Email Security

DR. MOHAMMED ABDULRIDHA HUSSAIN

Pretty Good Privacy (PGP)

- Largely 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.
- PGP is now on an Internet standards track (RFC 3156; *MIME Security with OpenPGP*).
- Algorithms includes RSA, DSS, and Diffie-Hellman for public-key encryption;CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.
- **Operational Description**
- The actual operation of PGP, as opposed to the management of keys, consists of four services: authentication, confidentiality, compression, and e-mail compatibility
- **Notation**

K_s	=	session key used in symmetric encryption scheme
PR_a	=	private key of user A, used in public-key encryption scheme
PU_a	=	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

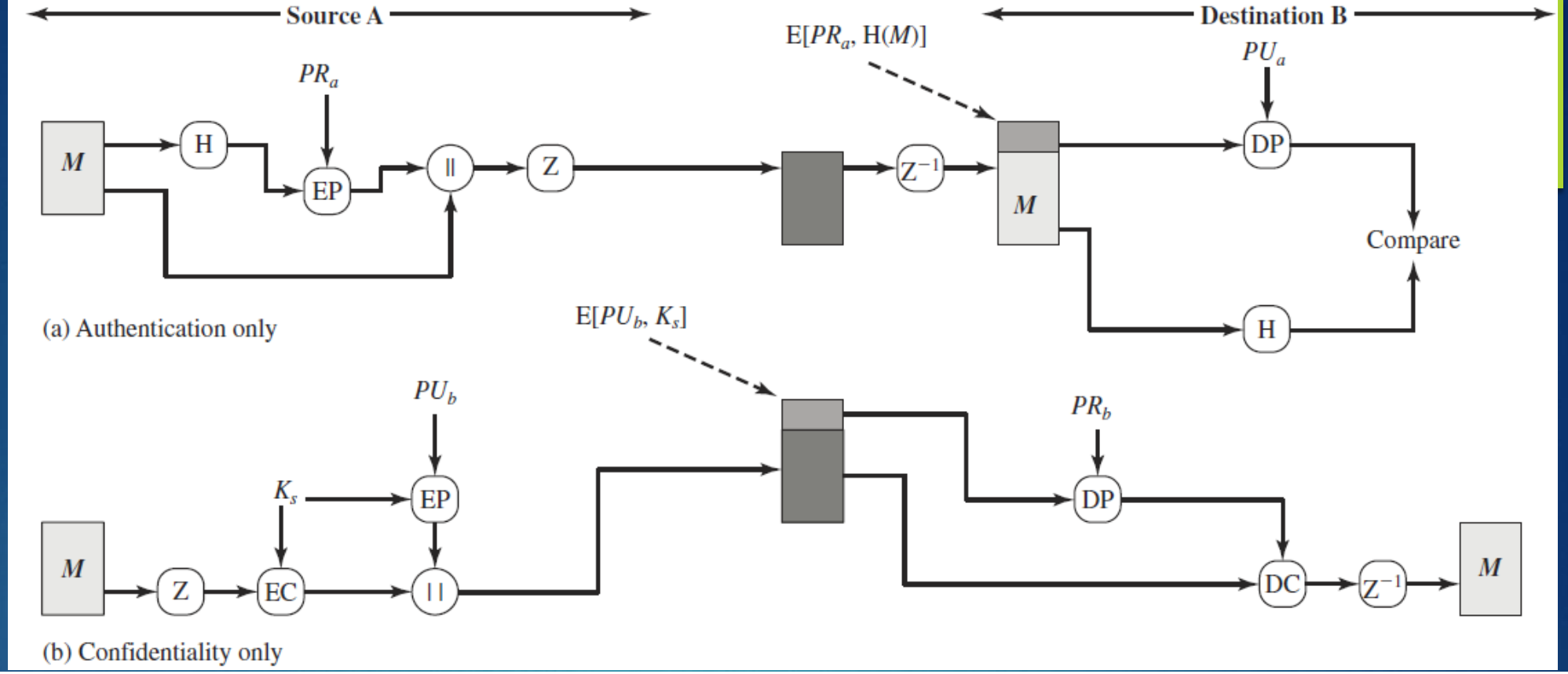
Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman 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.

