Unit 4

Electronic Mail Security

Electronic Mail Security

This section discusses two protocols providing security services for e-mails:

1.Pretty Good Privacy (PGP) and

2. Secure/Multipurpose Internet Mail Extension (S/MIME).

OBJECTIVES :

- To introduce “Internet security” at the Application Level, and two protocols, PGP and S/MIME, that implement that idea.
- To show how PGP and S/MIME can provide confidentiality and message authentication.

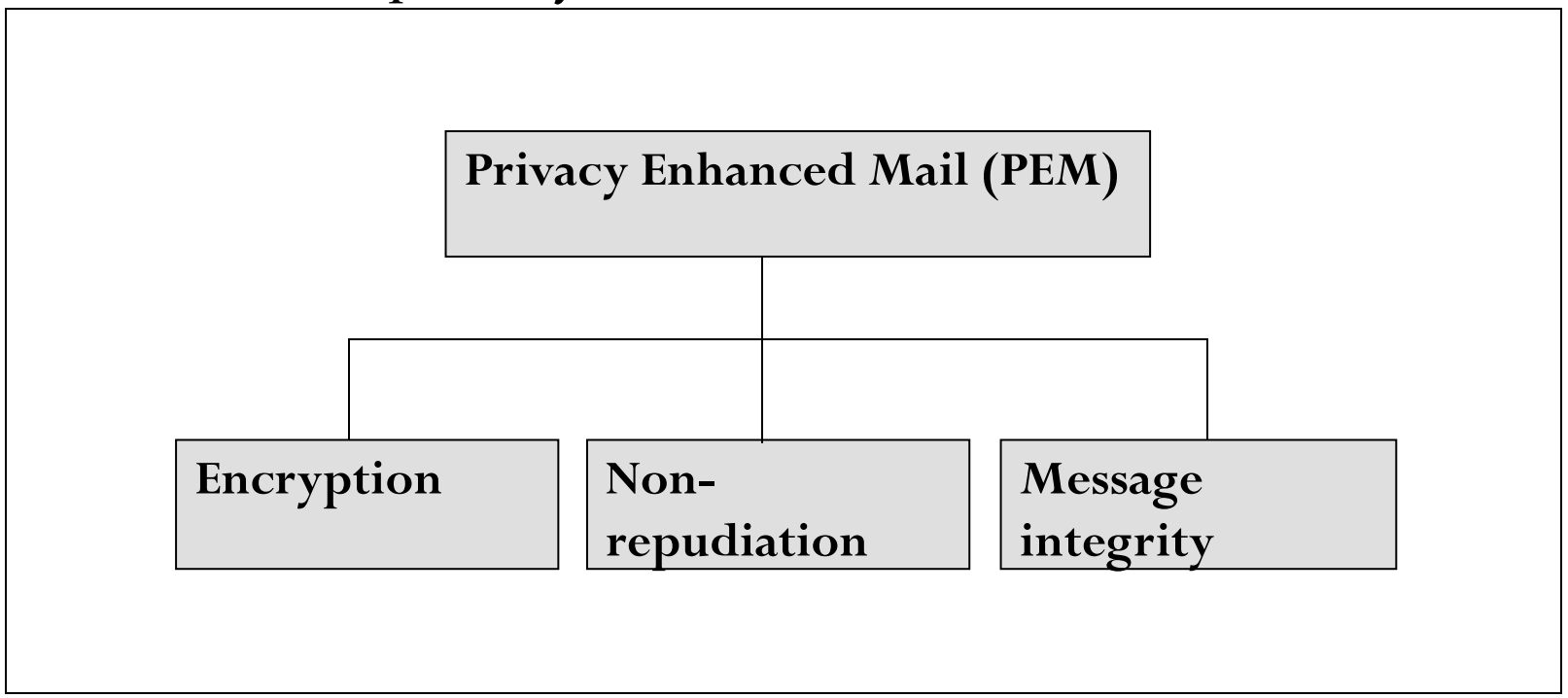
Topics Discussed in the Section

- ✓ E-mail Security
- ✓ Pretty Good Privacy (PGP)
- ✓ Key Rings
- ✓ PGP Certificates
- ✓ S/MIME
- ✓ Applications of S/MIME

