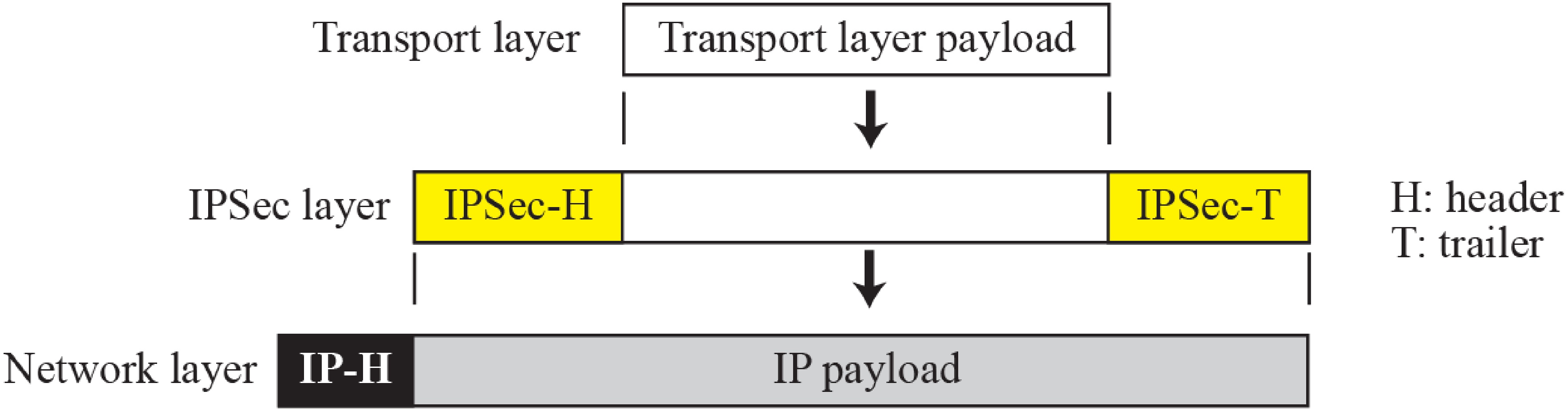
NETWORK LAYER SECURITY

IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level. IPSec helps create authenticated and confidential packets for the IP layer.

Topics Discussed in the Section

- ✓ **Two Modes**
- ✓ **Two Security Protocols**
- ✓ **Services Provided by IPSec**
- ✓ **Security Association**
- ✓ **Internet Key Exchange (IKE)**
- ✓ **Virtual Private Network (VPN)**

