

Cryptography and Network Security Chapter 15

Fourth Edition
by William Stallings



Chapter 15 – Electronic Mail Security

Despite the refusal of VADM Poindexter and LtCol North to appear, the Board's access to other sources of information filled much of this gap. The FBI provided documents taken from the files of the National Security Advisor and relevant NSC staff members, including messages from the PROOF system between VADM Poindexter and LtCol North. The PROOF messages were conversations by computer, written at the time events occurred and presumed by the writers to be protected from disclosure. In this sense, they provide a first-hand, contemporaneous account of events.

—The Tower Commission Report to President Reagan on the Iran-Contra Affair, 1987

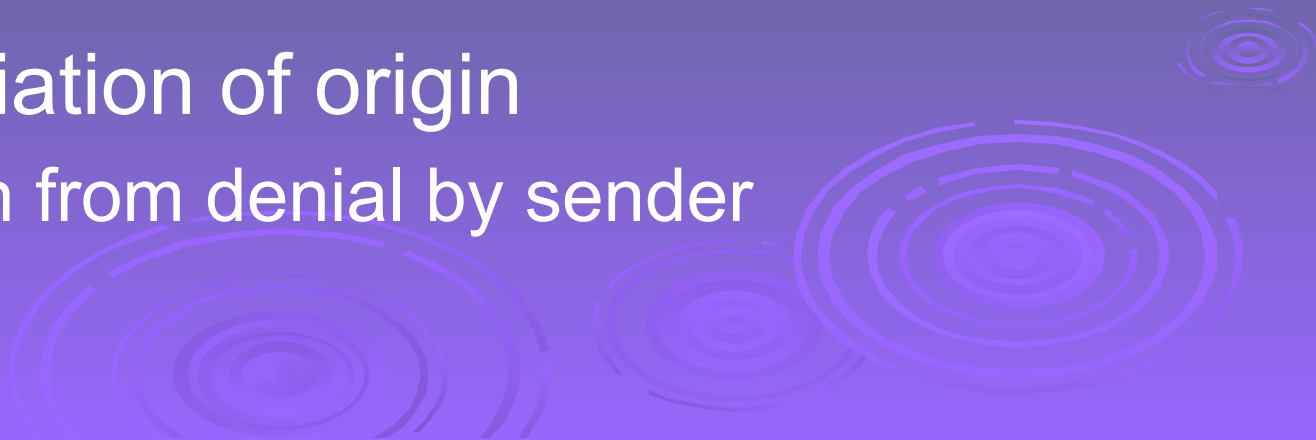
Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
 - may be inspected either in transit
 - or by suitably privileged users on destination system



Email Security Enhancements

- confidentiality
 - protection from disclosure
- authentication
 - of sender of message
- message integrity
 - protection from modification
- non-repudiation of origin
 - protection from denial by sender



Pretty Good Privacy (PGP)

- ❑ widely used de facto secure email
- ❑ developed by Phil Zimmermann
- ❑ selected best available crypto algs to use
- ❑ integrated into a single program
- ❑ on Unix, PC, Macintosh and other systems
- ❑ originally free, now also have commercial versions available



PGP Operation – Authentication

1. sender creates message
2. use SHA-1 to generate 160-bit hash of message
3. signed hash with RSA using sender's private key, and is attached to message
4. receiver uses RSA with sender's public key to decrypt and recover hash code
5. receiver verifies received message using hash of it and compares with decrypted hash code

PGP Operation – Confidentiality

1. sender generates message and 128-bit random number as session key for it
2. encrypt message using CAST-128 / IDEA / 3DES in CBC mode with session key
3. session key encrypted using RSA with recipient's public key, & attached to msg
4. receiver uses RSA with private key to decrypt and recover session key
5. session key is used to decrypt message

PGP Operation – Confidentiality & Authentication

- can use both services on same message
 - create signature & attach to message
 - encrypt both message & signature
 - attach RSA / ElGamal encrypted session key



PGP Operation – Compression

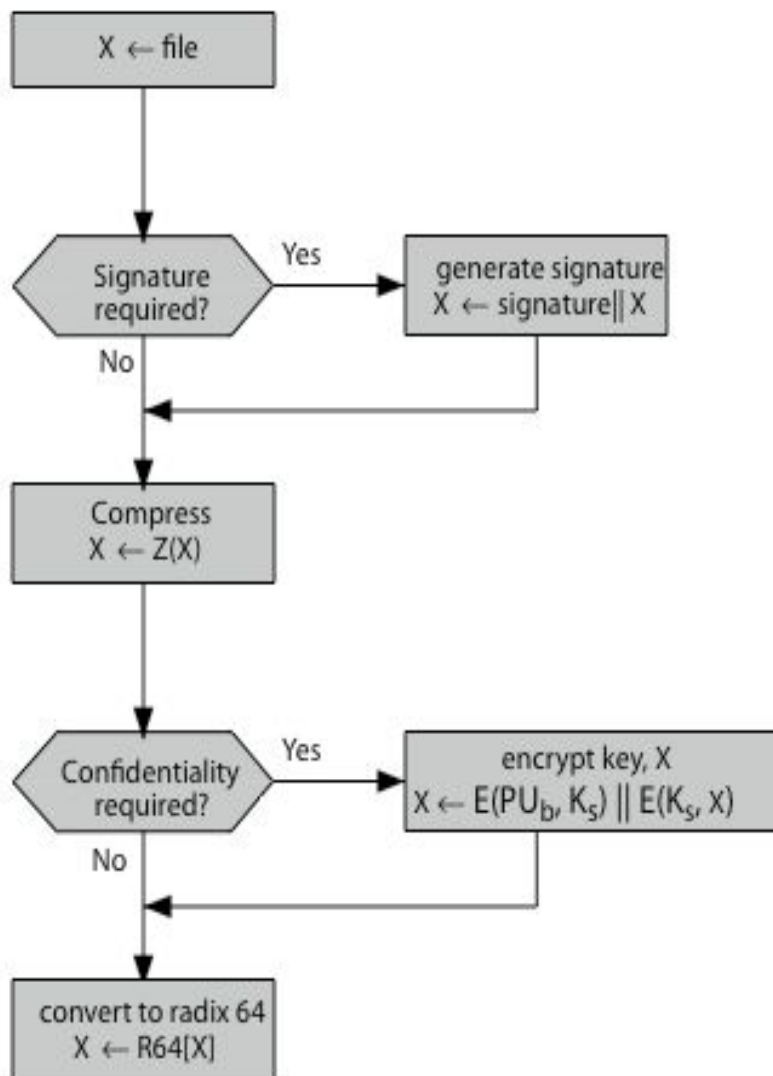
- by default PGP compresses message after signing but before encrypting
 - so can store uncompressed message & signature for later verification
 - & because compression is non deterministic
- uses ZIP compression algorithm