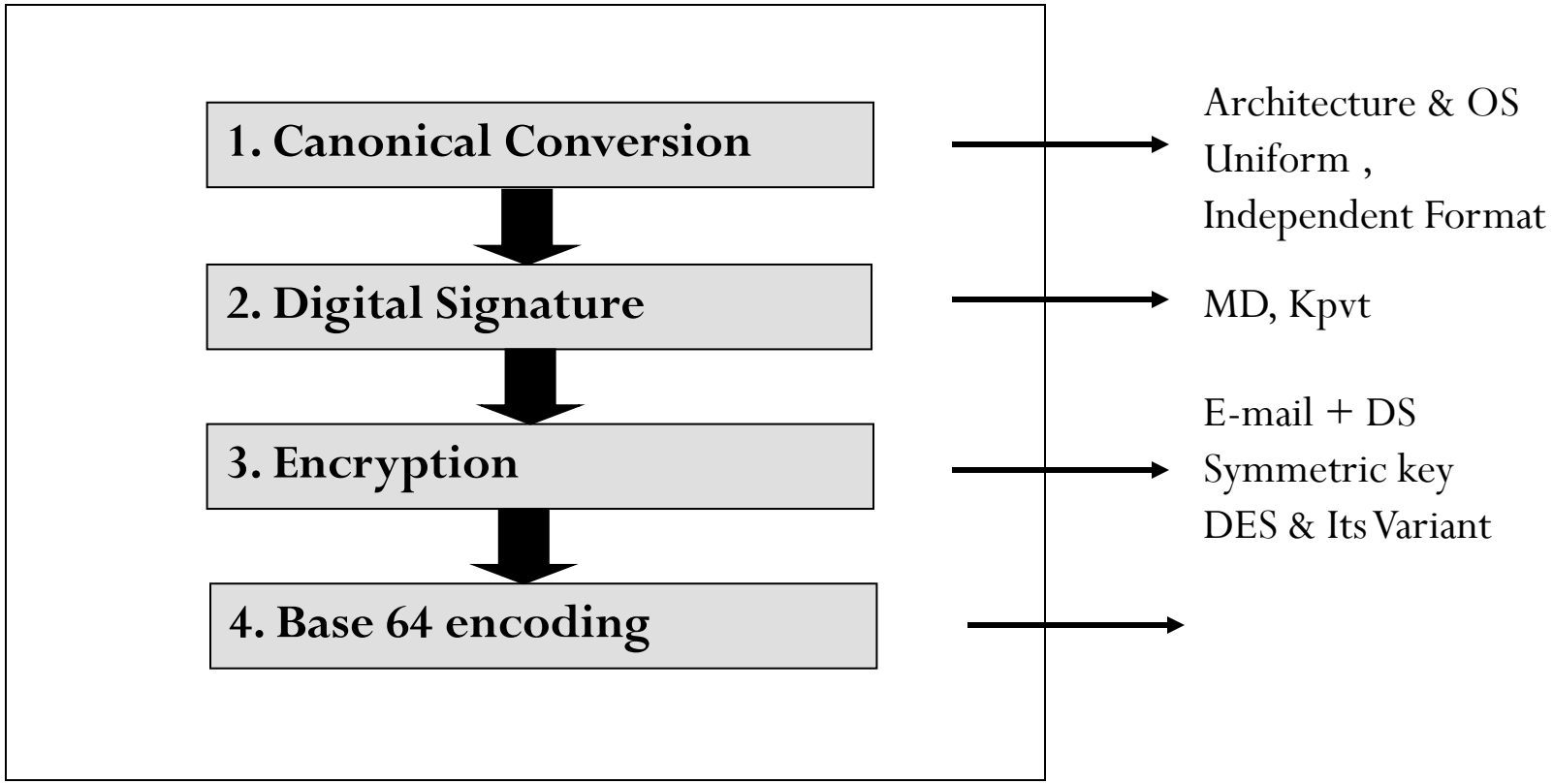
PEM Security Features

- Initially developed by IETF & Privacy Security Research Group.

- Standard adopted by Internet Architecture Board.



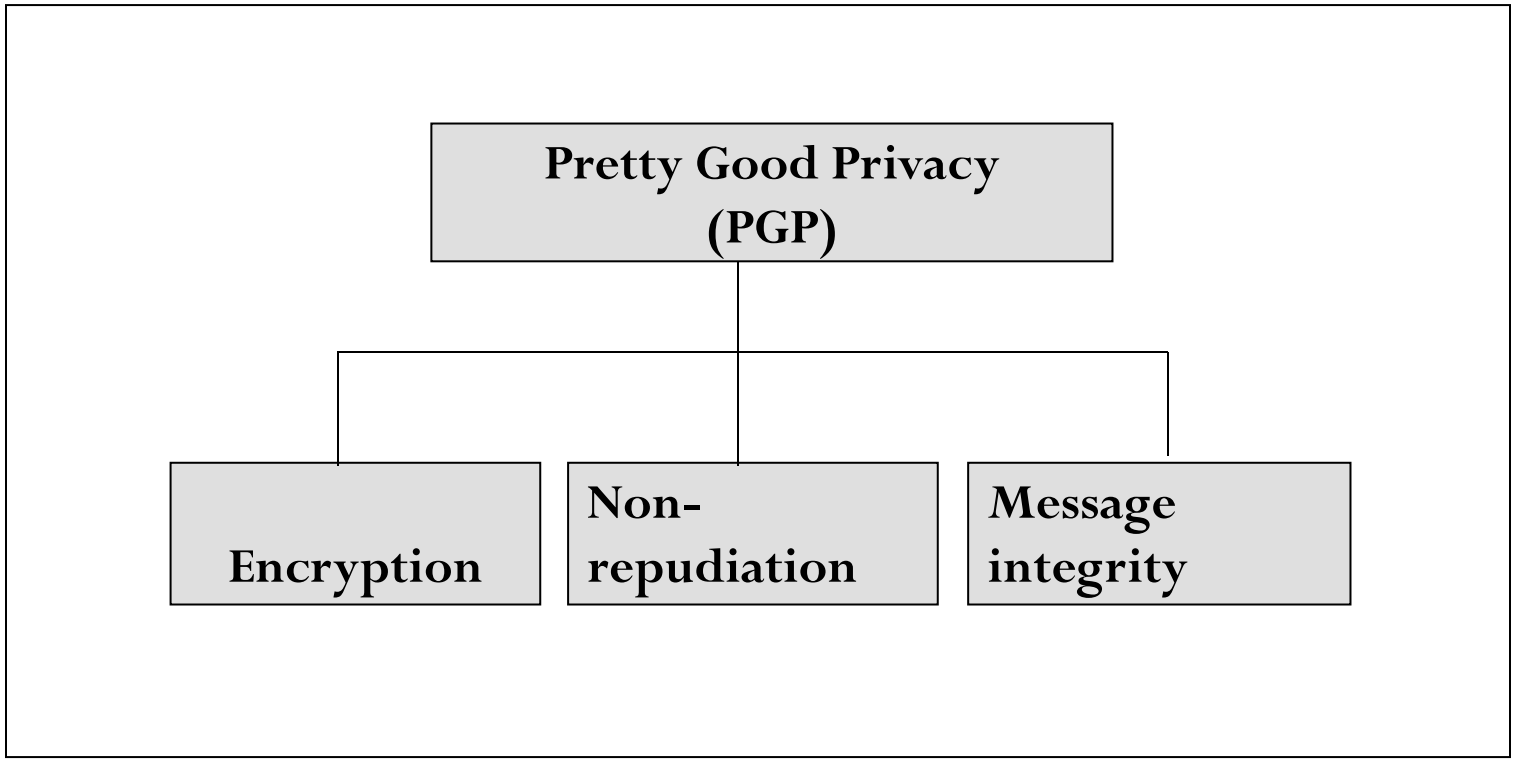
PEM Operations



Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- Supports the basic requirements of cryptography.
- Simple to use
- Completely Free