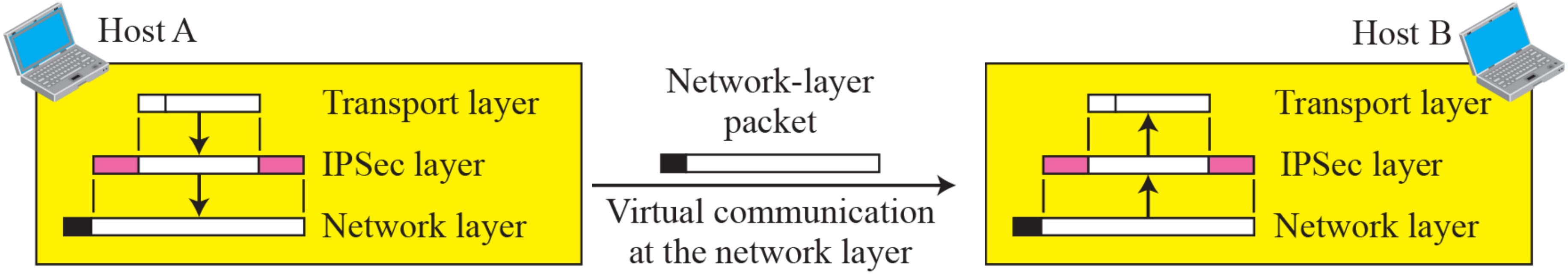
.1 *IPSec in transport mode*



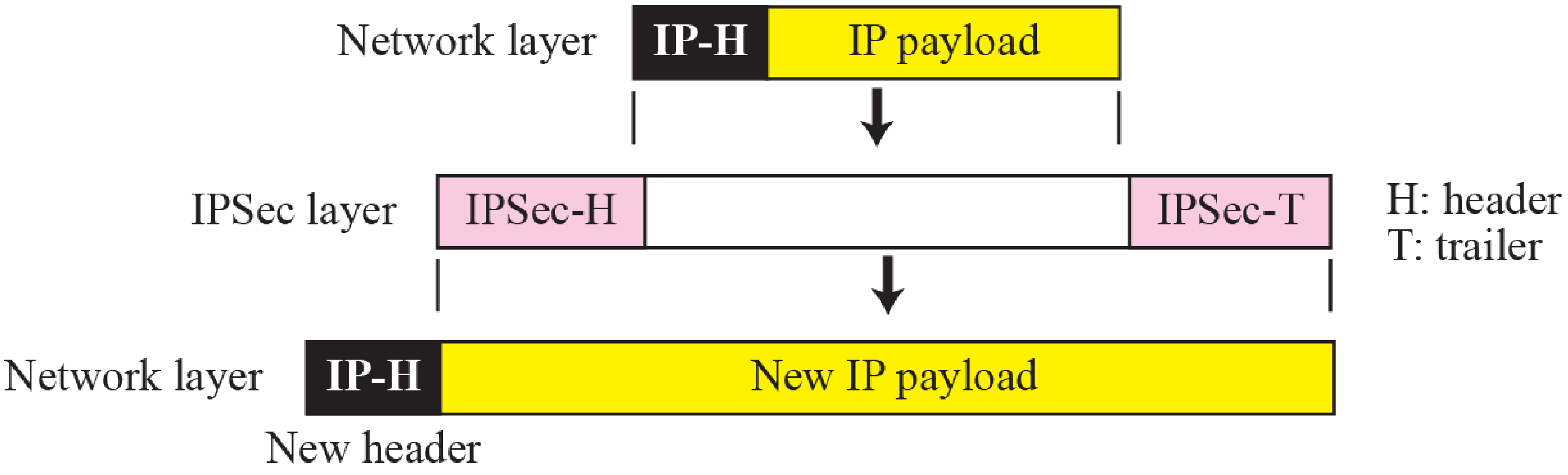
Note

***IPSec in transport mode does not protect the IP header;
it only protects the information coming from the transport layer.***

