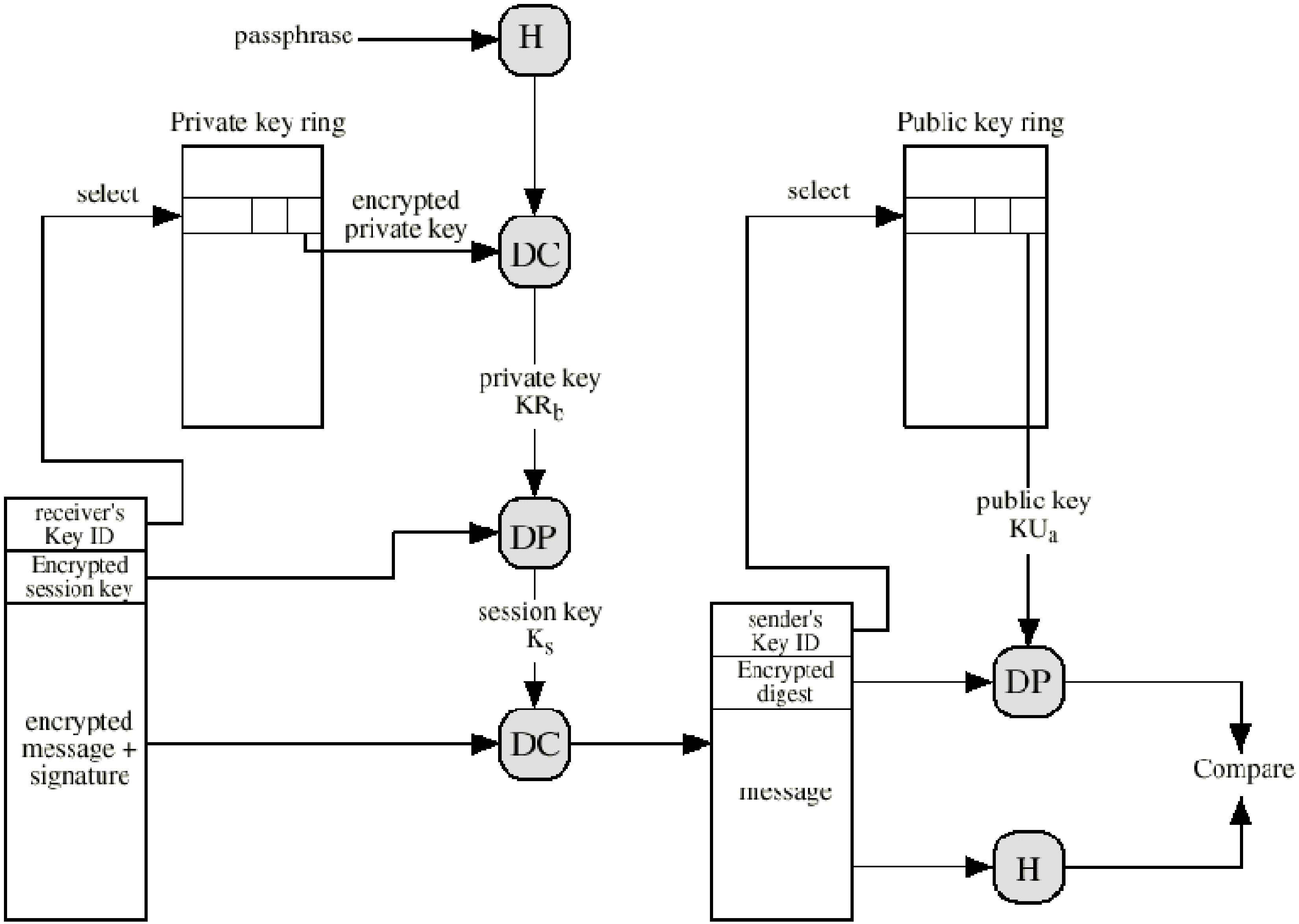


Figure 5.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

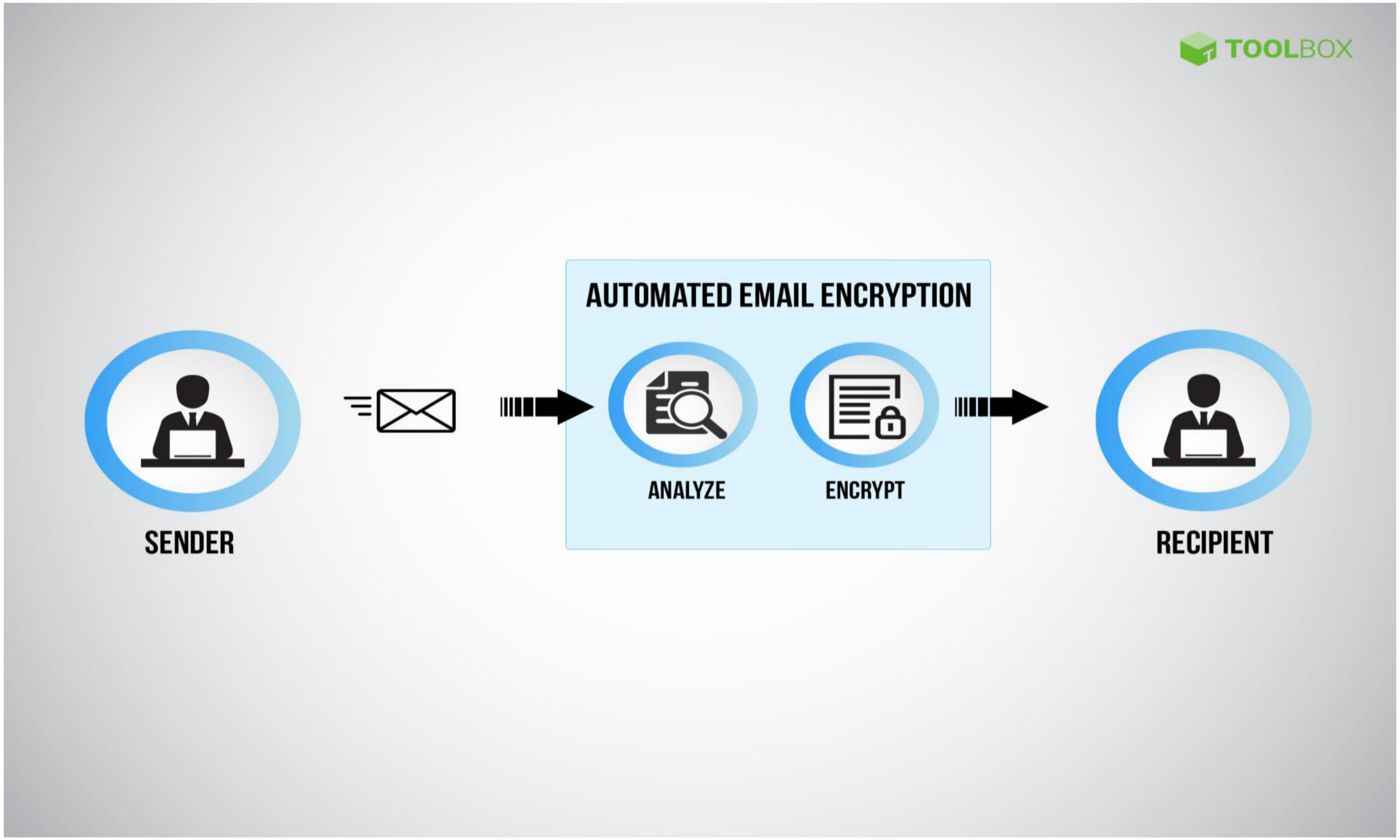
Email Security

- ***Email security can be defined as the use of various techniques to secure sensitive information in email communication and accounts against unauthorized access, loss, or compromise.***
- ***In simpler terms, email security allows an individual or organization to protect the overall access to one or more email addresses or accounts.***