PGP Security Features



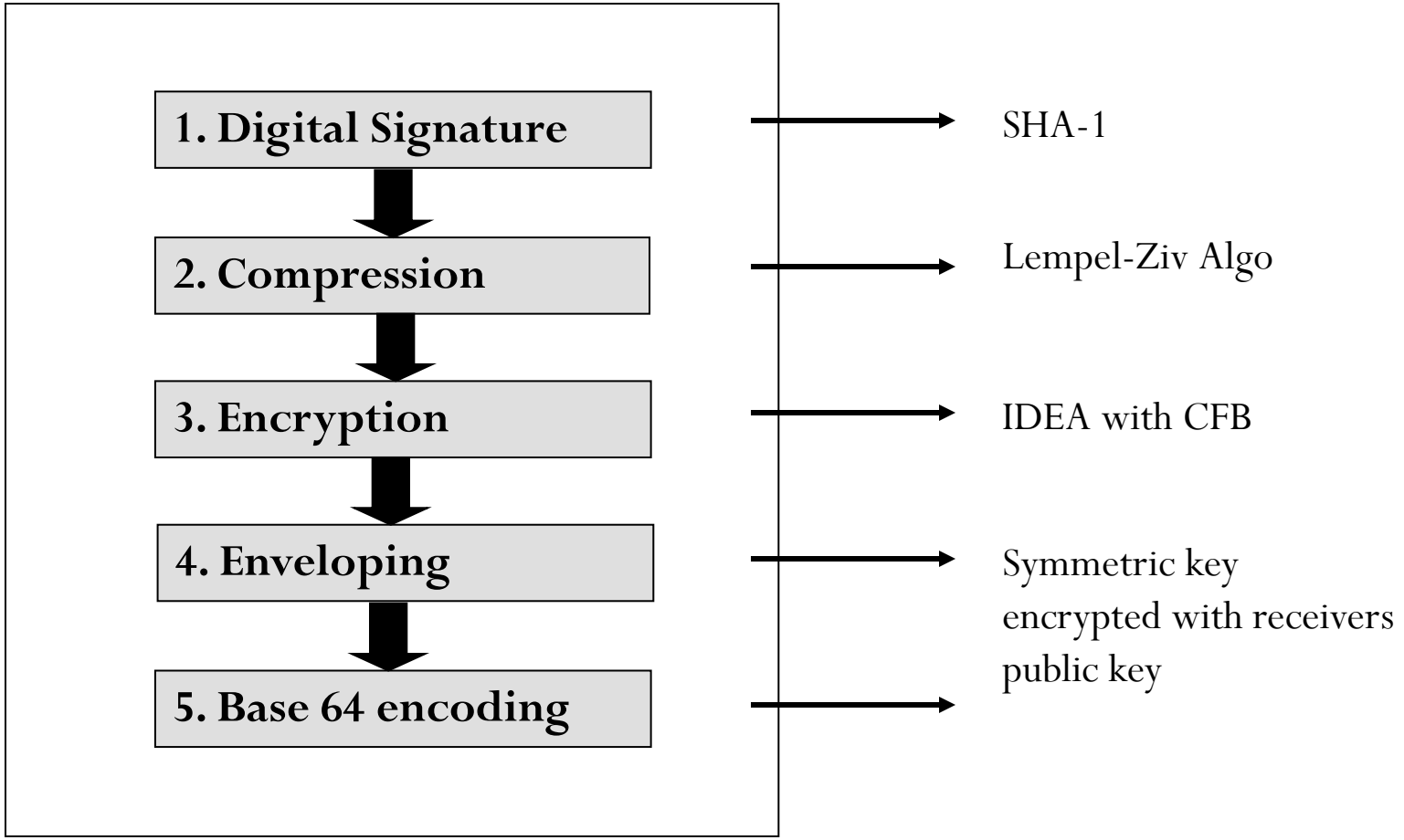
Note

In e-mail security, the sender of the message needs to include the name or identifiers of the algorithms used in the message,along with the value of key.

PGP Algorithm

Algorithm Type	Description
Asymetric Key	RSA,DSS
Message Digest	MD5,SHA-1,RIPE-MD
Encryption	IDEA,DES-3,AES

PGP Operations

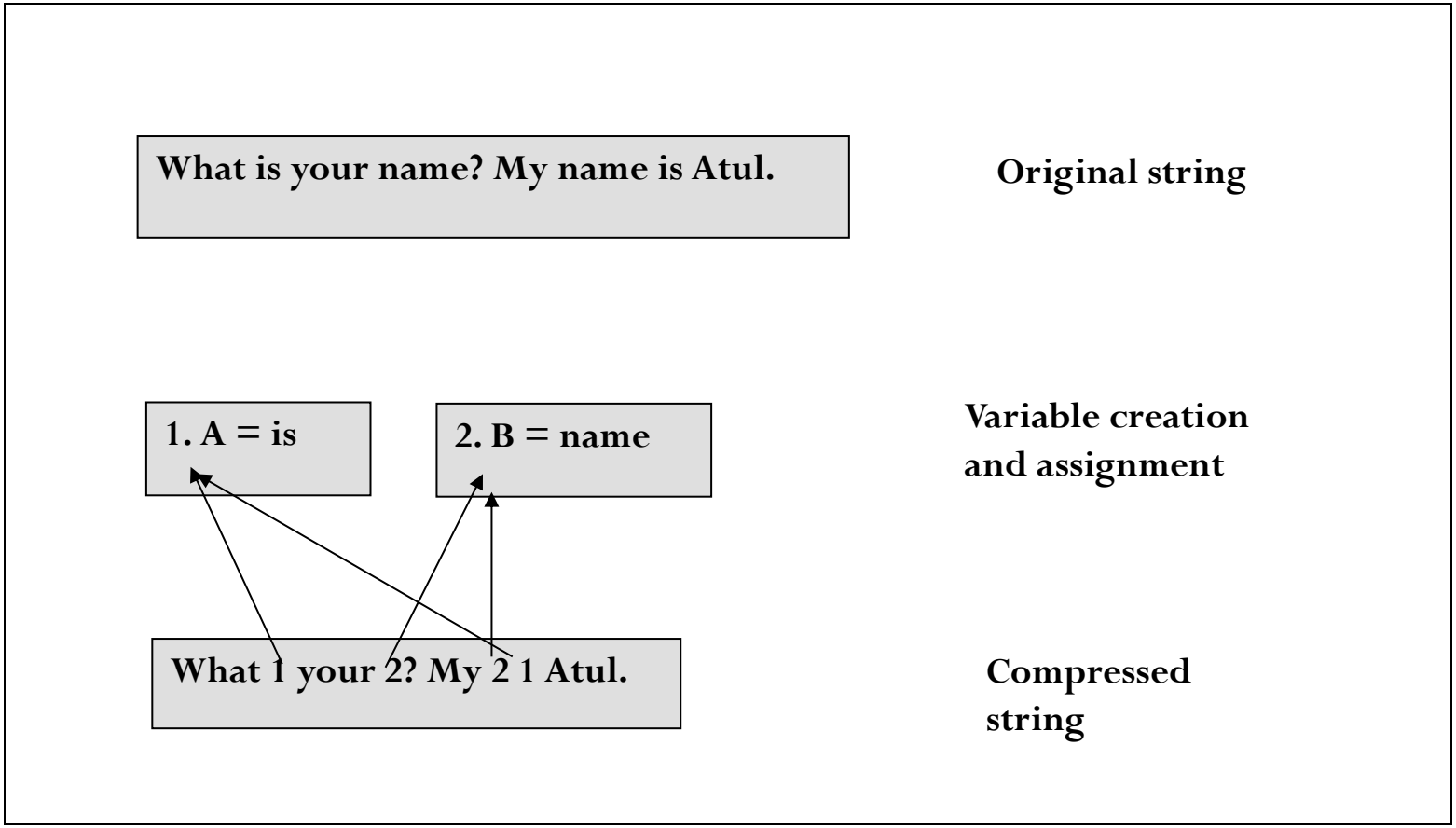


PGP Security Options

- While sending an E-mail Message following Security Option can be choosen:

- Signature Only (Step 1 and 2)
- Signature and Base-64 encoding(Step 1,2 and 5)
- All 5 steps

Step 2: Lempel-Ziv Algorithm (Zip)