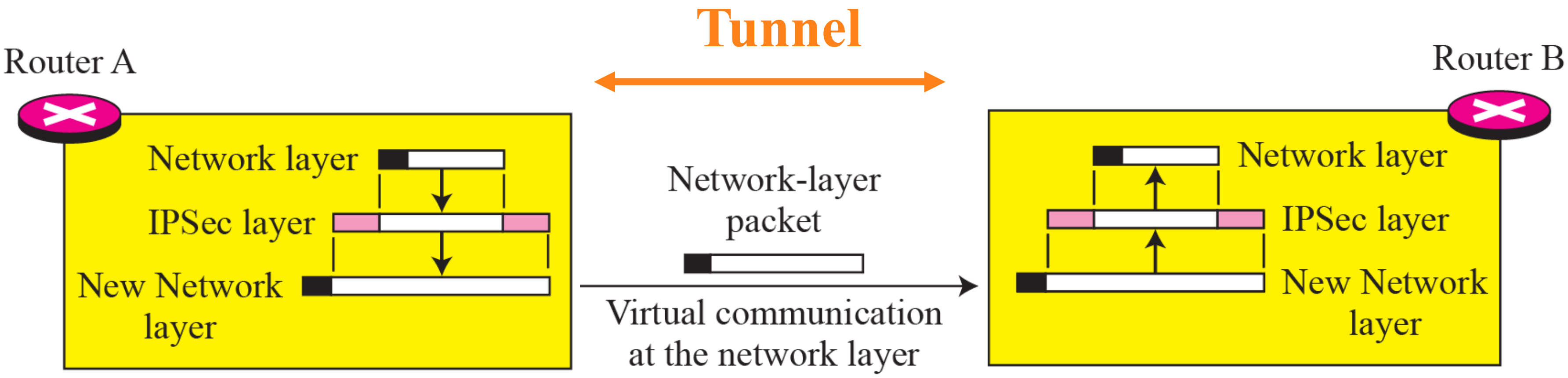
.2 *Transport mode in Action*



.3 *IPSec in tunnel mode*



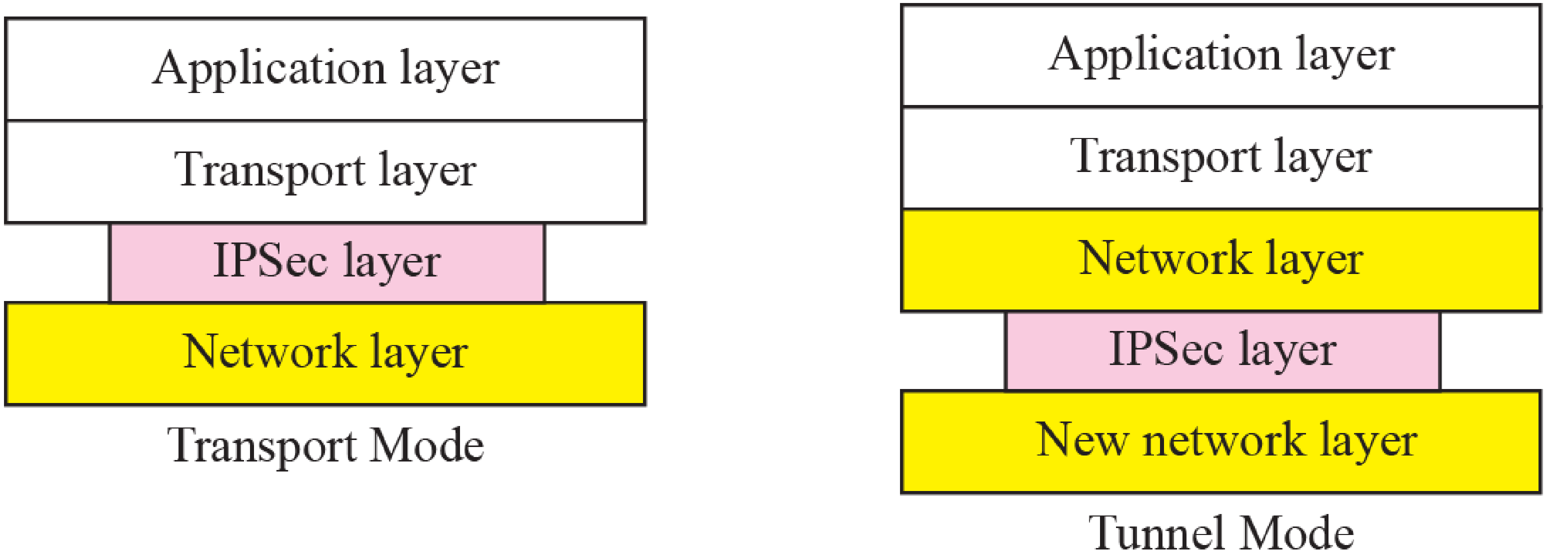
.4 *Tunnel-mode in action*



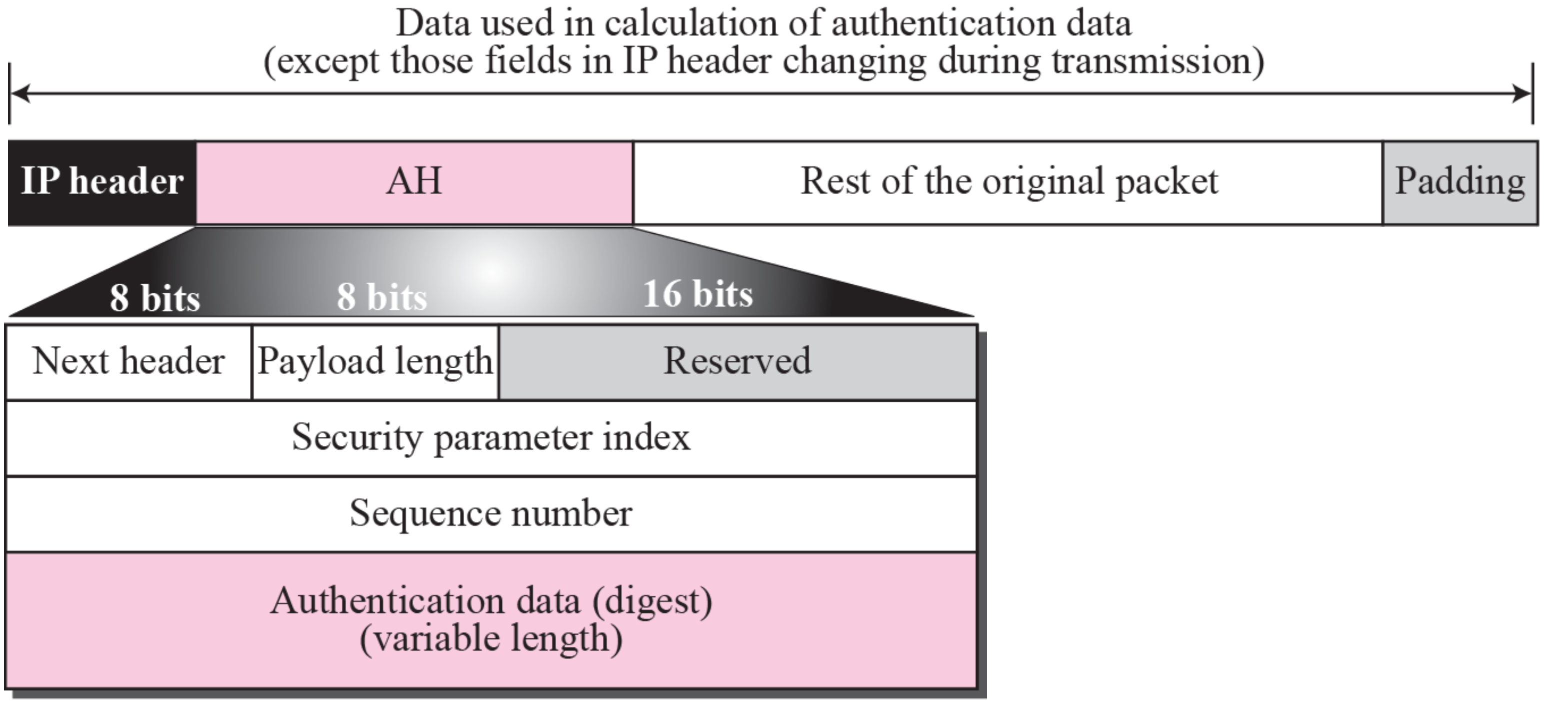
Note

IPSec in tunnel mode protects the original IP header.