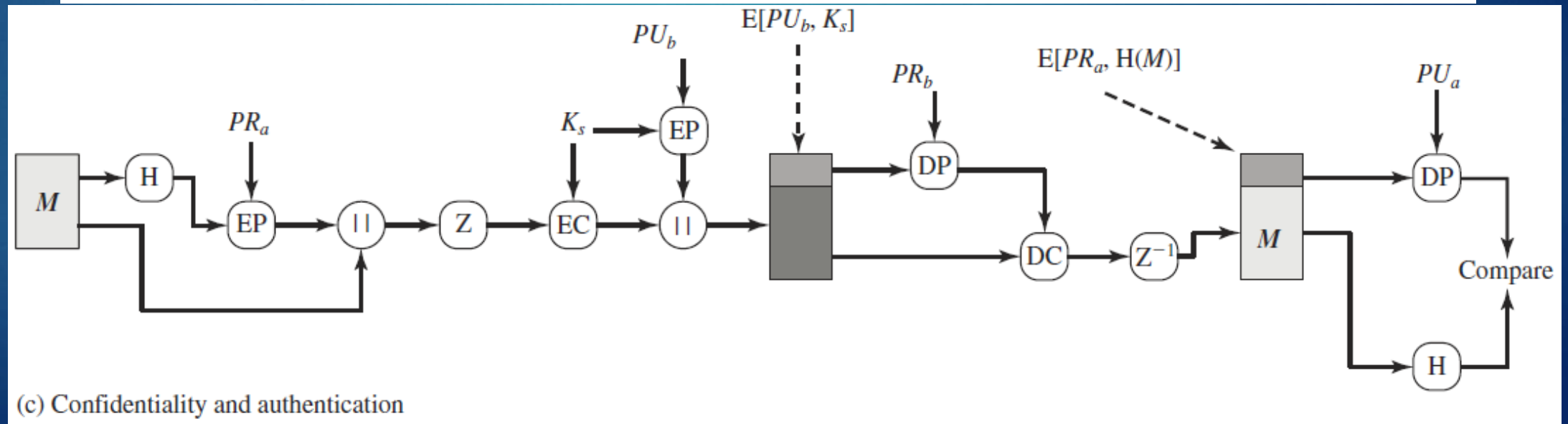
AUTHENTICATION

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.

CONFIDENTIALITY

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.


Source A
Destination B
E[PR_a, H(M)]
PR_a
PU_a
M
H
EP
||
Z
Z^{-1}
M
DP
Compare
H
(a) Authentication only
E[PU_b, K_s]
PU_b
PR_b
K_s
EP
DP
M
Z
EC
||
DC
Z^{-1}
M
(b) Confidentiality only


E[PU_b, K_s]
PU_b
PR_b
E[PR_a, H(M)]
PU_a
PR_a
K_s
EP
DP
M
H
EP
||
Z
EC
||
DC
Z^{-1}
M
DP
Compare
H
(c) Confidentiality and authentication