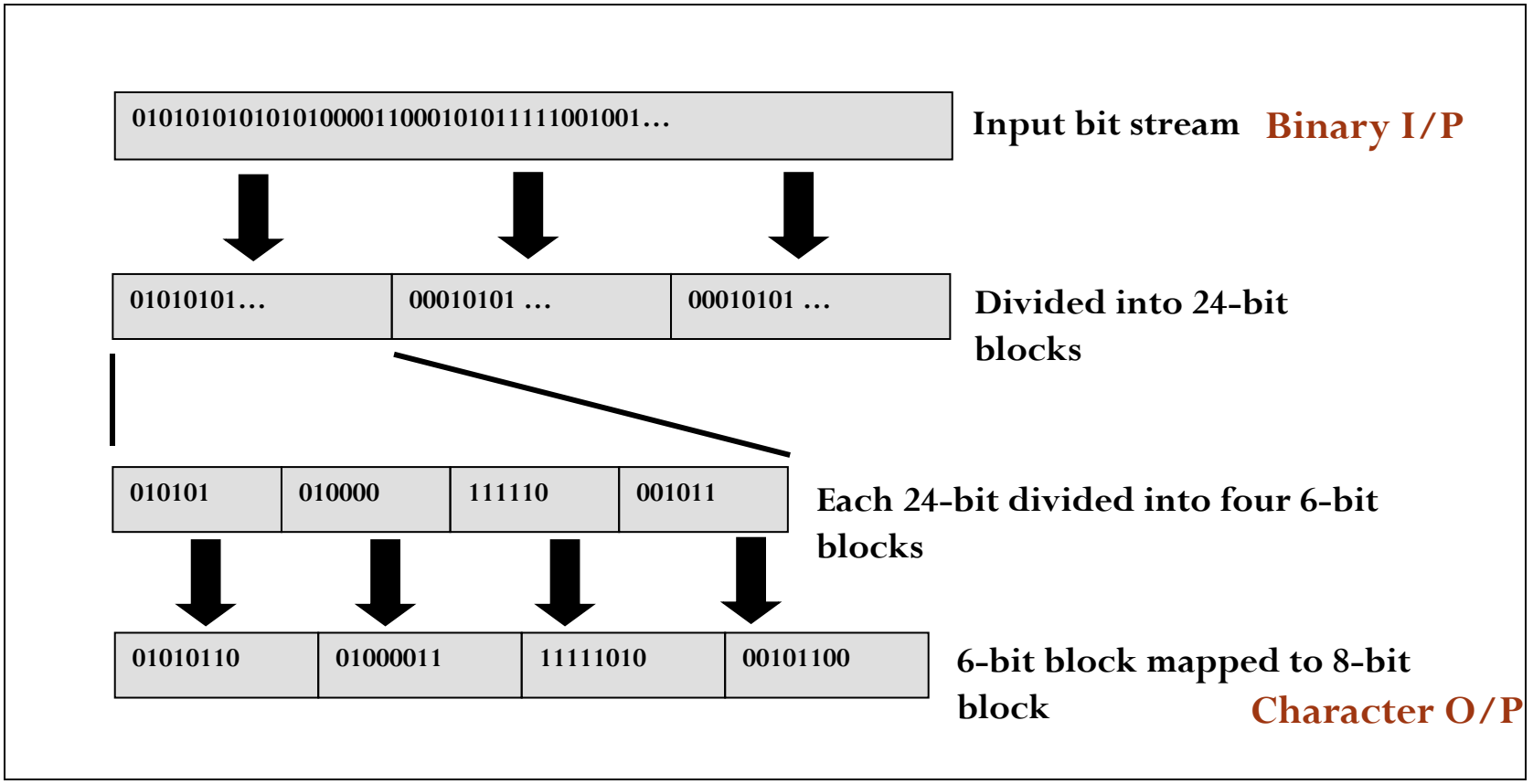


Step 4: Formation of digital Envelope

Envelope

In e-mail security, the encryption/decryption is done using a symmetric-key algorithm, but the secret key to decrypt the message is
encrypted with the public key of the receiver and is sent with the message.

Step 5:Base-64 Encoding Concept



base64_encoding_table.

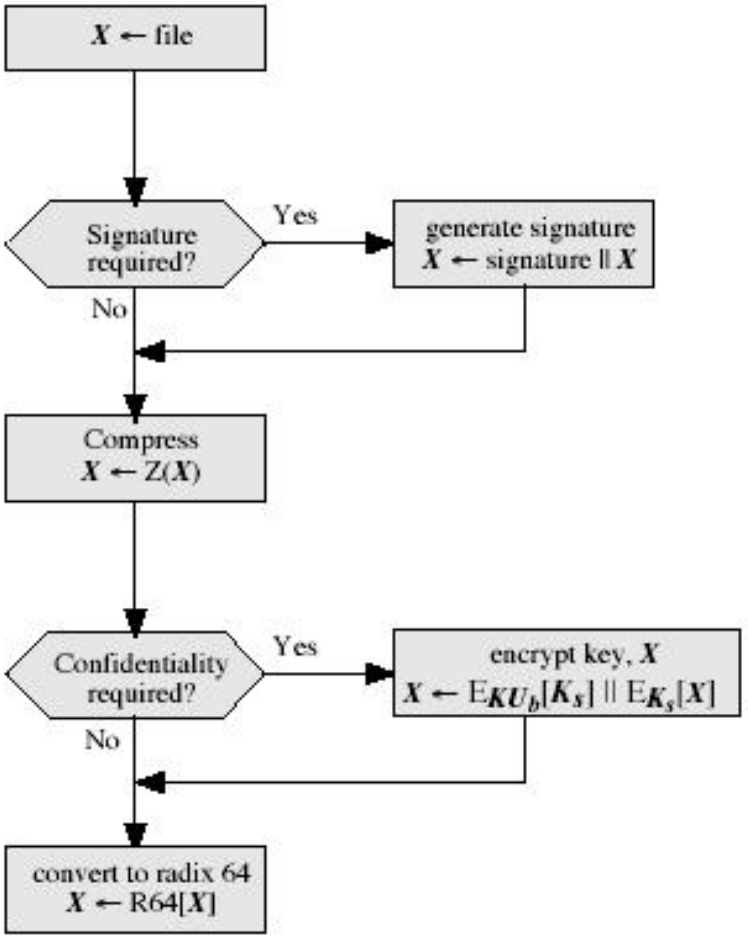
Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z
011010	a
011011	b
011100	c
011101	d
011110	e
011111	f