.5 *Transport mode versus tunnel mode*



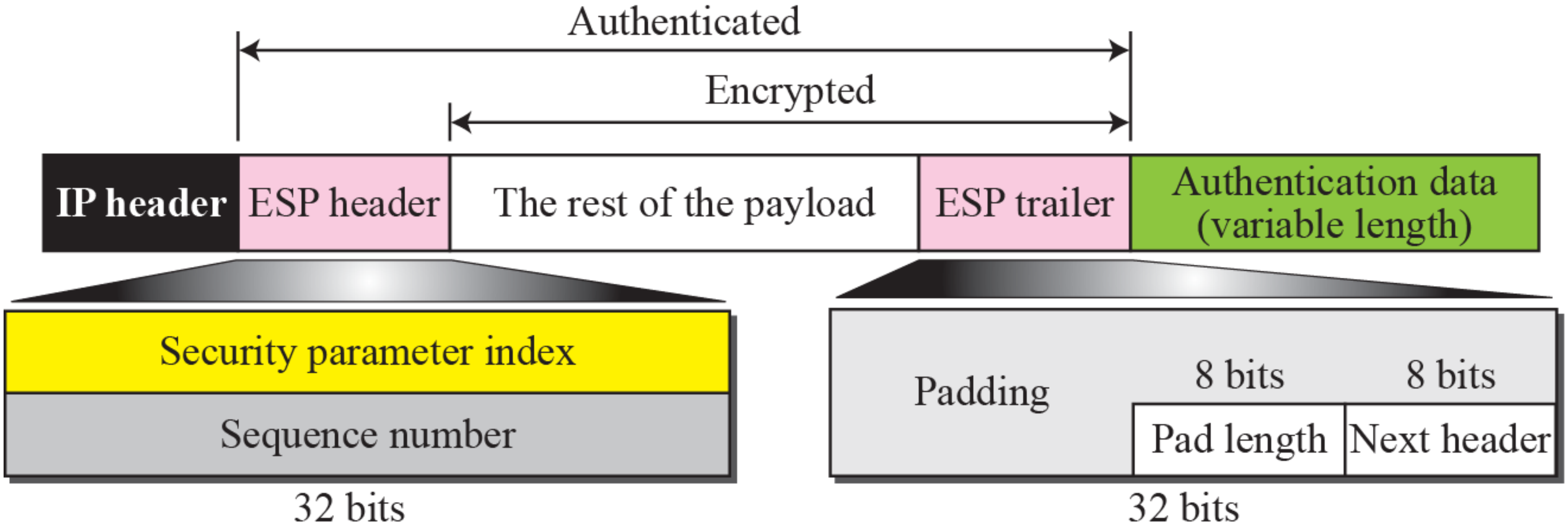
.6 *Authentication Header (AH) protocol*


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

Note

The AH protocol provides source authentication and data integrity, but not privacy.

.7 *Encapsulating Security Payload (ESP)*



Note

ESP provides source authentication, data integrity, and privacy.

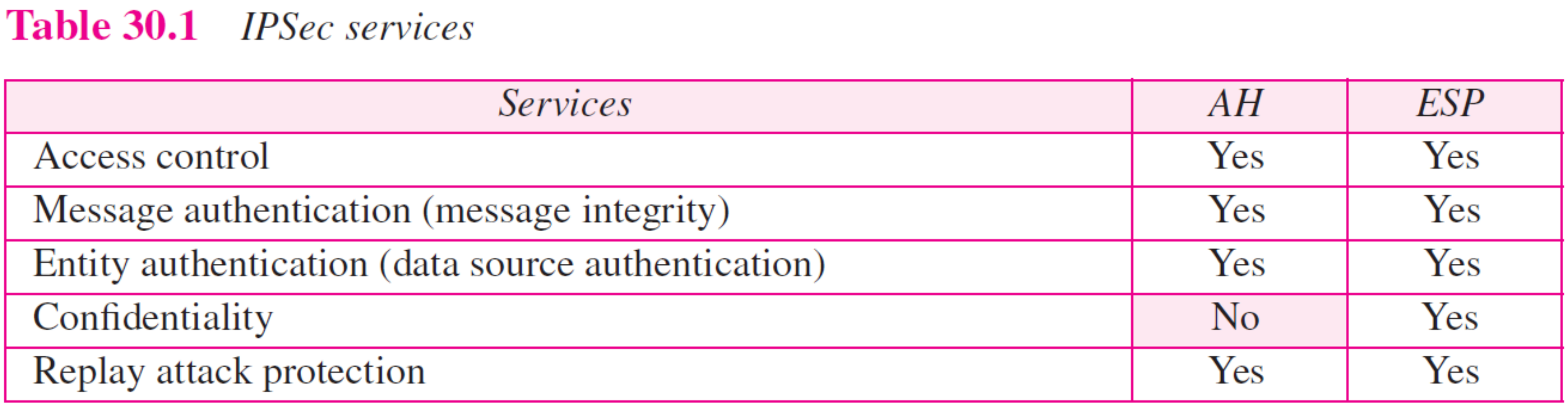
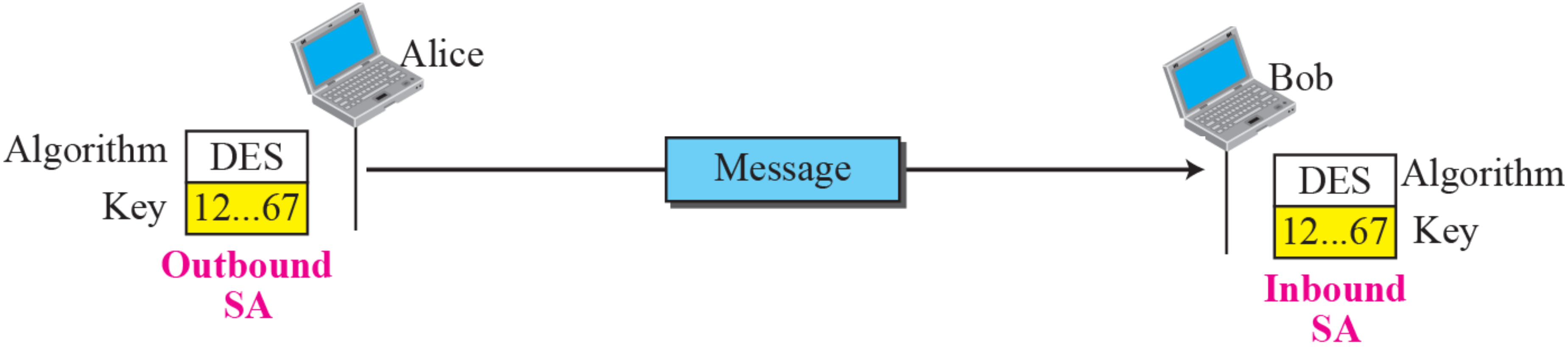