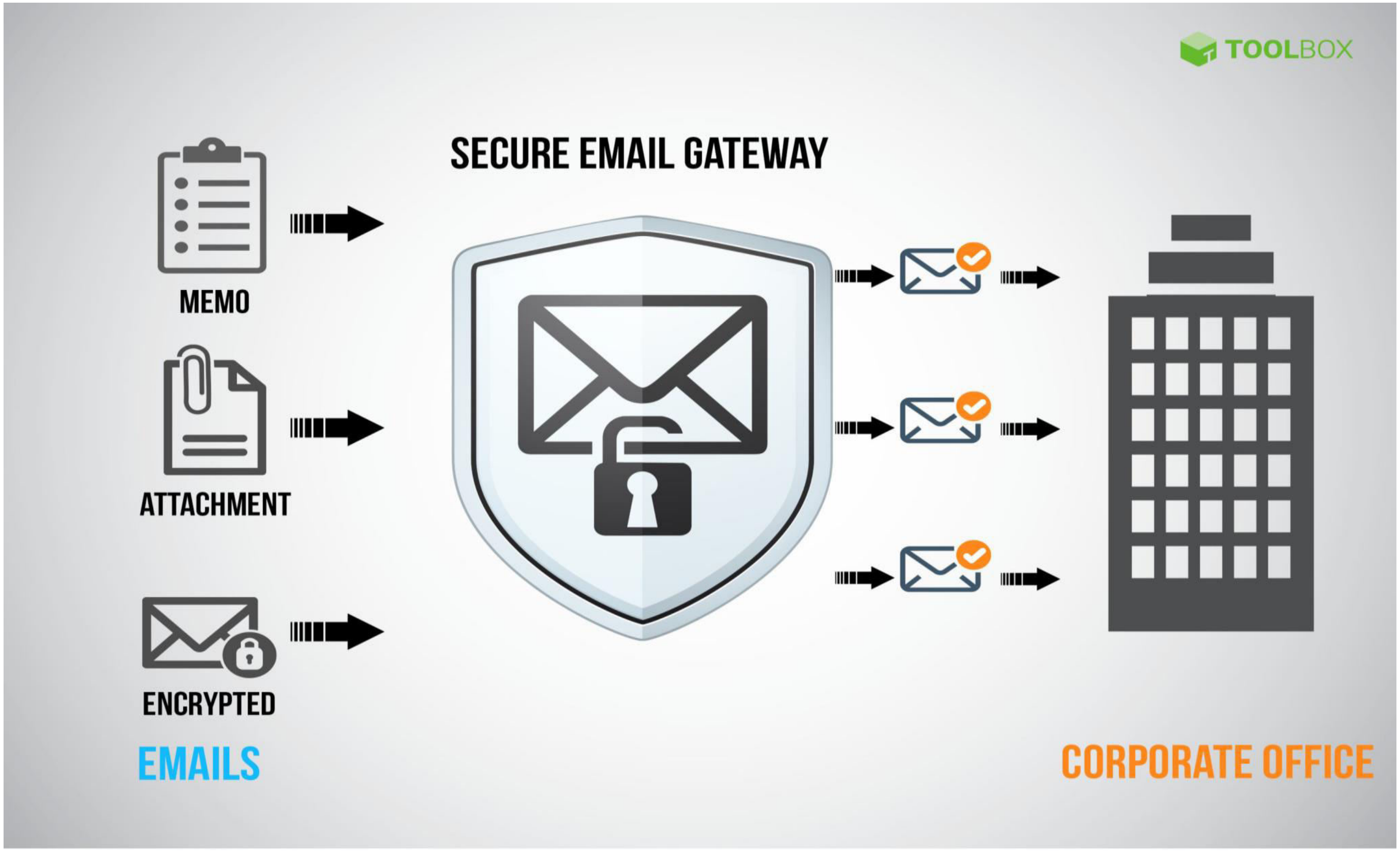
Stopping attacks at the entry point

1. Strong passwords
2. Password rotations
3. Spam filters
4. Desktop-based anti-virus or anti-spam application

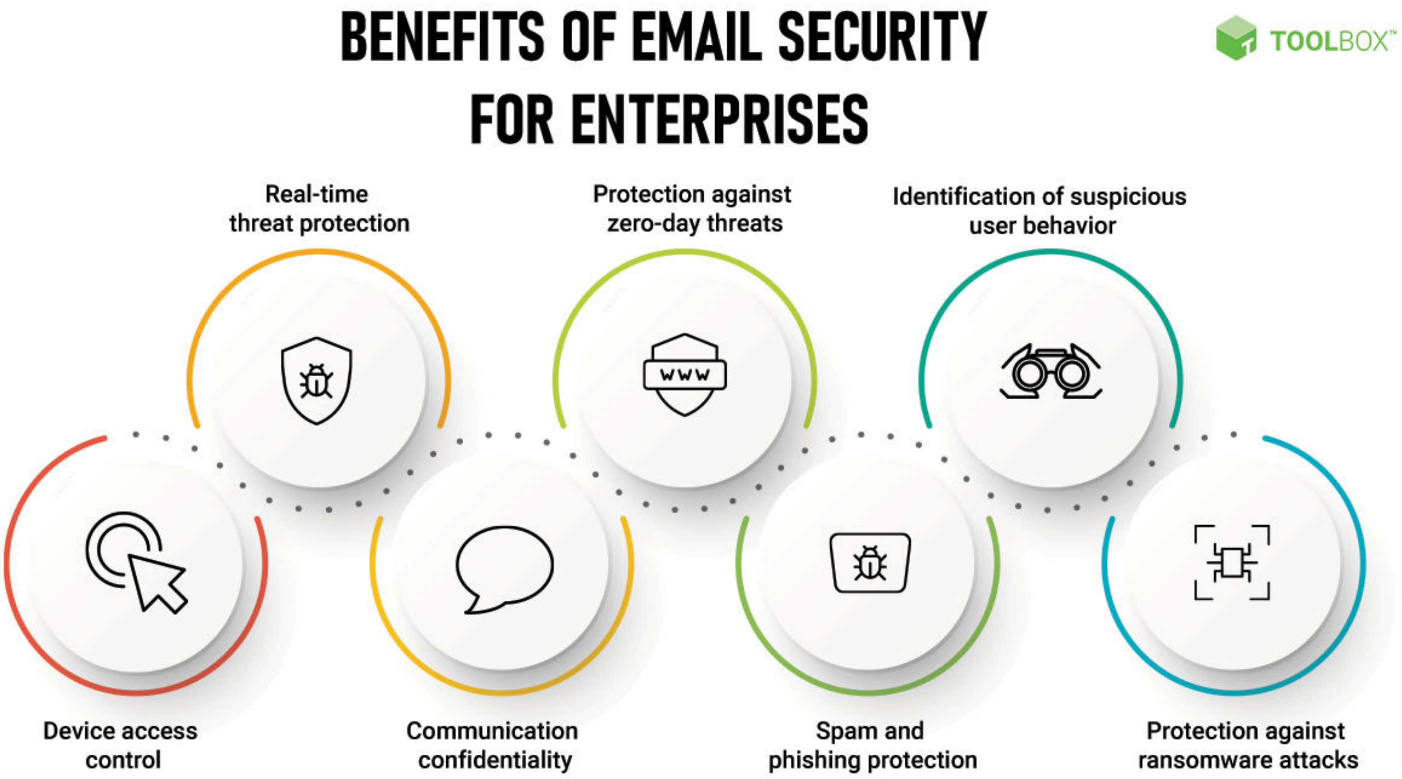
Email Encryption automate



Securing Email Gateway



Benefits of Email Security



BENEFITS OF EMAIL SECURITY FOR ENTERPRISES

Device access control