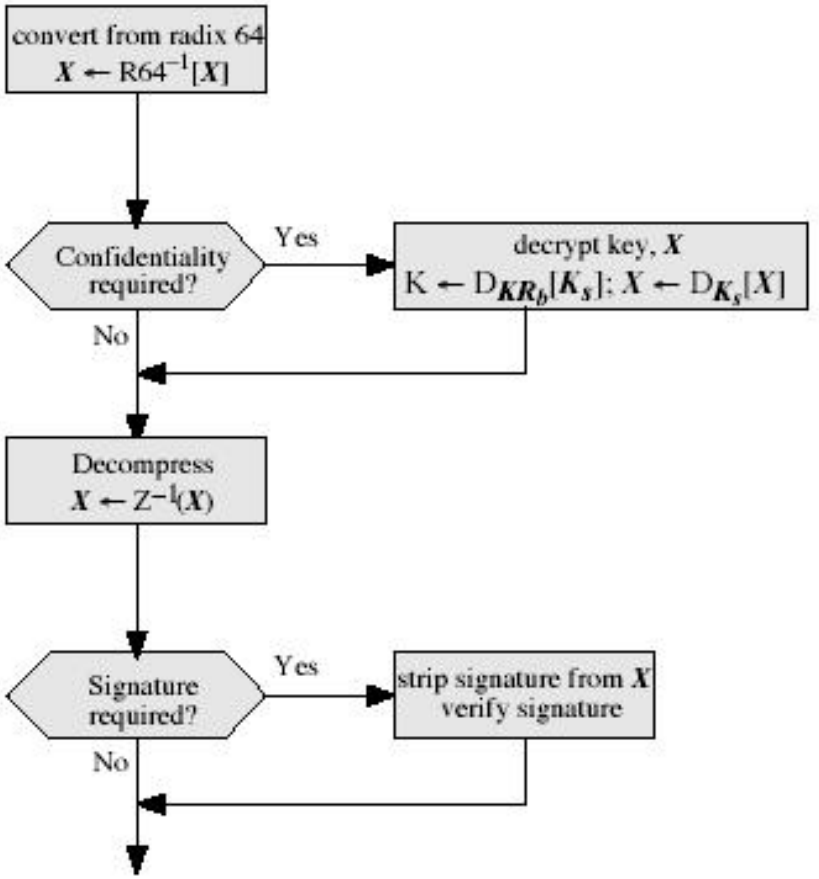
Binary	ASCII
100000	g
100001	h
100010	i
100011	j
100100	k
100101	l
100110	m
100111	n
101000	o
101001	p
101010	q
101011	r
101100	s
101101	t
101110	u
101111	v

Binary	ASCII
110000	w
110001	x
110010	y
110011	z
110100	0
110101	1
110110	2
110111	3
111000	4
111001	5
111010	6
111011	7
111100	8
111101	9
111110	+
111111	/

PGP Operations



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

(MIME)
Multipurpose Internet Mail Extensions

- **Traditional email communication is text-only**
- **Modern email communication demands multimedia (sound, video, pictures, etc)**
- **Enhancements provided in the form of MIME**

MIME Extensions to Email

From: Atul Kahate <akahate@yahoo.com>
To: Amit Joshi<amit@rediffmail.com>
Subject: Cover image for the book
MIME-Version: 1.0
Content-Type: image/gif → *Mulimedia File*

<Actual image data in the binary form such as R019a0asdjas0 …>

S/MIME Functionalities

- 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 Functionalities

Functionality	*Description*
Enveloped data	Consists of encrypted content of any type, and the encryption key encrypted with the receiver's public key.
Signed data	Consists of a message digest encrypted with the sender's private key. The content and the digital signature are both Base-64 encoded.
Clear-signed data	Similar to Signed data. However, only the digital signature is Base-64 encoded.
Signed and Enveloped data	Signed-only and Enveloped-only entities can be combined, so that the Enveloped data can be signed, or the Signed/Clear-signed data can be enveloped.

The following shows an example of an enveloped-data in which a small message is encrypted using triple DES.

Content-Type: application/pkcs7-mime; mime-type=enveloped-data
Content-Transfer-Encoding: Radix-64
Content-Description: attachment
name="report.txt";
cb32ut67f4bhijHU21oi87eryb0287hmnklsgFDoY8bc659GhIGfH6543mhjkdsaH23YjBnmN
ybmlkzjhgfdyhGe23Kjk34XiuD678Es16se09jy76jHuytTMDcbnmlkjgfFdiuyu678543m0n3h
G34un12P2454Hoi87e2ryb0H2MjN6KuyrlsgFDoY897fk923jljk1301XiuD6gh78EsUyT23y

S/MIME Content Types

Type	Sub-type	Description
Multipart	Signed	A clear signed message consisting of the message and the digital signature.
Application	PKCS#7 MIME Signed Data	A signed MIME entity.
	PKCS#7 MIME Enveloped Data	An enveloped MIME entity.
	PKCS#7 MIME Degenerate Signed Data	An entity that contains only digital certificates. No Content
	PKCS#7 Signature	The content type of the signature subpart of a multipart/signed message.
	PKCS#10 MIME	A certificate registration request.

S/MIME Additional Security Features

- SIGNED RECEIPTS:-
  - Acknowledgement
  - Proof of delivery
- SECURITY LABLE:-
  - Sensitivity
  - Access control
  - Priority
- SECURE MAILING LISTS:-
  - Mailing List Agent(MLA)
  - Used when their is N no. of Recipient