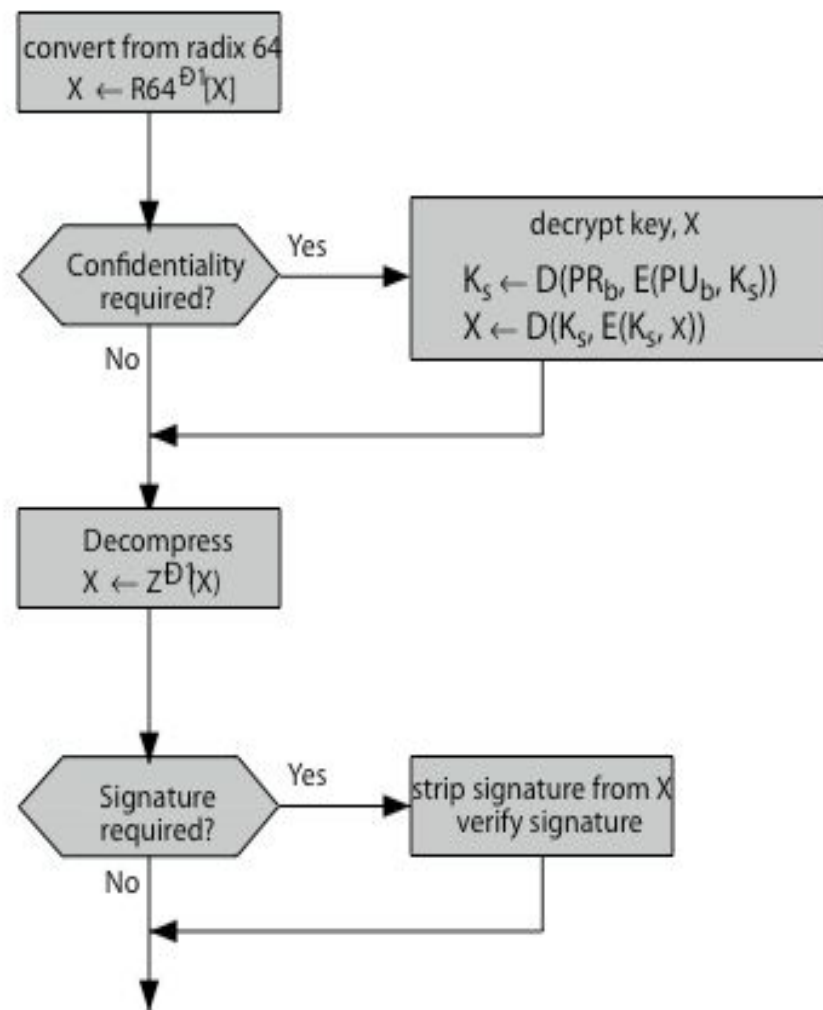
PGP Operation – Email Compatibility

- when using PGP will have binary data to send (encrypted message etc)
- however email was designed only for text
- hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
 - maps 3 bytes to 4 printable chars
 - also appends a CRC
- PGP also segments messages if too big

PGP Operation – Summary

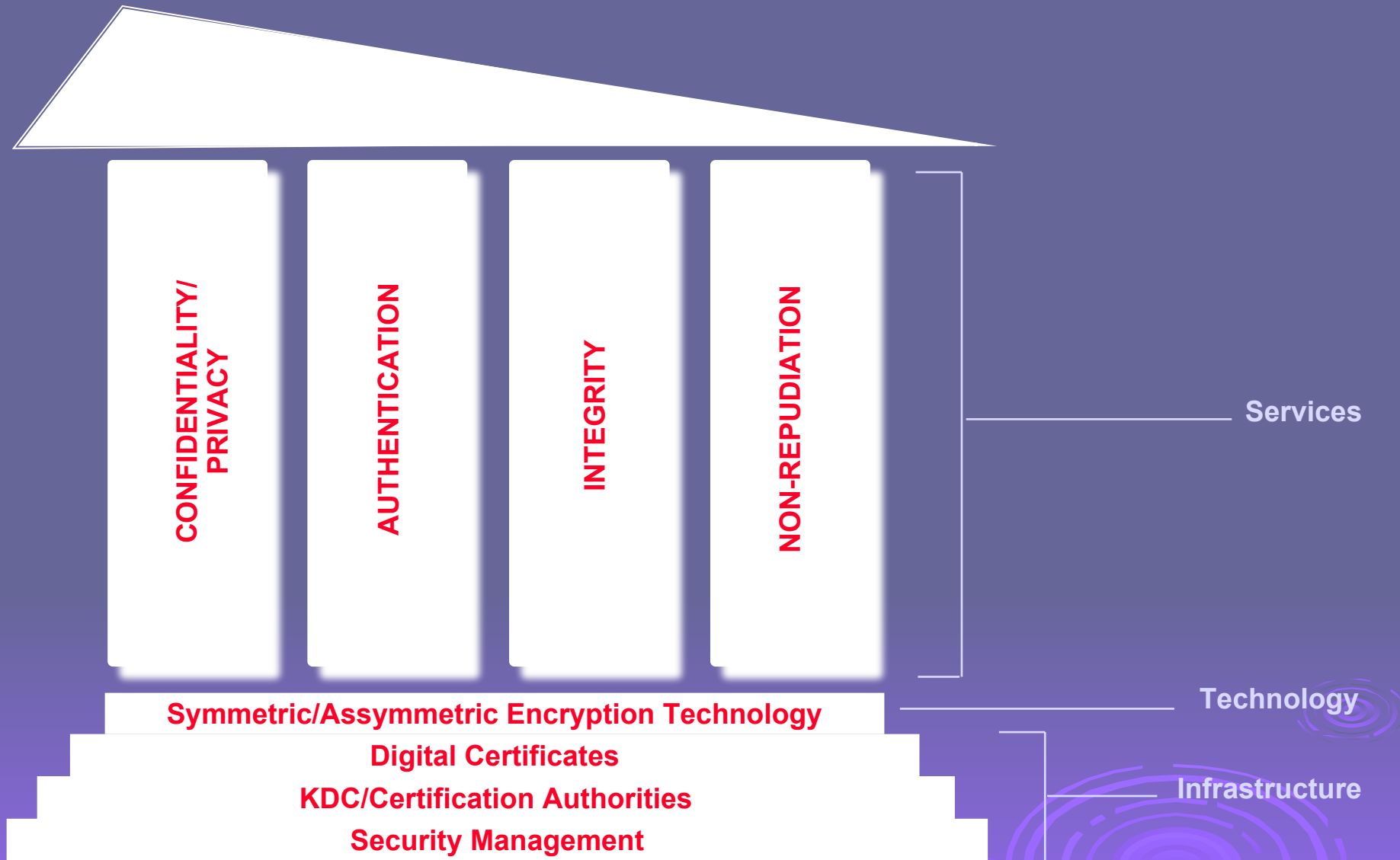


(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

Security



- Public Key Technology Best Suited to Solve Business Needs
- Infrastructure = Certification Authorities