COMPRESSION

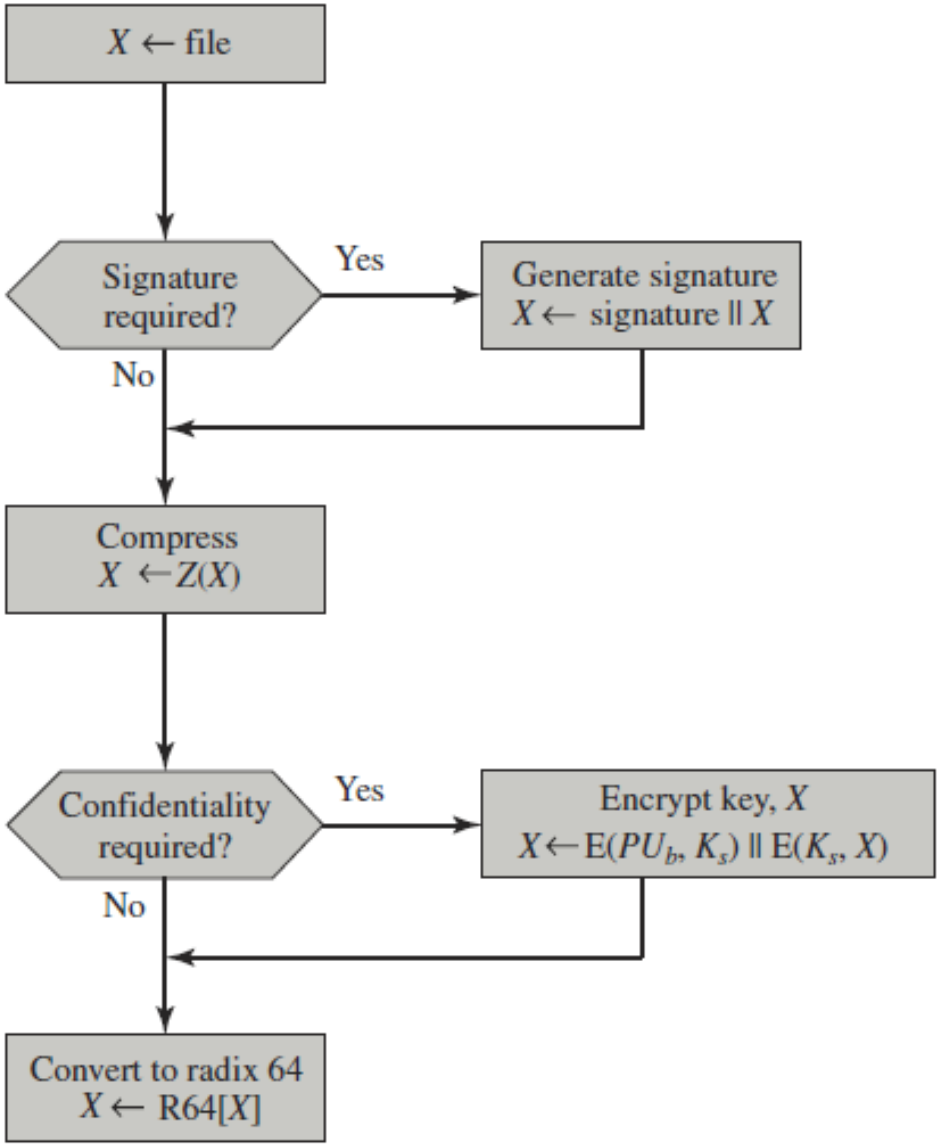
- PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission and for file storage.