Sender → MLA → Receive

Figure 30.22 *A plaintext message*

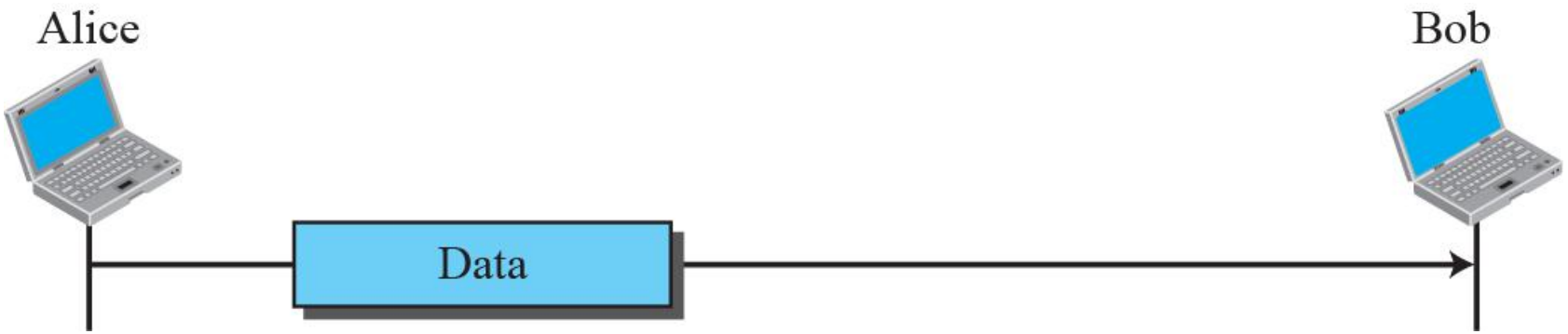


Figure 30.23 *An authenticated message*

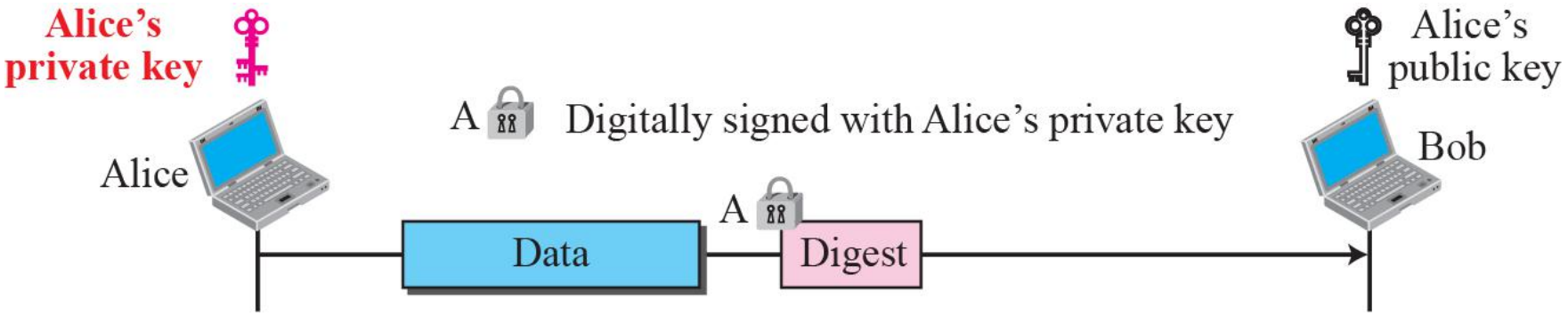


Figure 30.24 *A compressed message*

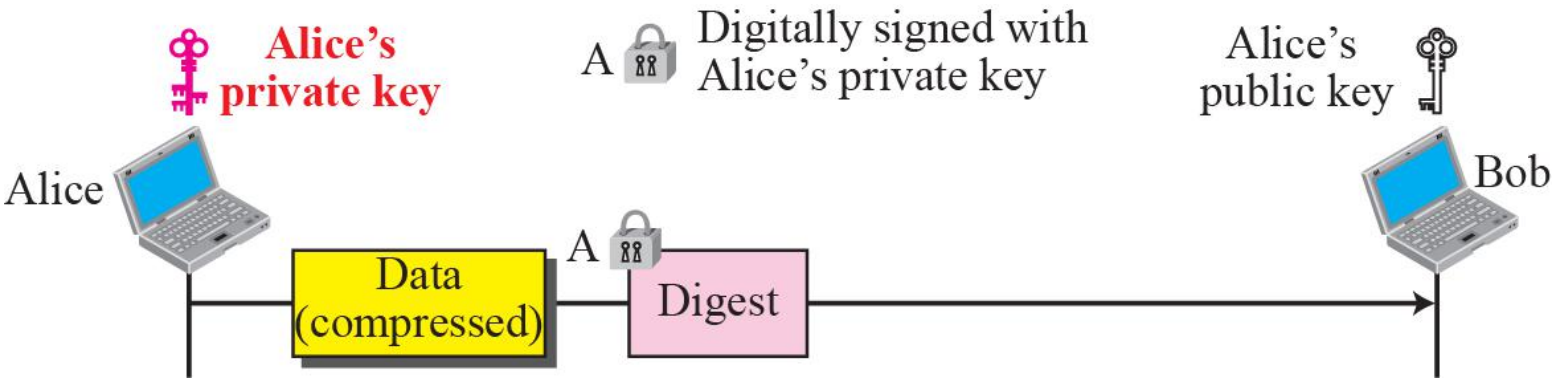


Figure 30.25 *A confidential message*

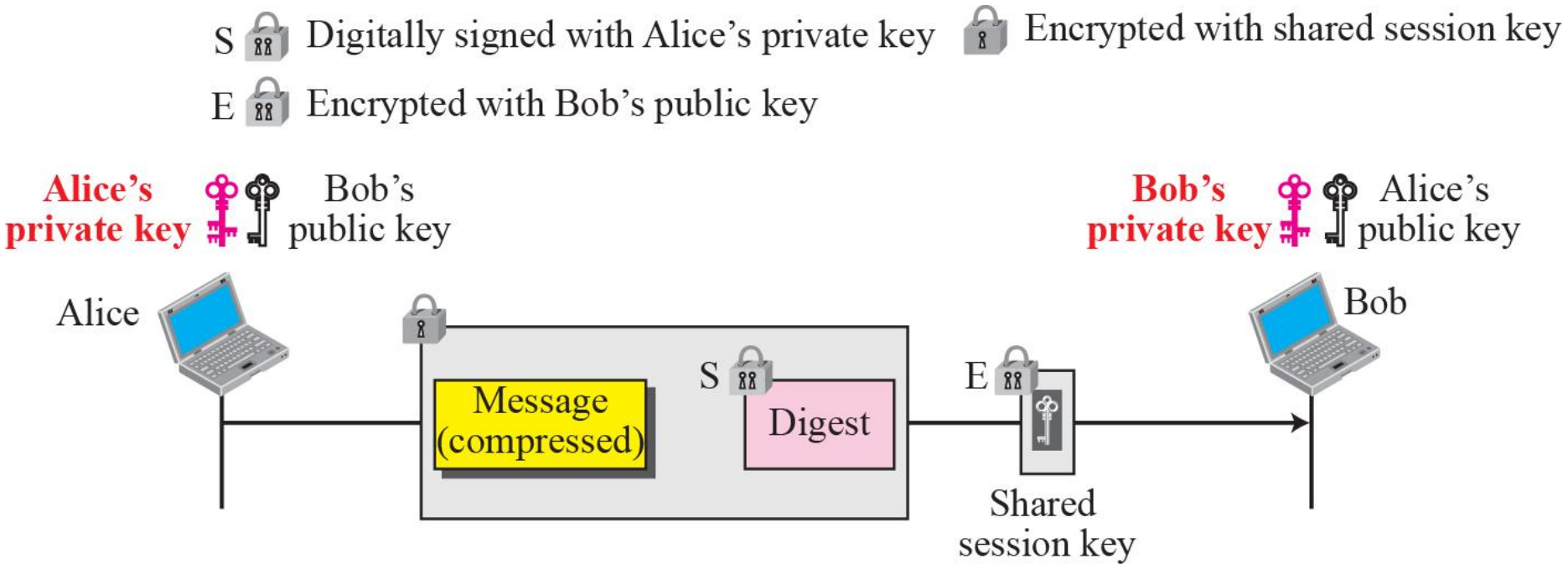


Figure 30.26 *Key rings in PGP*

Note

In PGP, there can be multiple paths from fully or partially trusted authorities to any subject.