Figure 15.1 PGP Cryptographic Functions

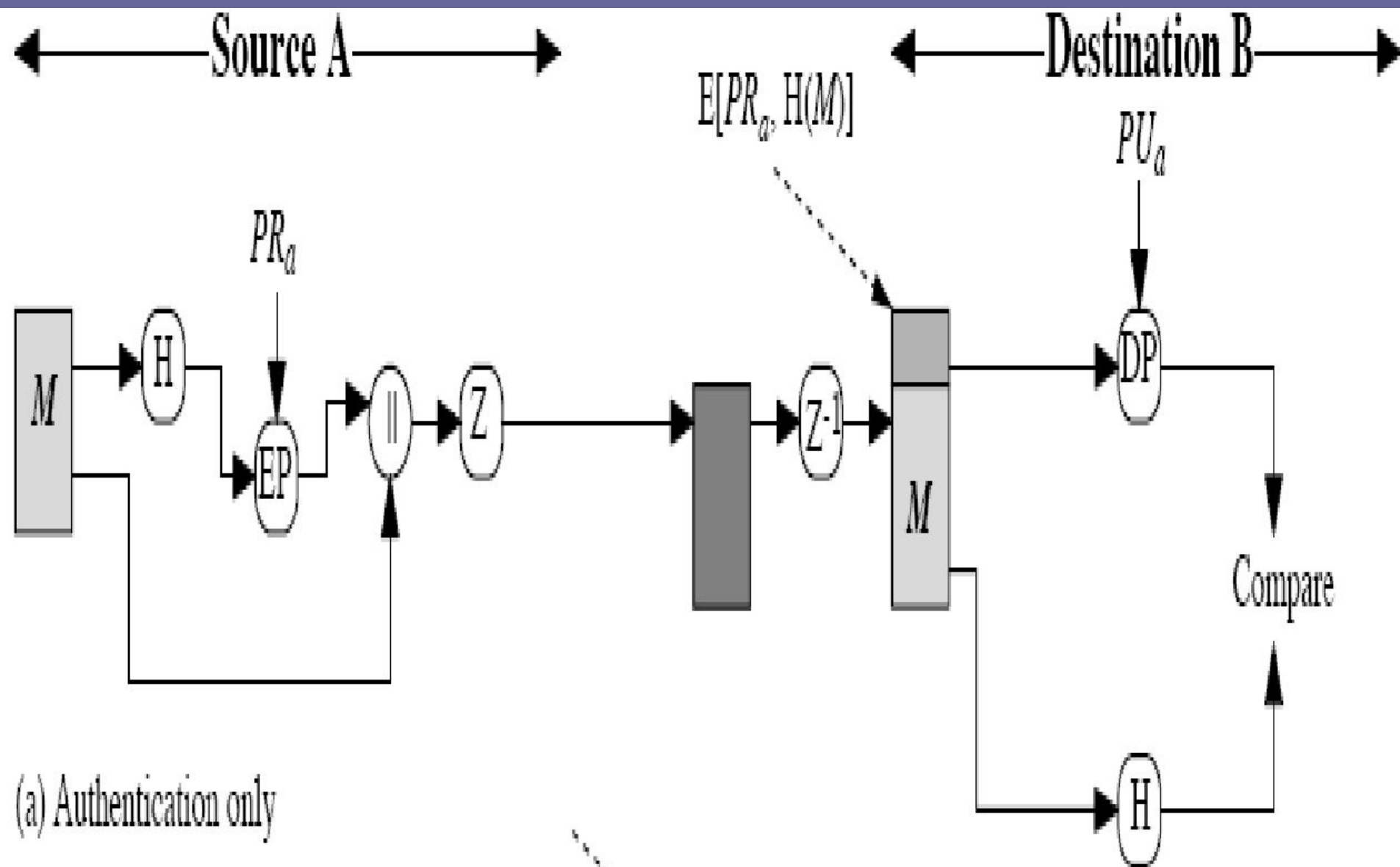
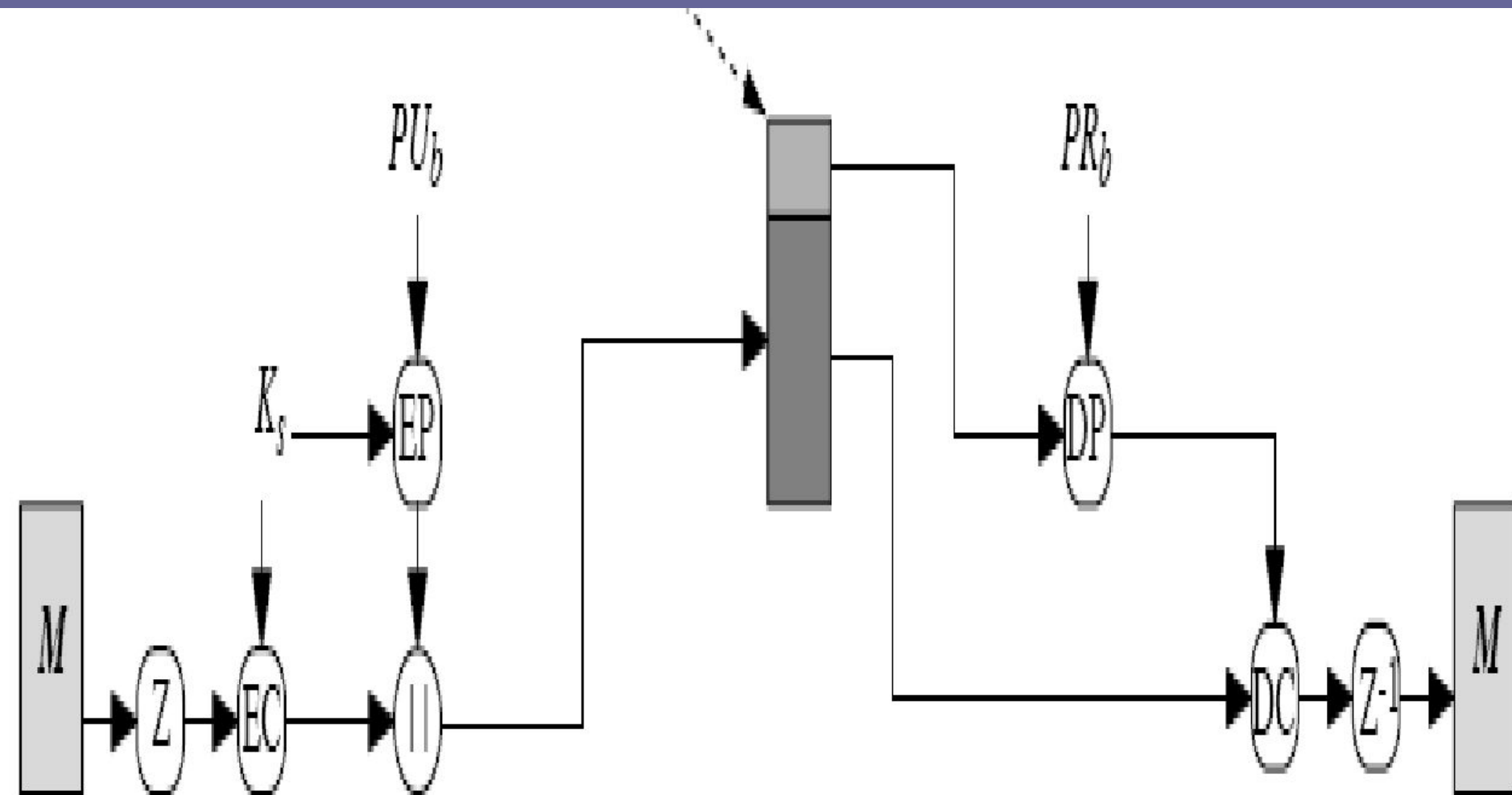
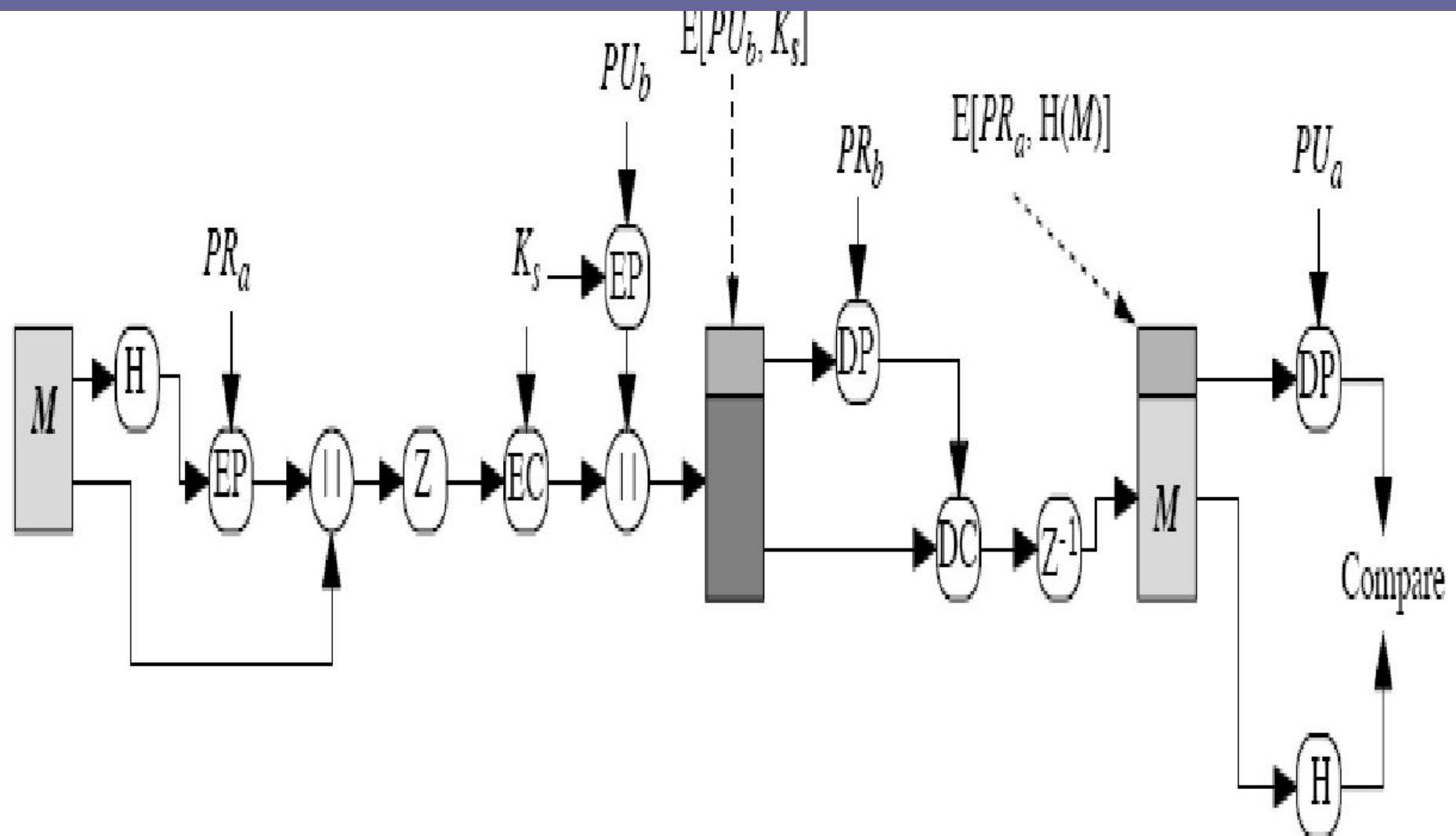