E-MAIL COMPATIBILITY

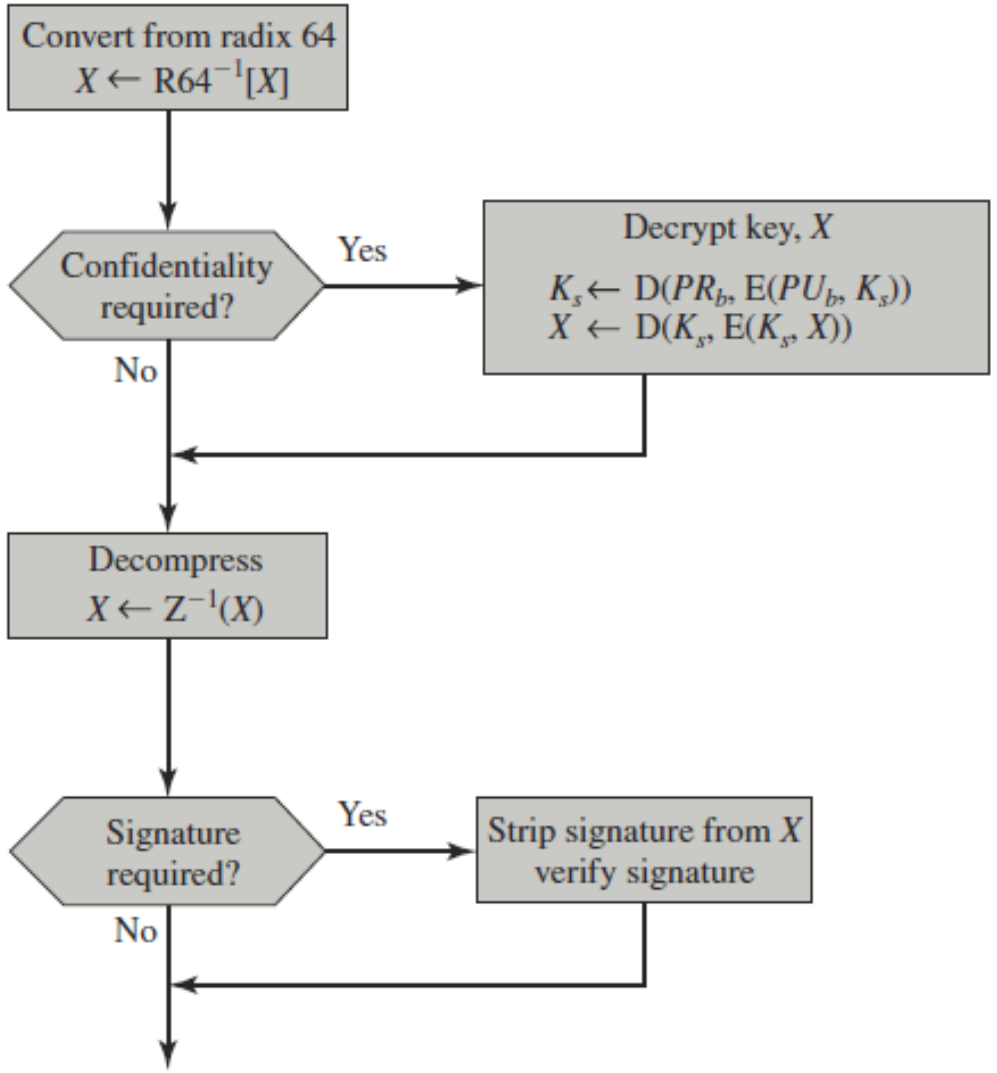
- Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters.
- The scheme used for this purpose is radix-64 conversion. Each group of three octets of binary data is mapped into four ASCII characters.