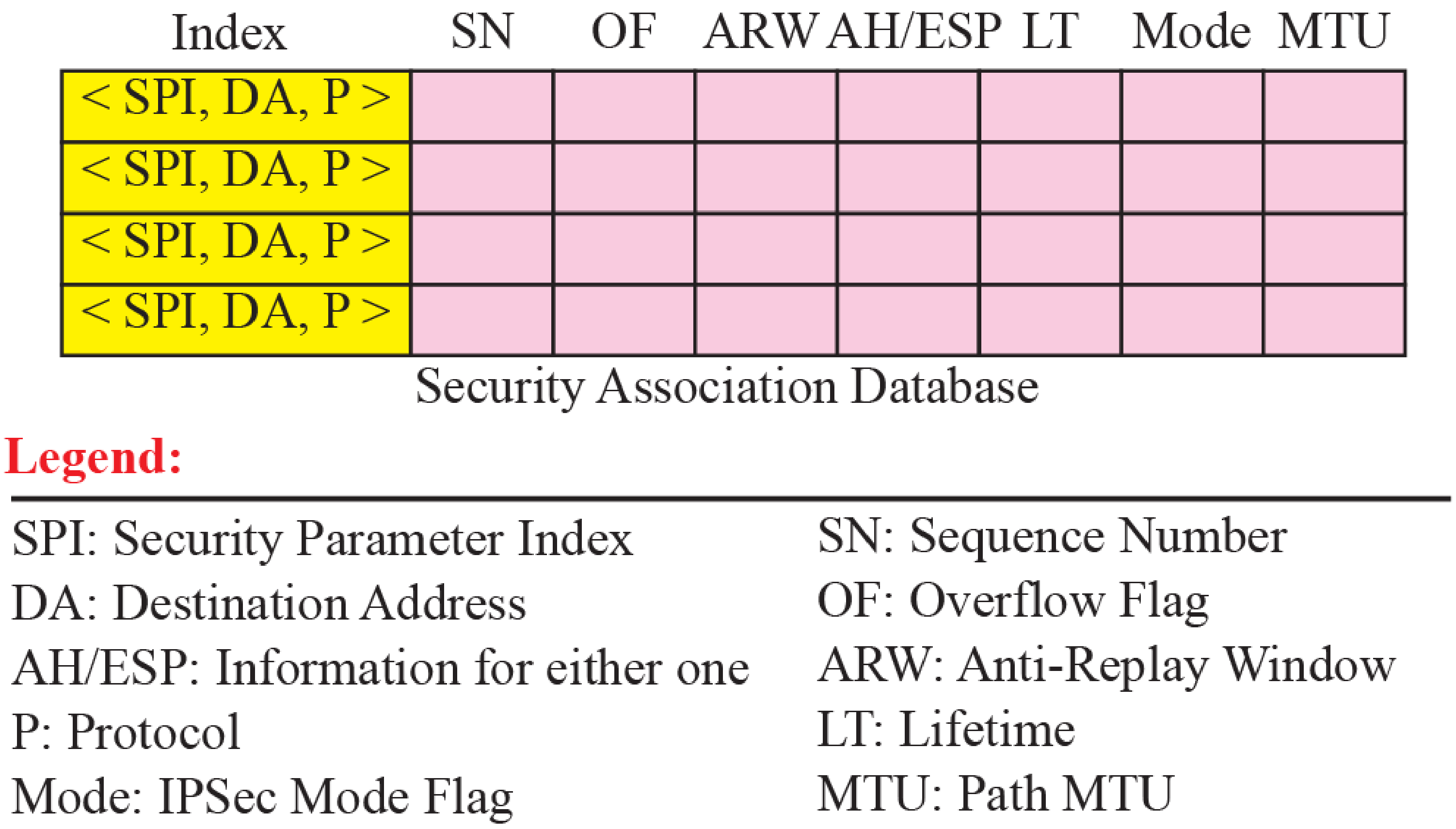
Table 30.1 *IPSec services*

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

.8 Simple SA


Alice
Algorithm
DES
Key
12...67
Outbound SA
Message
Bob
DES
Algorithm
12...67
Key
Inbound SA