Figure 15.1 PGP Cryptographic Functions



(b) Confidentiality only

Figure 15.1 PGP Cryptographic Functions



(c) Confidentiality and authentication

PGP Session Keys

- need a session key for each message
 - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- generated using ANSI X12.17 mode
- uses random inputs taken from previous uses and from keystroke timing of user



PGP Public & Private Keys

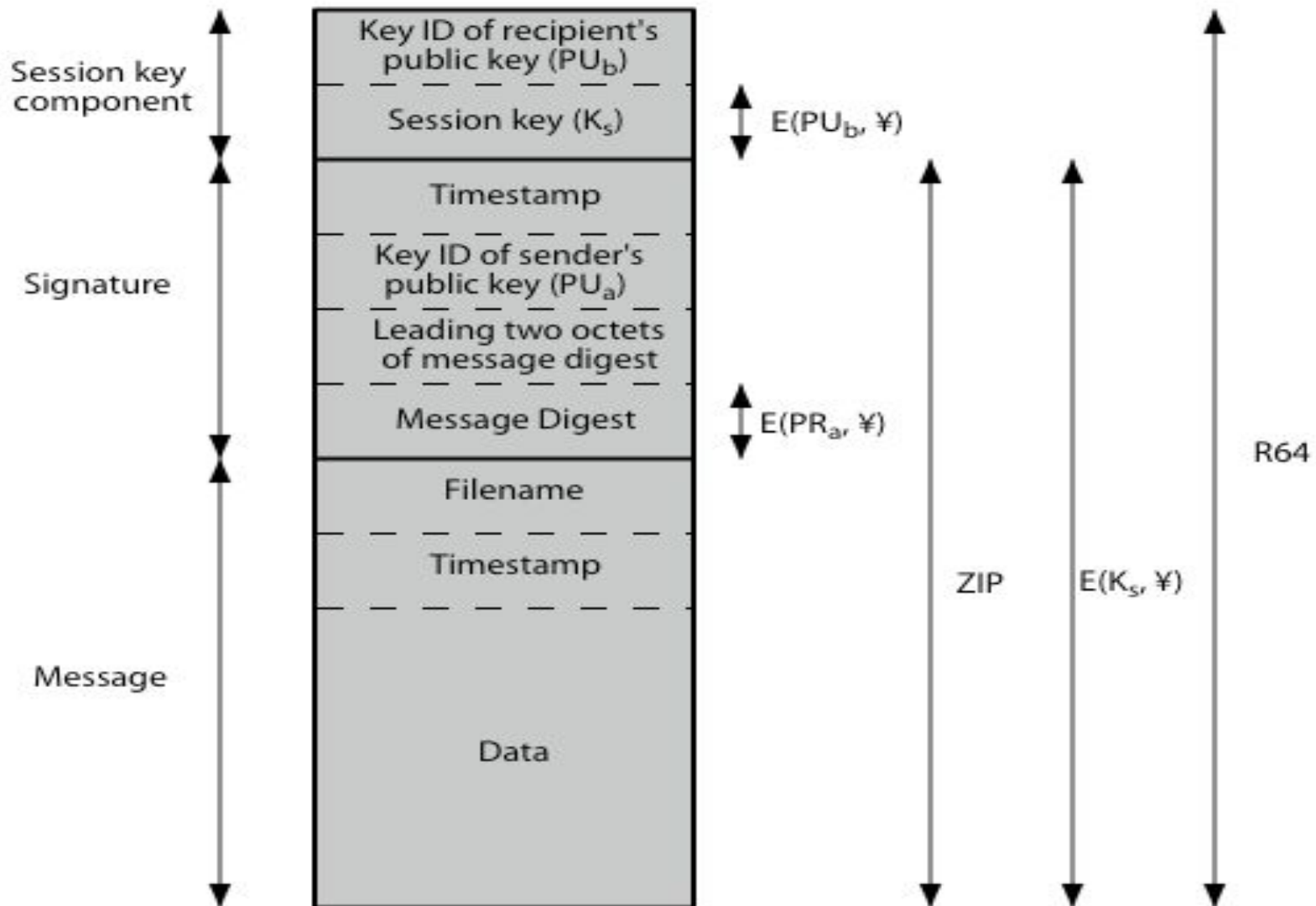
- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
 - could send full public-key with every message
 - but this is inefficient
- rather use a key identifier based on key
 - is least significant 64-bits of the key
 - will very likely be unique
- also use key ID in signatures