Cryptographic Keys and Key Rings

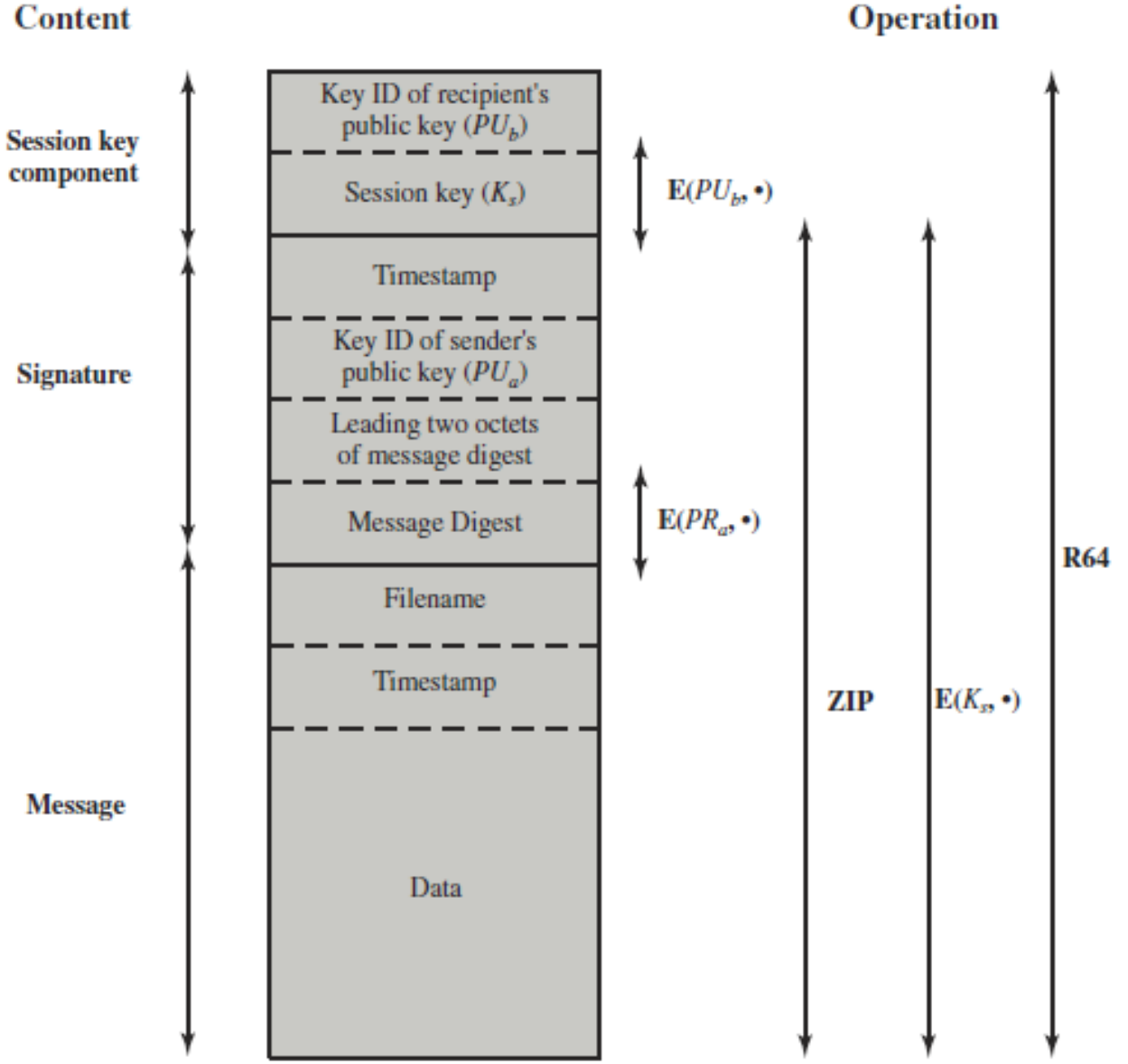
- PGP makes use of four types of keys: one-time session symmetric keys, public keys, private keys, and passphrase-based symmetric keys.
- Public-Key management and Securing Private-Key



(a) Generic transmission diagram (from A)