.9 SAD



Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							

Security Association Database

Legend:

SPI: Security Parameter Index
DA: Destination Address
AH/ESP: Information for either one
P: Protocol
Mode: IPSec Mode Flag

SN: Sequence Number
OF: Overflow Flag
ARW: Anti-Replay Window
LT: Lifetime
MTU: Path MTU

.10 *SPD*

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Legend:

SA: Source Address

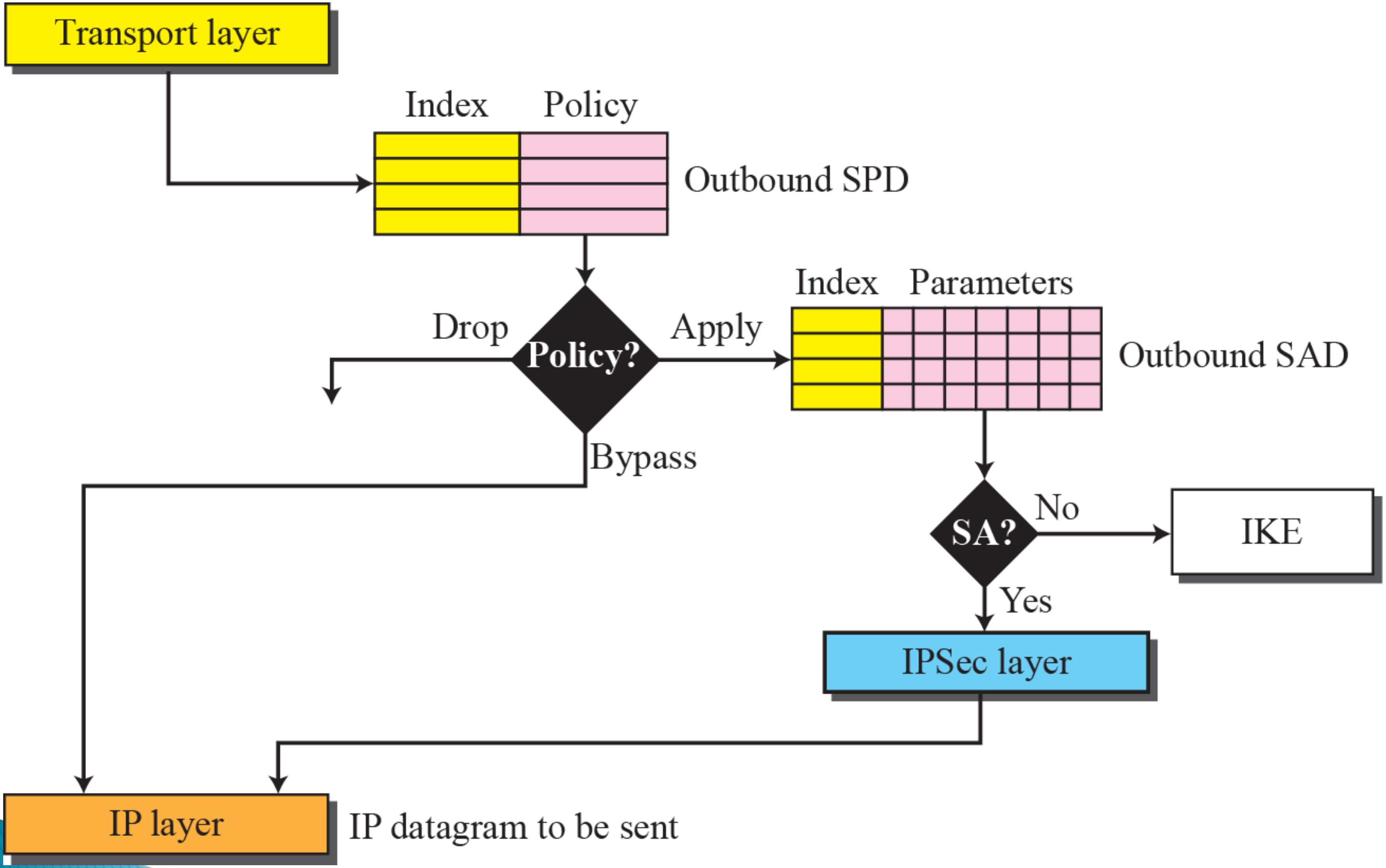
DA: Destination Address

P: Protocol

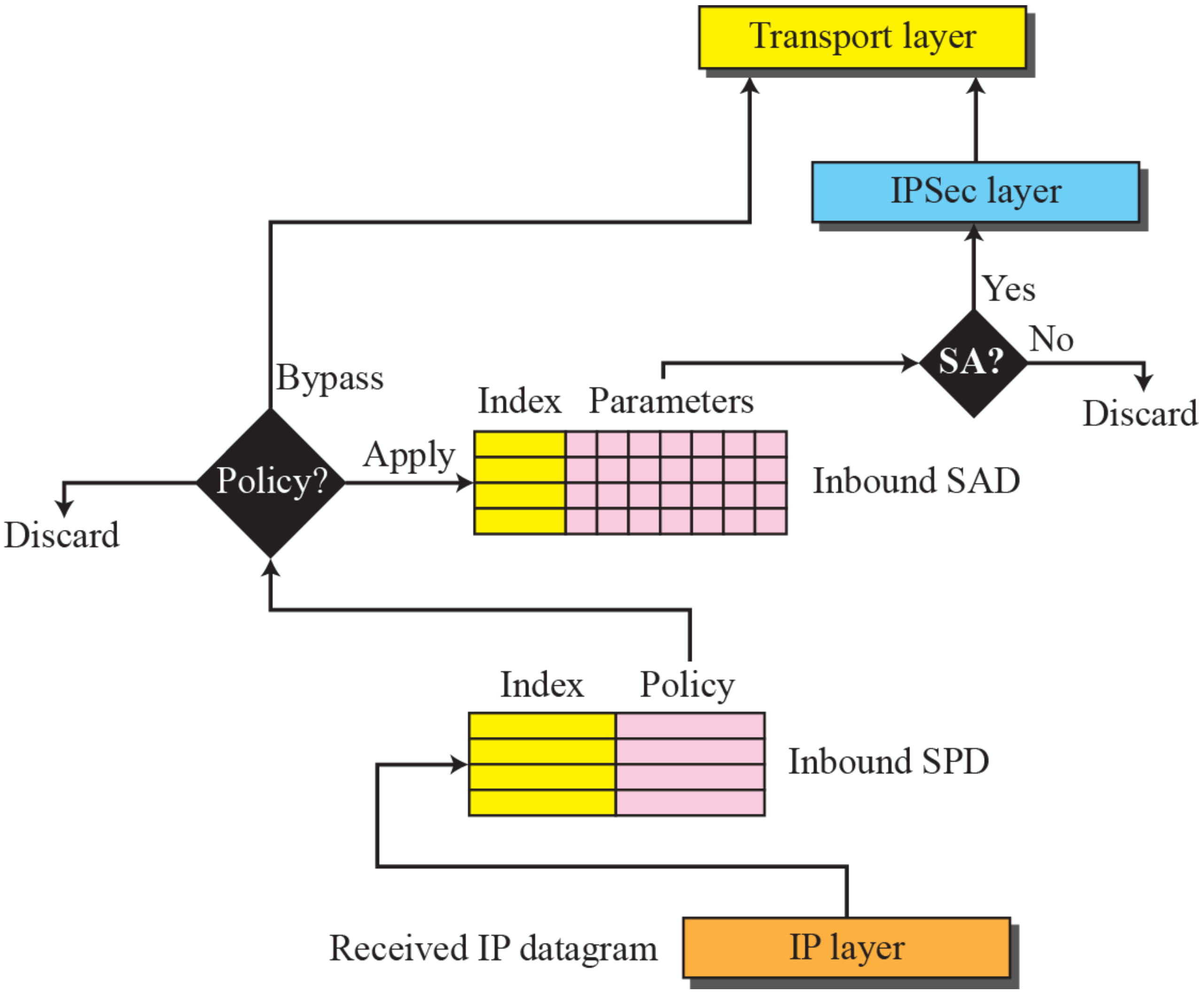
SPort: Source Port

DPort: Destination Port

.11 *Outbound processing*



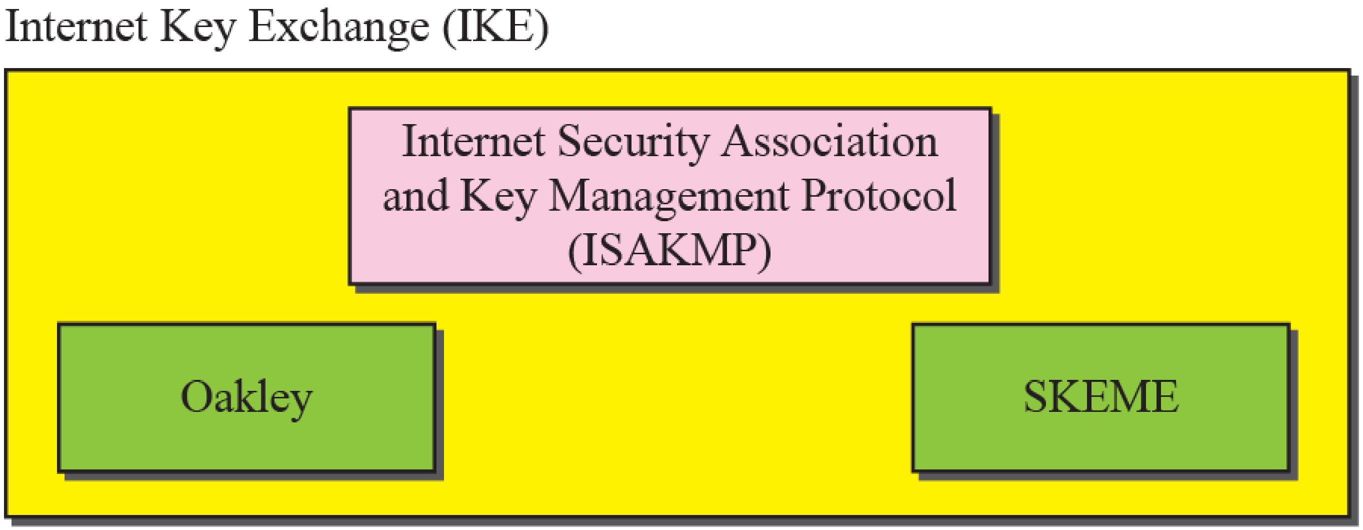
.12 *Inbound processing*



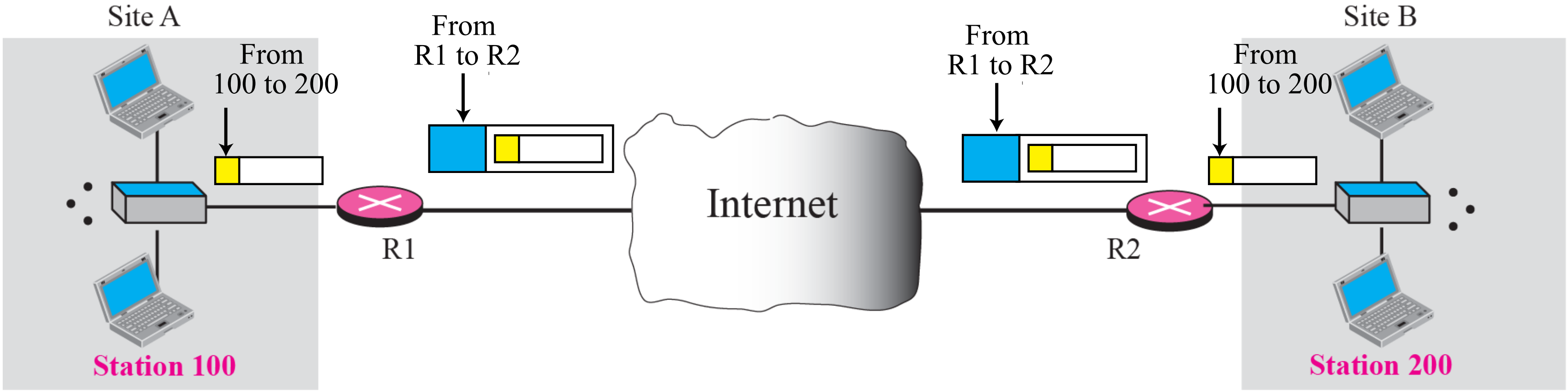
Note

IKE creates SAs for IPSec.

.13 *IKE components*


Internet Key Exchange (IKE)
Internet Security Association and Key Management Protocol (ISAKMP)