PGP Message Format

Content

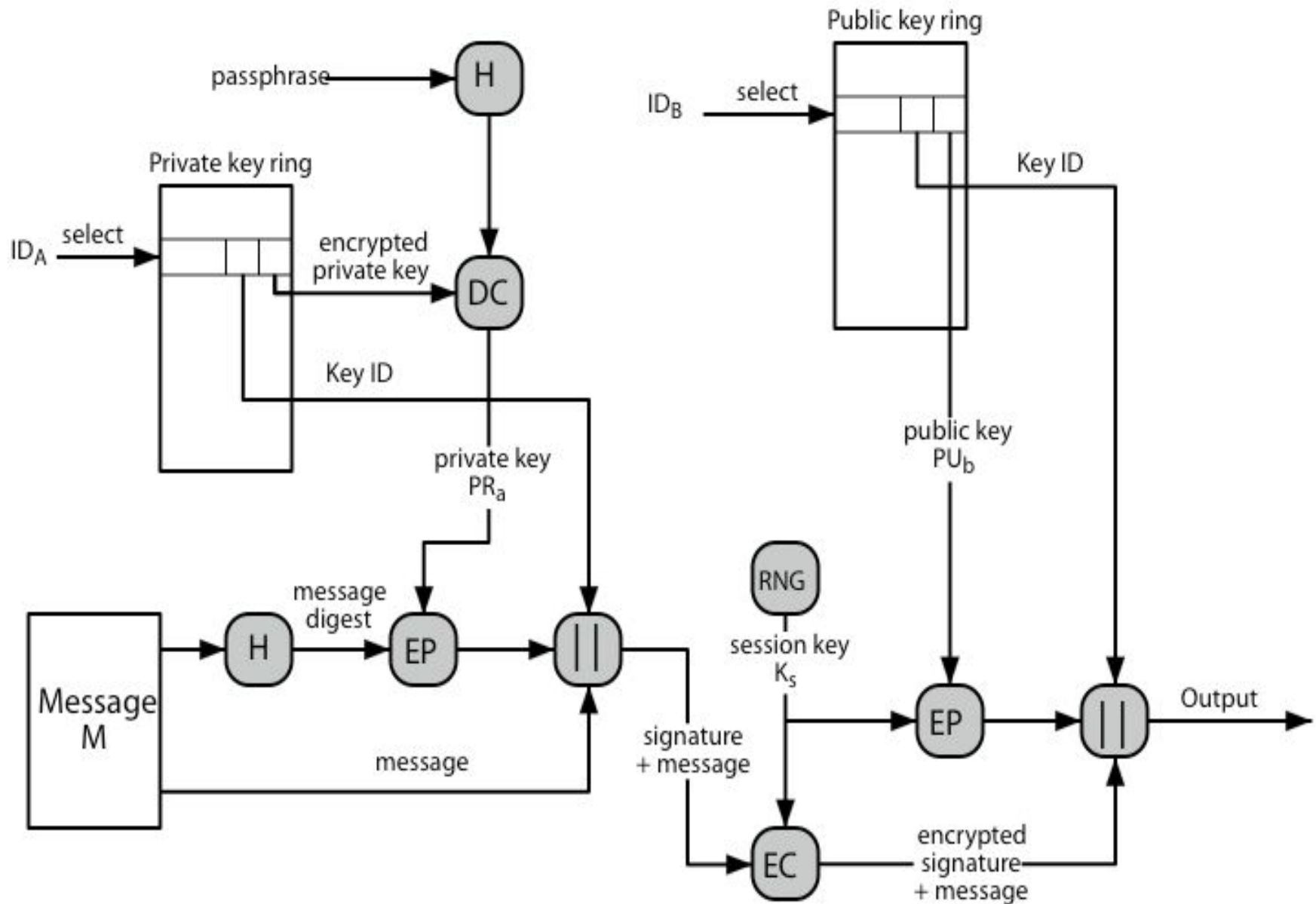
Operation



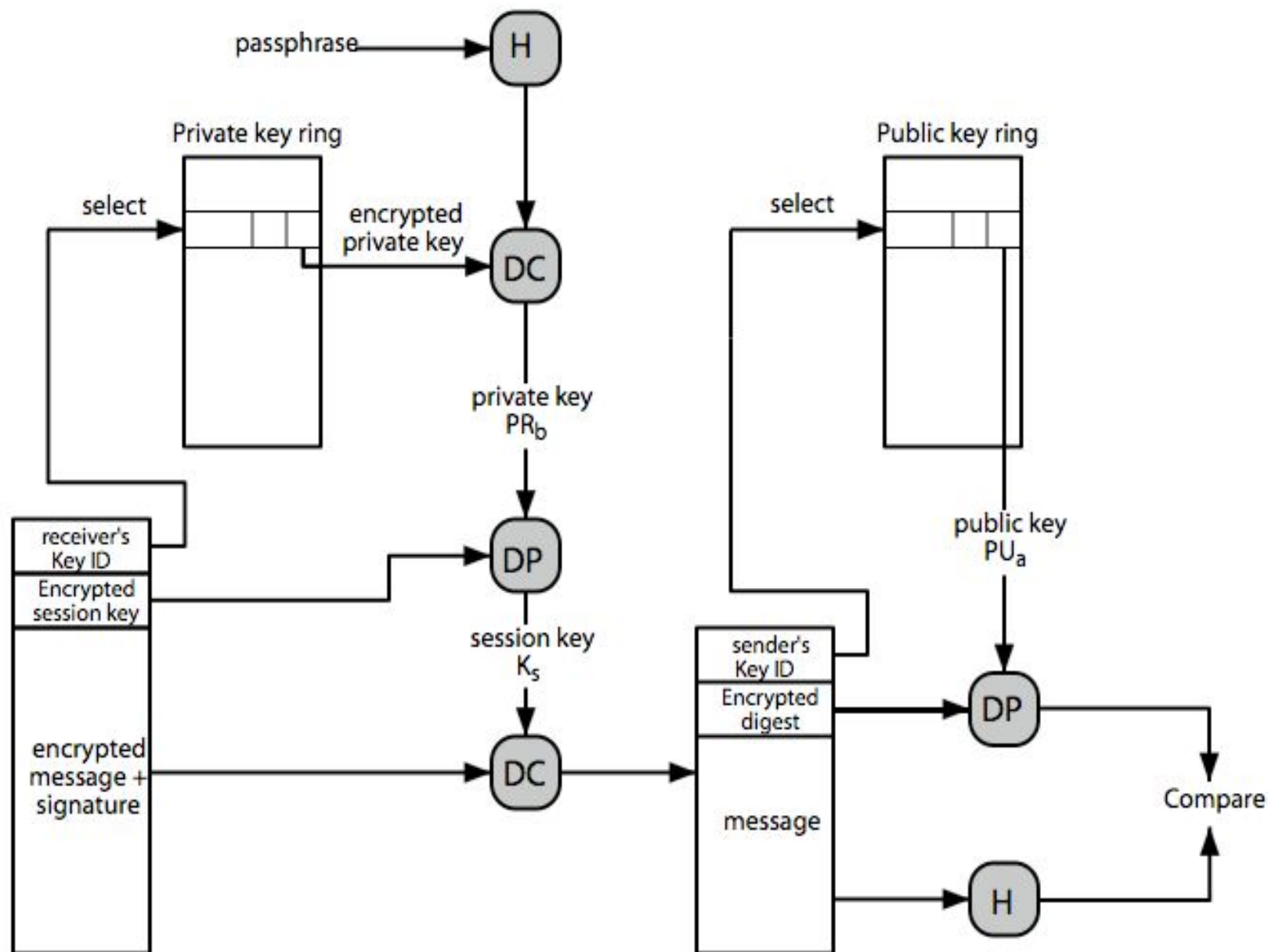
PGP Key Rings

- each PGP user has a pair of keyrings:
 - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
 - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase
- security of private keys thus depends on the pass-phrase security