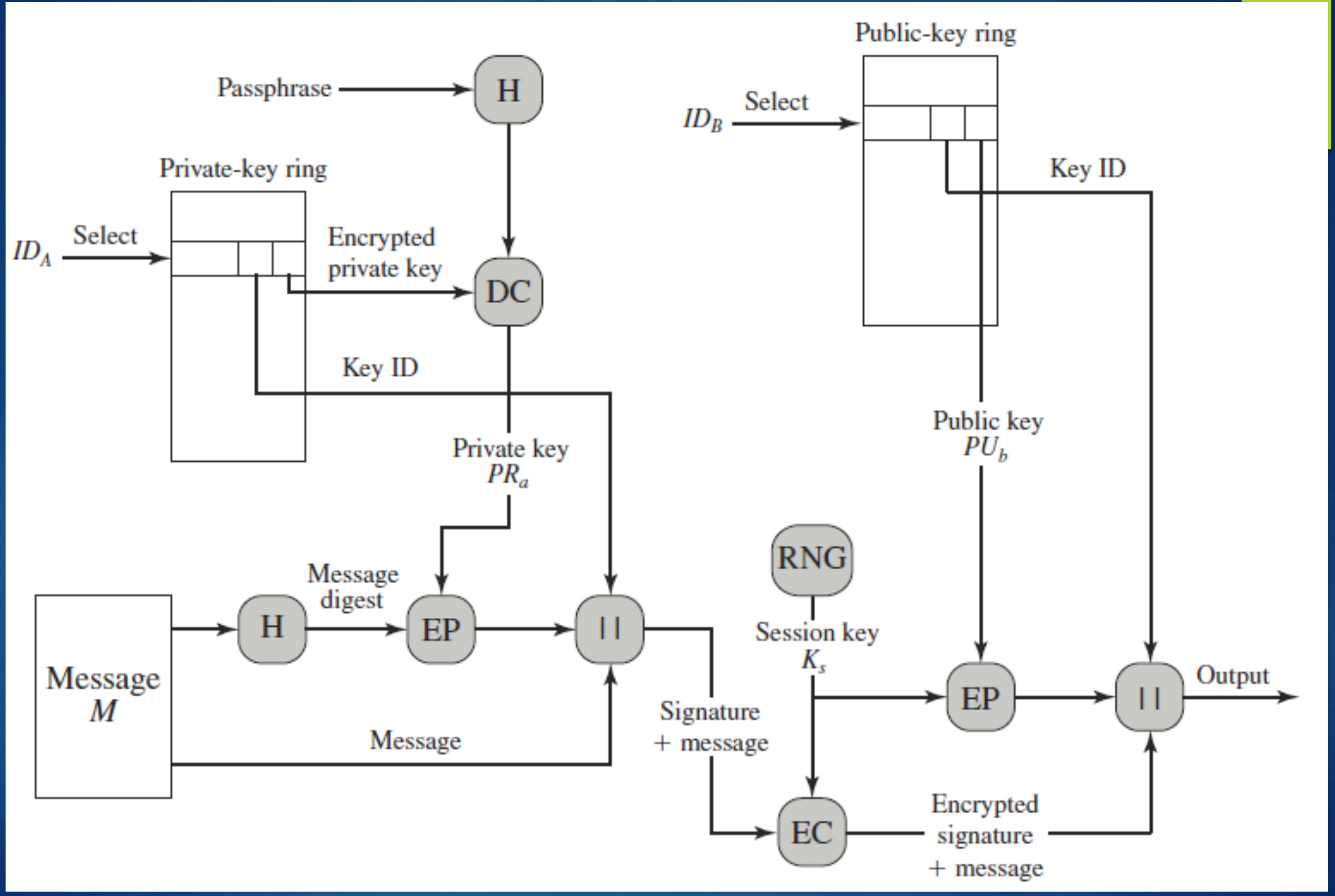


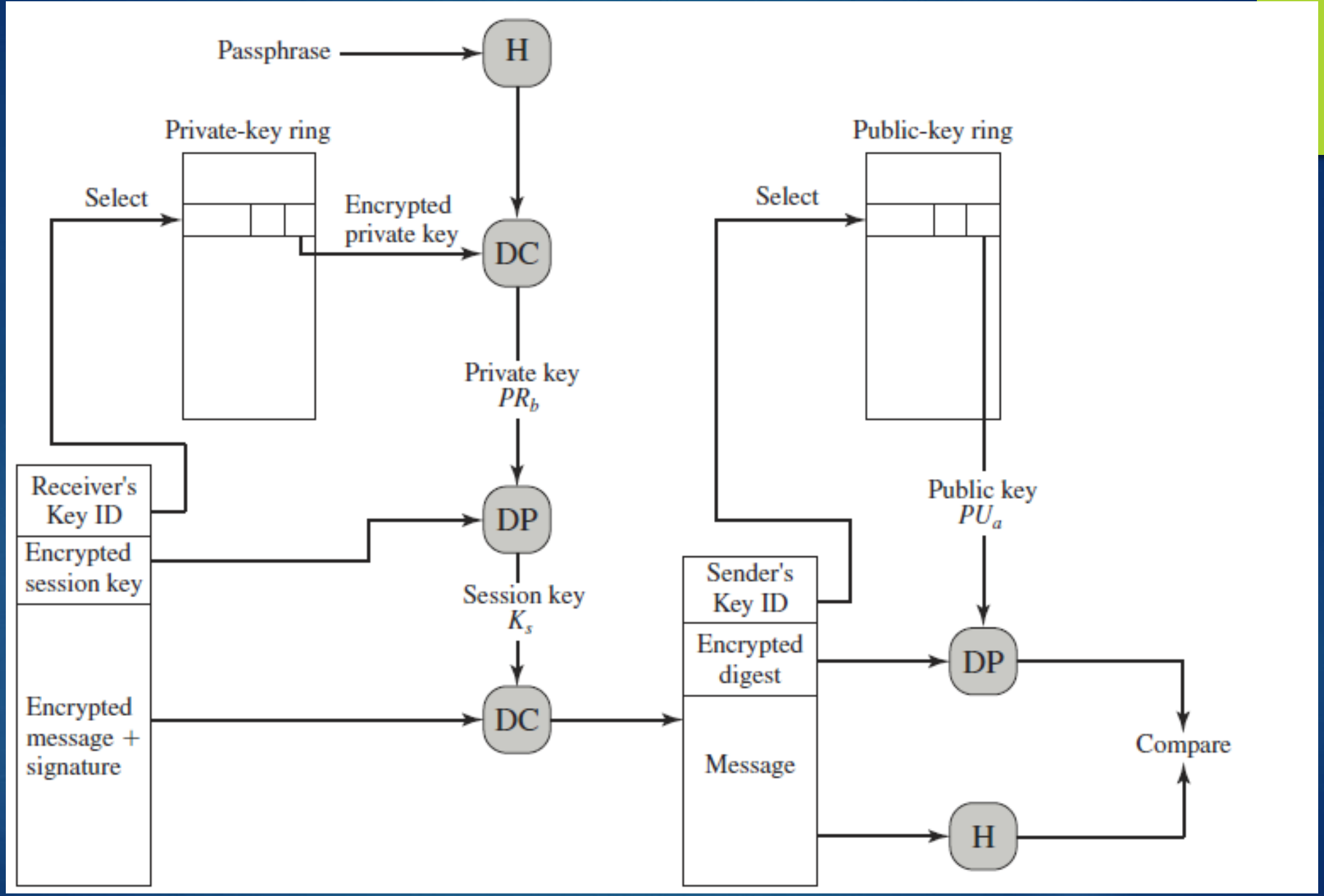
(b) Generic reception diagram (to B)



Notation:

E(PU_b, •) = encryption with user b's public key
E(PR_a, •) = encryption with user a's private key
E(K_s, •) = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function


Passphrase
H
Private-key ring
ID_A
Select
Encrypted private key
DC
Key ID
Private key PR_a
Public-key ring
ID_B
Select
Key ID
Public key PU_b
RNG
Session key K_s
Message digest
H
EP
||
Message M
Message
Signature + message
EP
||
Output
EC
Encrypted signature + message


Passphrase
H
Private-key ring
Select
Encrypted private key
DC
Private key PR_b
Receiver's Key ID
Encrypted session key
Encrypted message + signature
DP
Session key K_s
DC
Public-key ring
Select
Public key PU_a
Sender's Key ID
Encrypted digest
Message
DP
H
Compare

- Generate Public-Private Keys
- How To store Private Key in secure manner and assign an ID
- Public Key Certificate
- Registration (Signed Certificate)
- Administrator (Local, or not)

References

- [1] William Stallings, “CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE”, Fifth ed. Prentice Hall, 2011