Real-time threat protection

Communication confidentiality

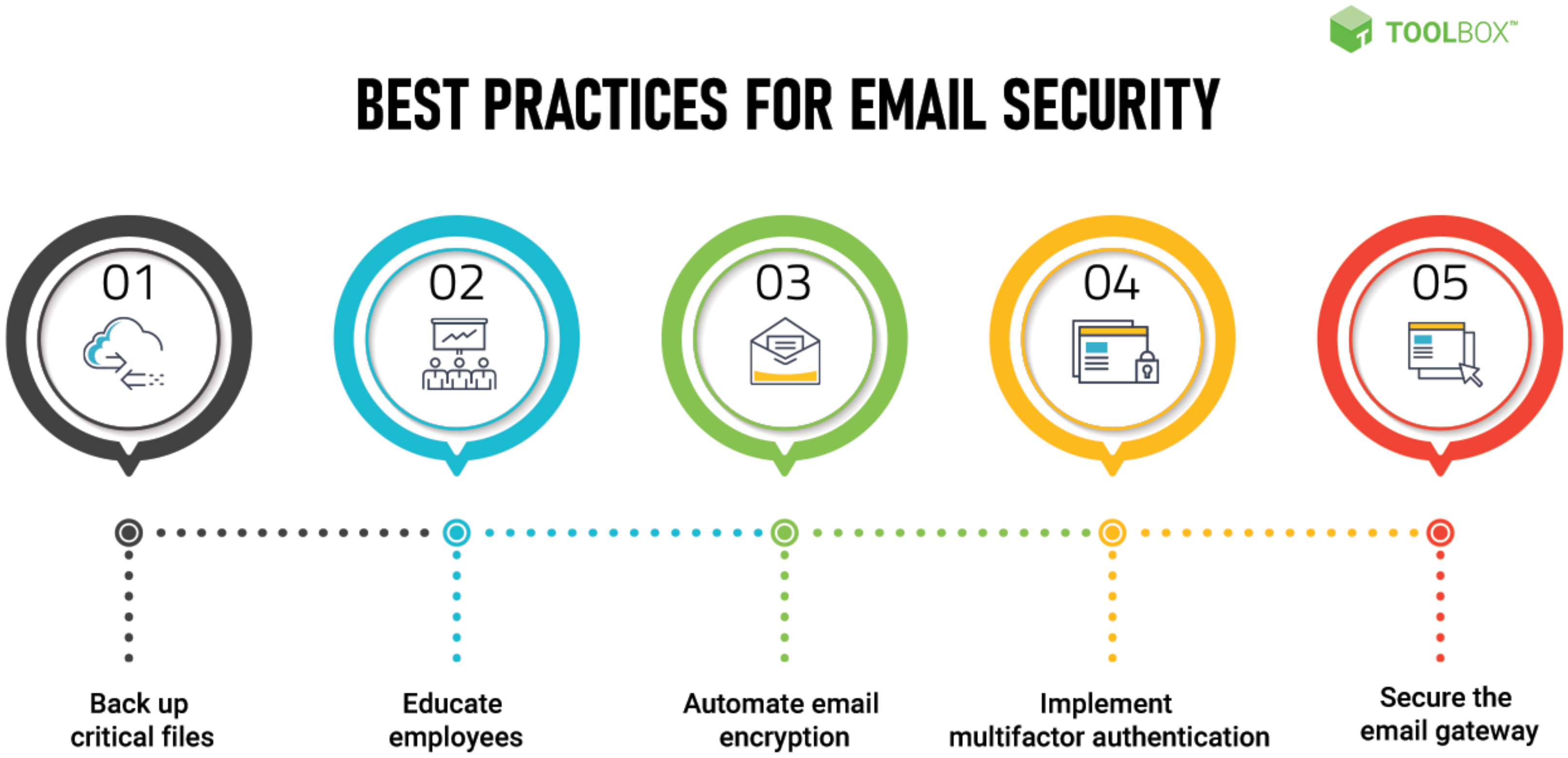
Protection against zero-day threats

Spam and phishing protection

Identification of suspicious user behavior

Protection against ransomware attacks

Best Practices



BEST PRACTICES FOR EMAIL SECURITY

01 Back up critical files

02 Educate employees

03 Automate email encryption

04 Implement multifactor authentication

05 Secure the email gateway

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)

- **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.

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.

Recommended Web Sites

- PGP home page: www.pgp.com
- MIT distribution site for PGP
- S/MIME Charter
- S/MIME Central: RSA Inc.'s Web Site