PGP Message Generation



PGP Message Reception



PGP Key Management

- ❑ rather than relying on certificate authorities
- ❑ in PGP every user is own CA
 - can sign keys for users they know directly
- ❑ forms a “web of trust”
 - trust keys have signed
 - can trust keys others have signed if have a chain of signatures to them
- ❑ key ring includes trust indicators
- ❑ users can also revoke their keys



General Structure of Private and Public Key Rings

Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	$PU_i \bmod 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

General Structure of Private and Public Key Rings

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag _i	User i	trust_flag _i		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

* = field used to index table

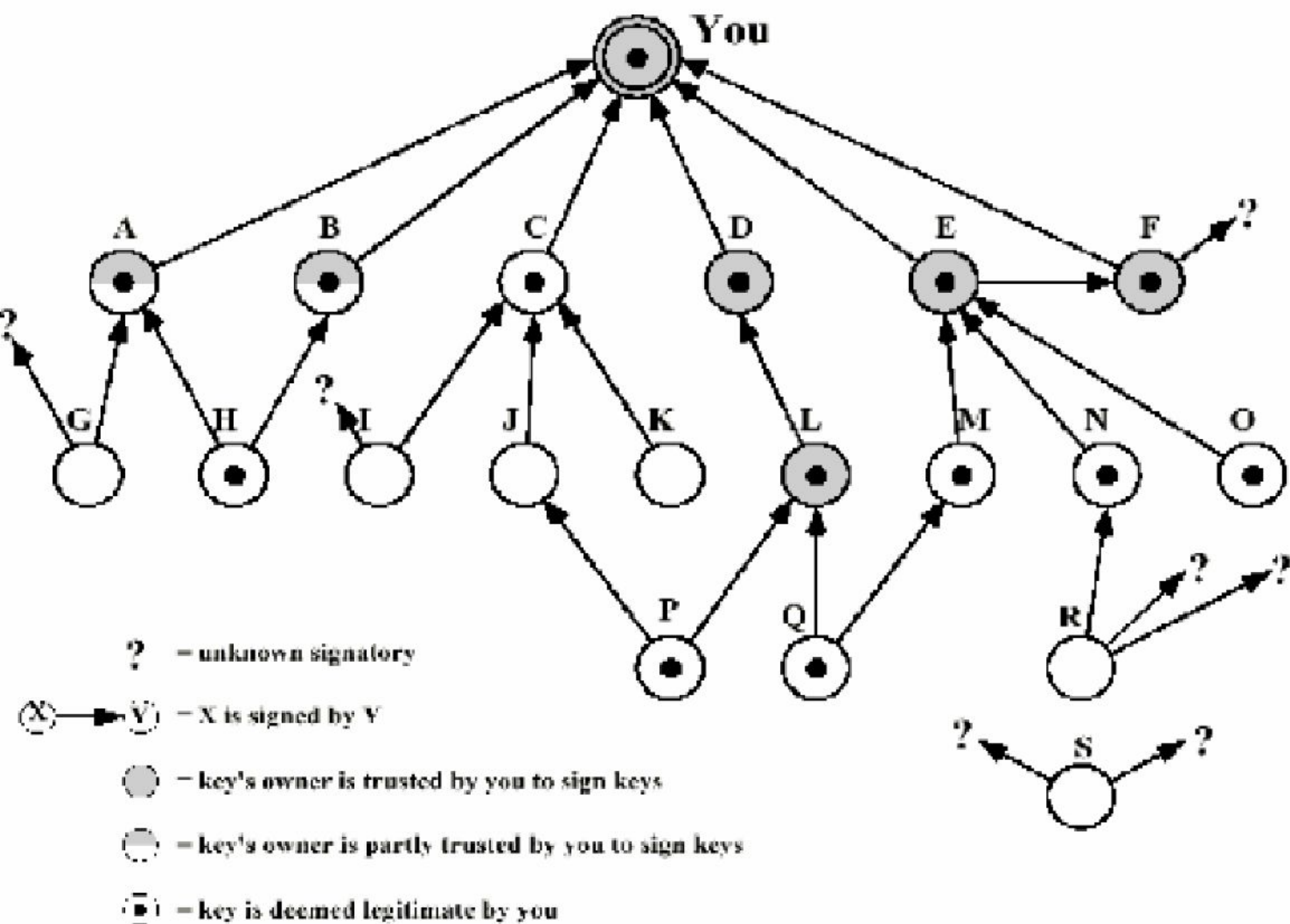


Figure 12.7 PGP Trust Model Example

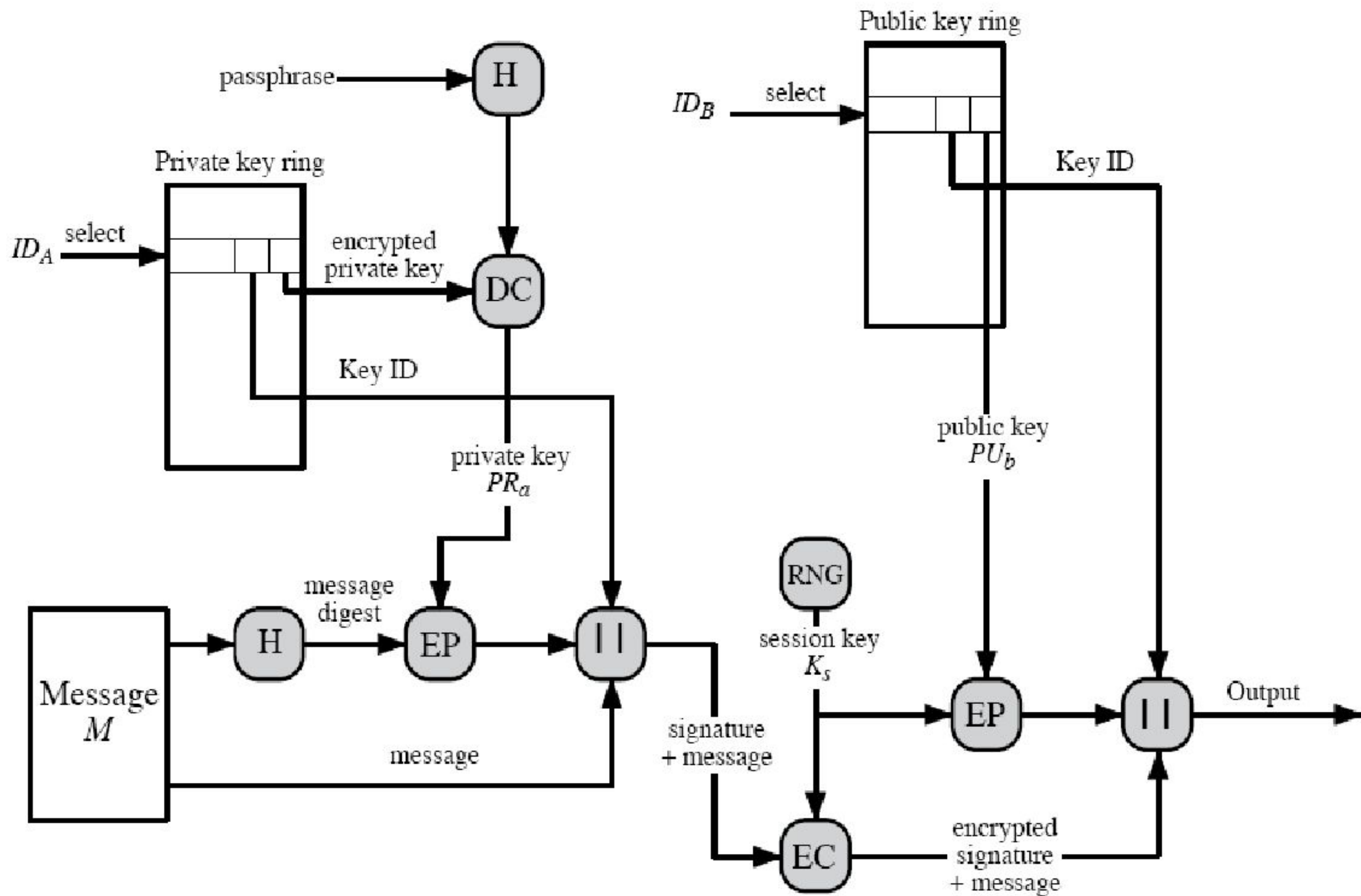


Figure 15.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

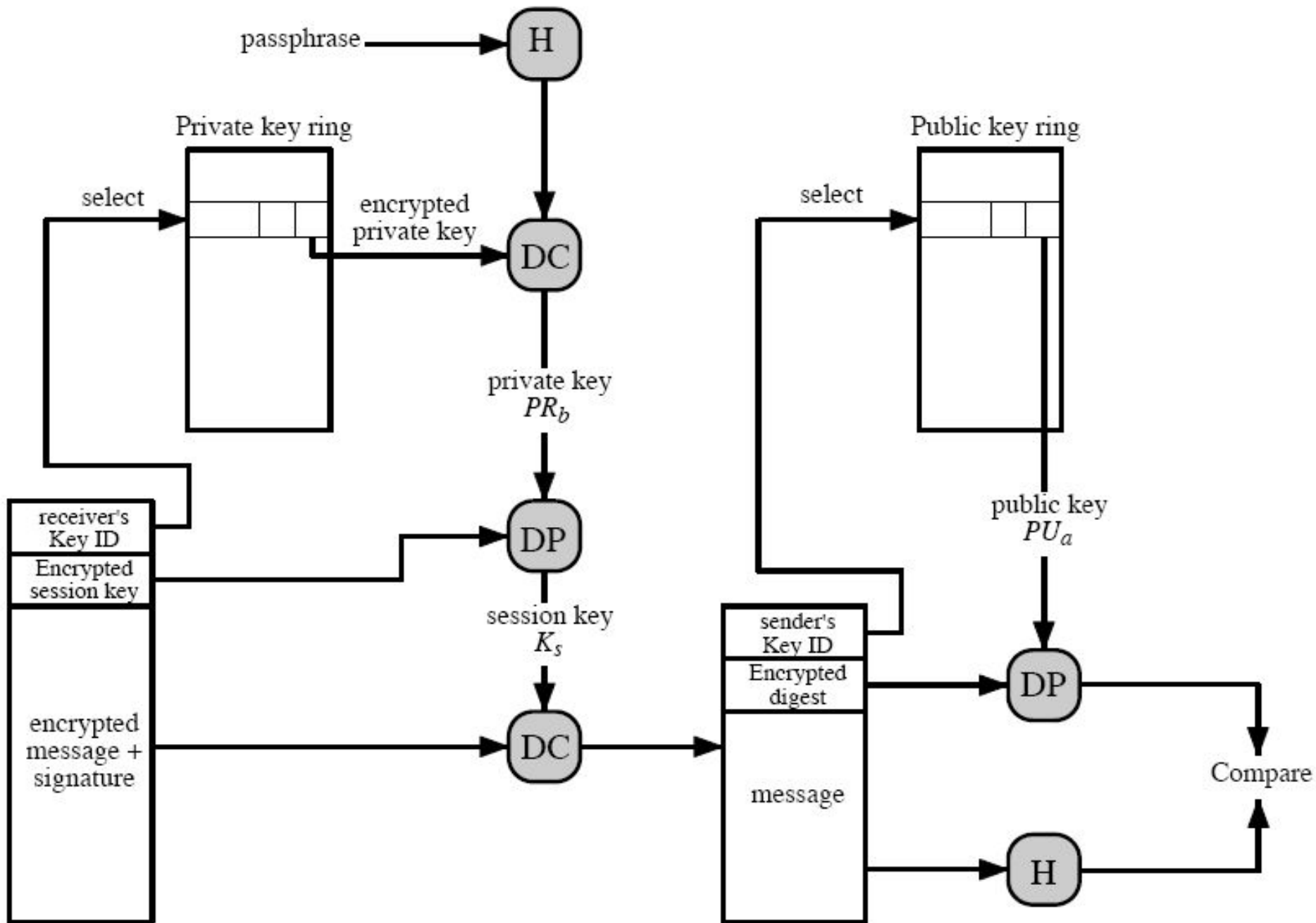


Figure 15.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
 - original Internet RFC822 email was text only
 - MIME provided support for varying content types and multi-part messages
 - with encoding of binary data to textual form