Figure 30.27 *Trust model*

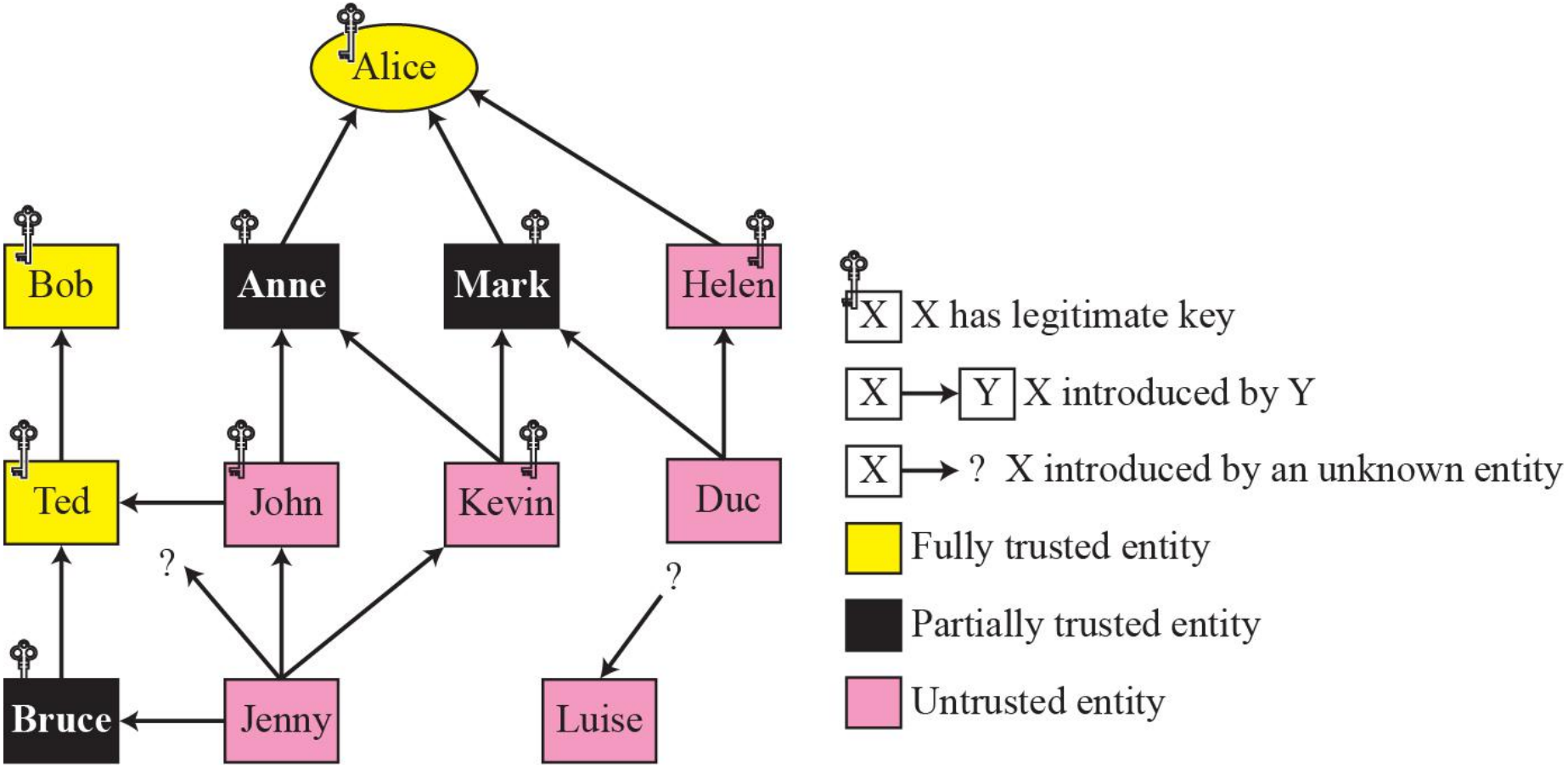


Figure 30.28 *Signed-data content type*

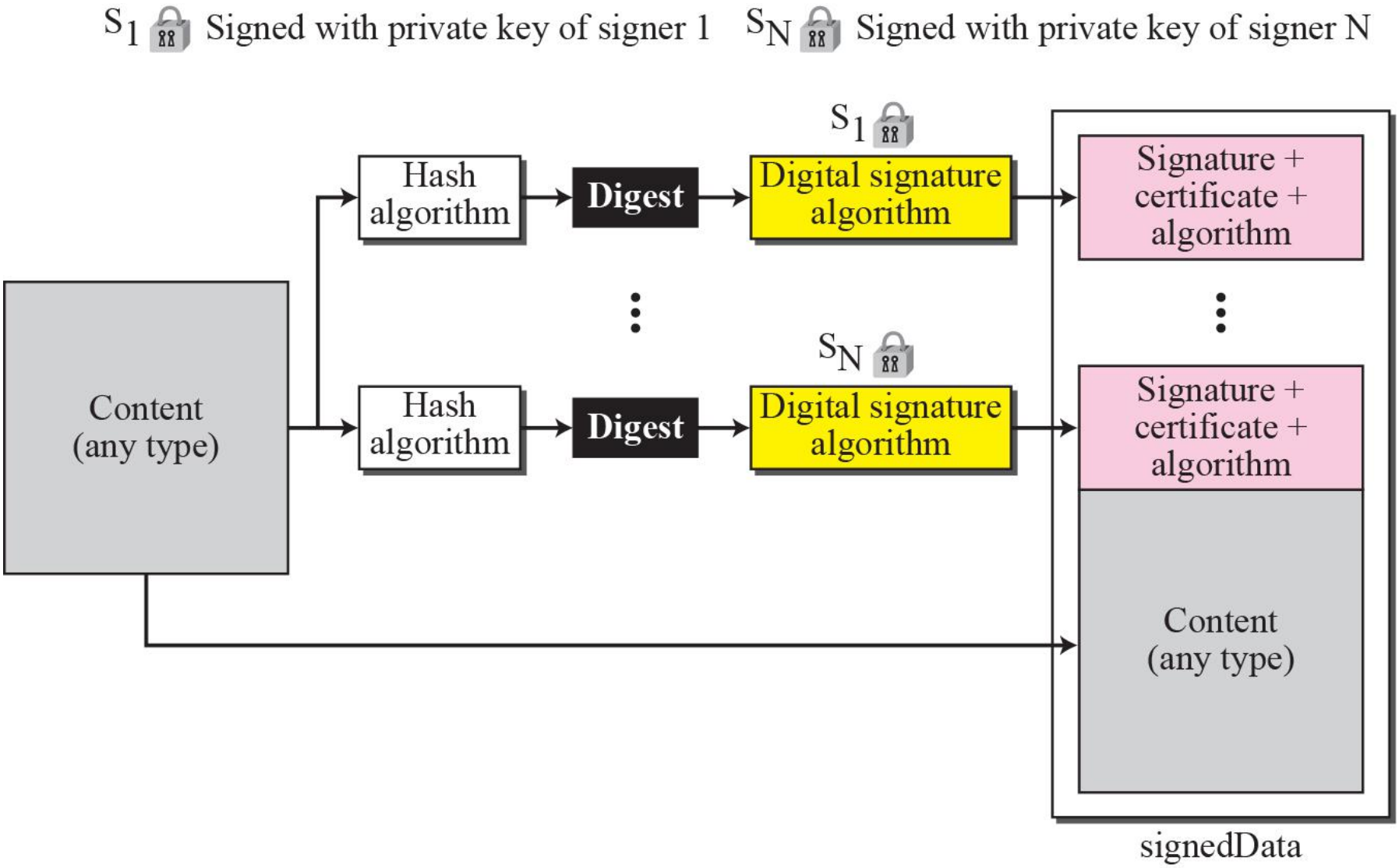


Figure 30.29 *Encrypted-data content type*