 - S/MIME added security enhancements
- have S/MIME support in many mail agents
 - eg MS Outlook, Mozilla, Mac Mail etc

Secure e-mail: S/MIME

- uses X.509v3 certificates for authentication, integrity and confidentiality

signed

text
Excel table
Word doc
digital signature in S/MIME format

encrypted

text
Excel table
Word doc
encrypted envelope in S/MIME format

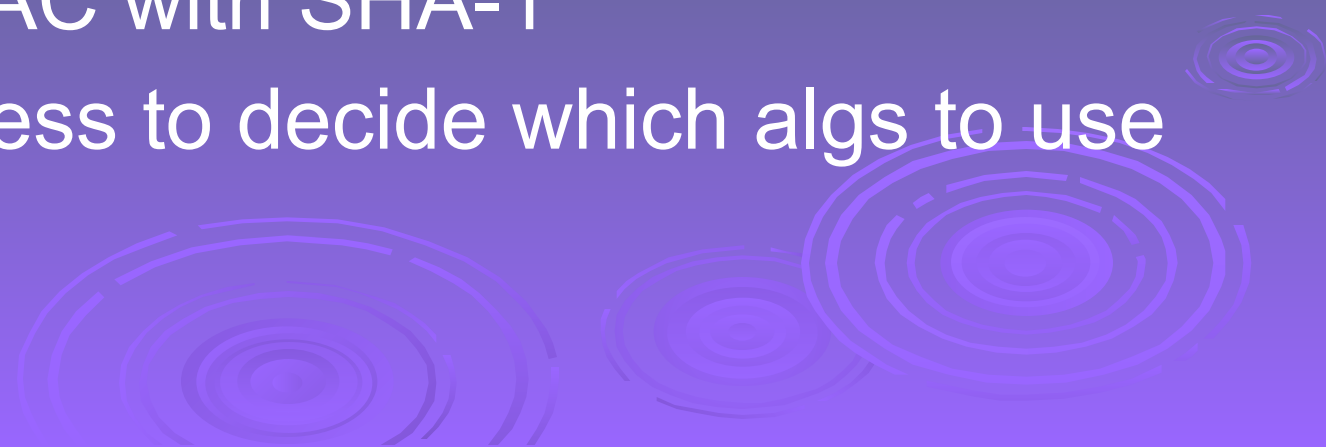
*signed and
encrypted*

text
Excel table
Word doc
digital signature in S/MIME format
encrypted envelope in S/MIME format


S/MIME Functions

- enveloped data
 - encrypted content and associated keys
- signed data
 - encoded message + signed digest
- clear-signed data
 - cleartext message + encoded signed digest
- signed & enveloped data
 - nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

- ❑ digital signatures: DSS & RSA
 - ❑ hash functions: SHA-1 & MD5
 - ❑ session key encryption: ElGamal & RSA
 - ❑ message encryption: AES, Triple-DES, RC2/4 and others
 - ❑ MAC: HMAC with SHA-1
 - ❑ have process to decide which algs to use
- 
- The bottom of the slide features several decorative concentric circles in a lighter shade of purple, resembling ripples in water, positioned in the lower right and bottom center areas.

S/MIME Messages

- S/MIME secures a MIME entity with a signature, encryption, or both
 - forming a MIME wrapped PKCS object
 - have a range of content-types:
 - enveloped data
 - signed data
 - clear-signed data
 - registration request
 - certificate only message
- 
- A decorative graphic in the bottom right corner consisting of several concentric circles, resembling ripples in water, rendered in a light blue color against the dark blue background.

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's



Certificate Authorities

- have several well-known CA's
- Verisign one of most widely used
- Verisign issues several types of Digital IDs
- increasing levels of checks & hence trust

Class Identity Checks Usage

- 1 name/email check web browsing/email
- 2 + enroll/addr check email, subs, s/w validate
- 3 + ID documents e-banking/service access

Table 15.3 MIME Content Types

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript
	octet-stream	General binary data consisting of 8-bit bytes.

Table 15.9 Radix-64 Encoding

6-bit value	character encoding	6-bit value	character encoding	6-bit value	character encoding	6-bit value	character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

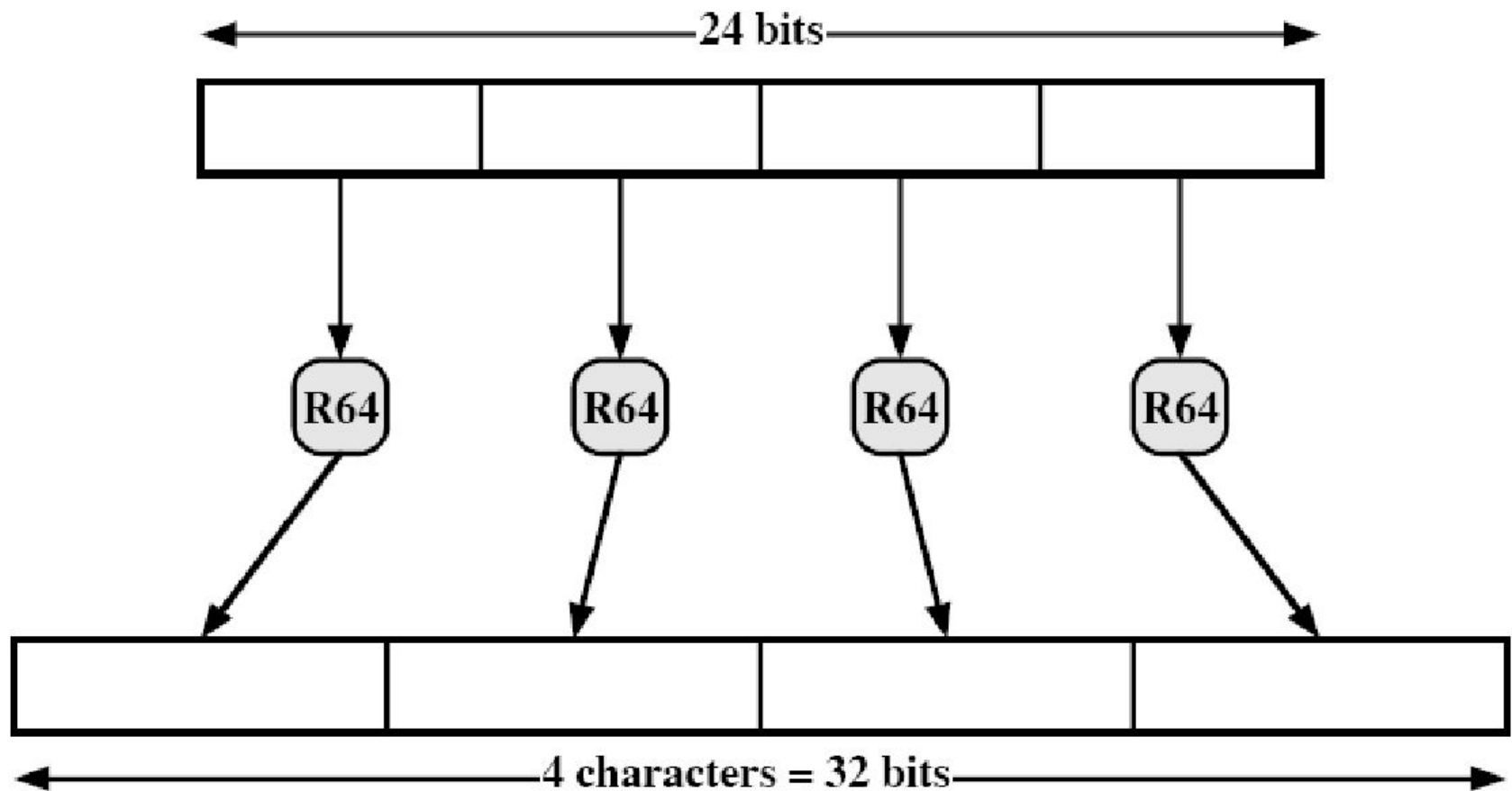
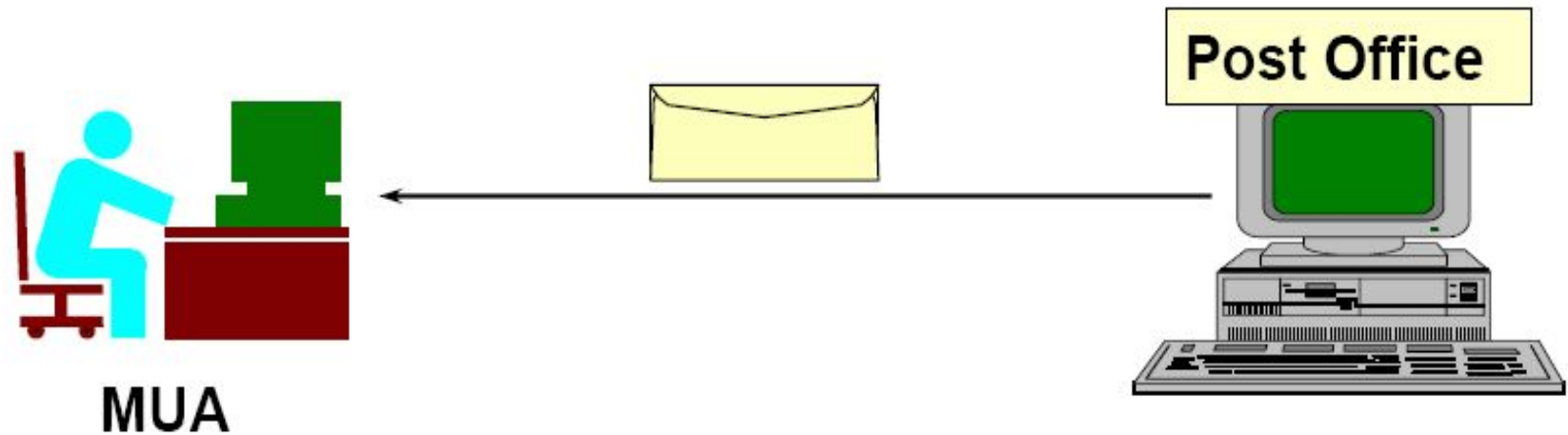


Figure 15.11 Printable Encoding of Binary Data into Radix-64 Format

Secure e-mail download



- IMAP or POP over SSL/TLS
- IMAPS or POPS provides:
 - user authentication
 - server authentication
 - mail confidentiality/integrity during transfer

Summary

- have considered:
 - secure email
 - PGP
 - S/MIME