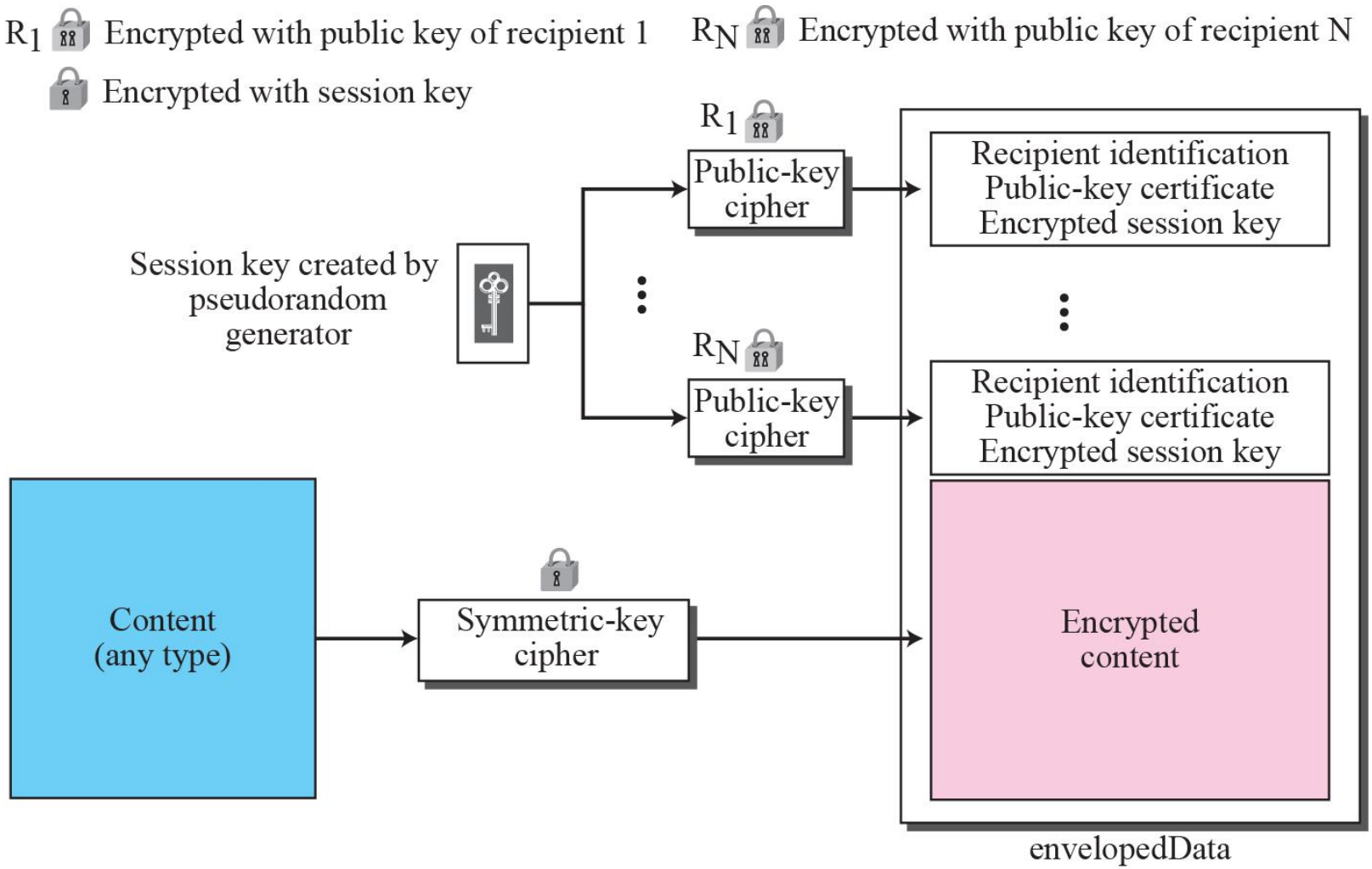


Figure 30.30 *Digest-data content type*

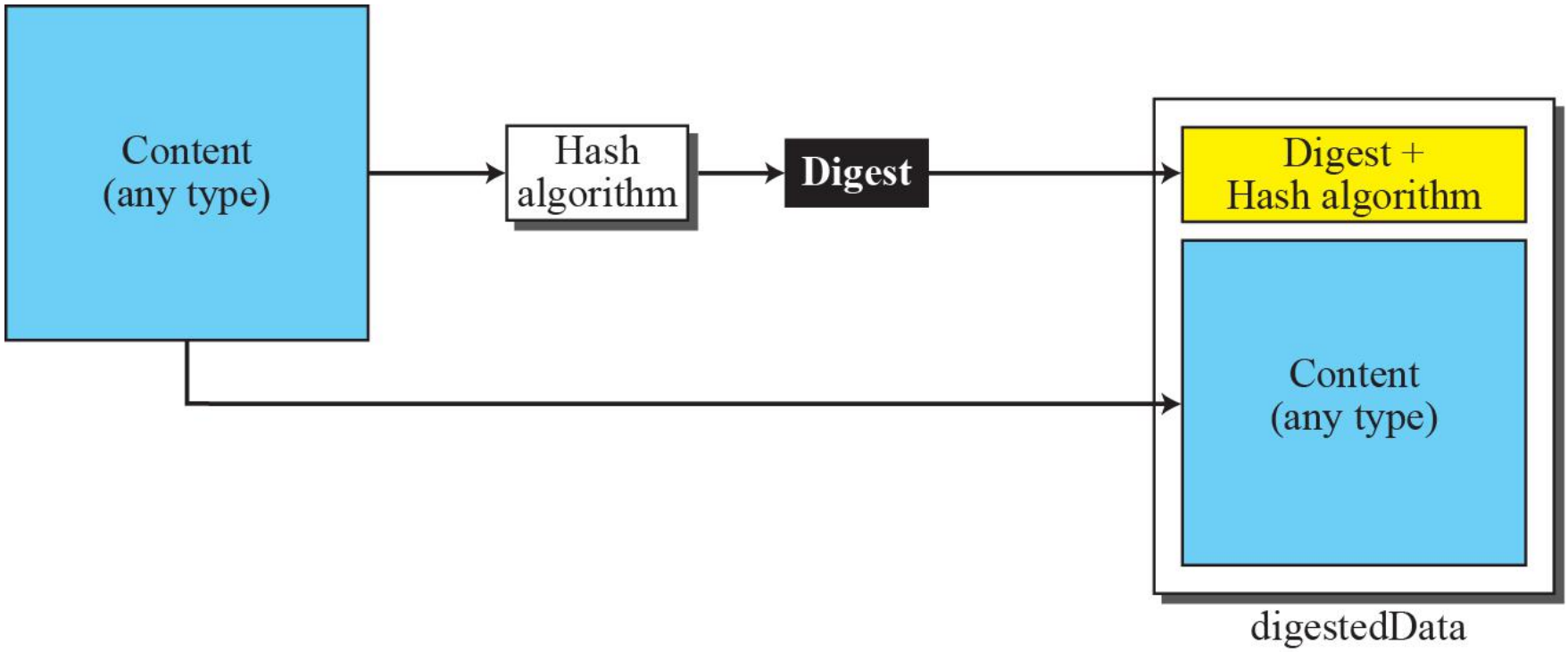


Figure 30.31 *Authenticated-data content type*