Oakley
SKEME

.14 *Virtual private network*



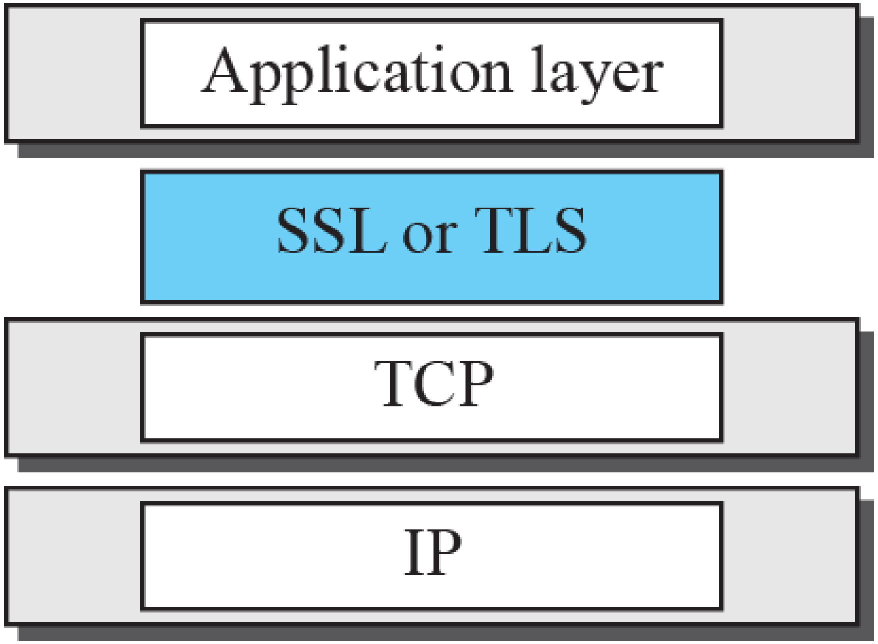
30-2 TRANSPORT LAYER SECURITY

Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) protocol and the Transport Layer Security (TLS) protocol. The latter is actually an IETF version of the former. We discuss SSL in this section; TLS is very similar. .15 shows the position of SSL and TLS in the Internet model.

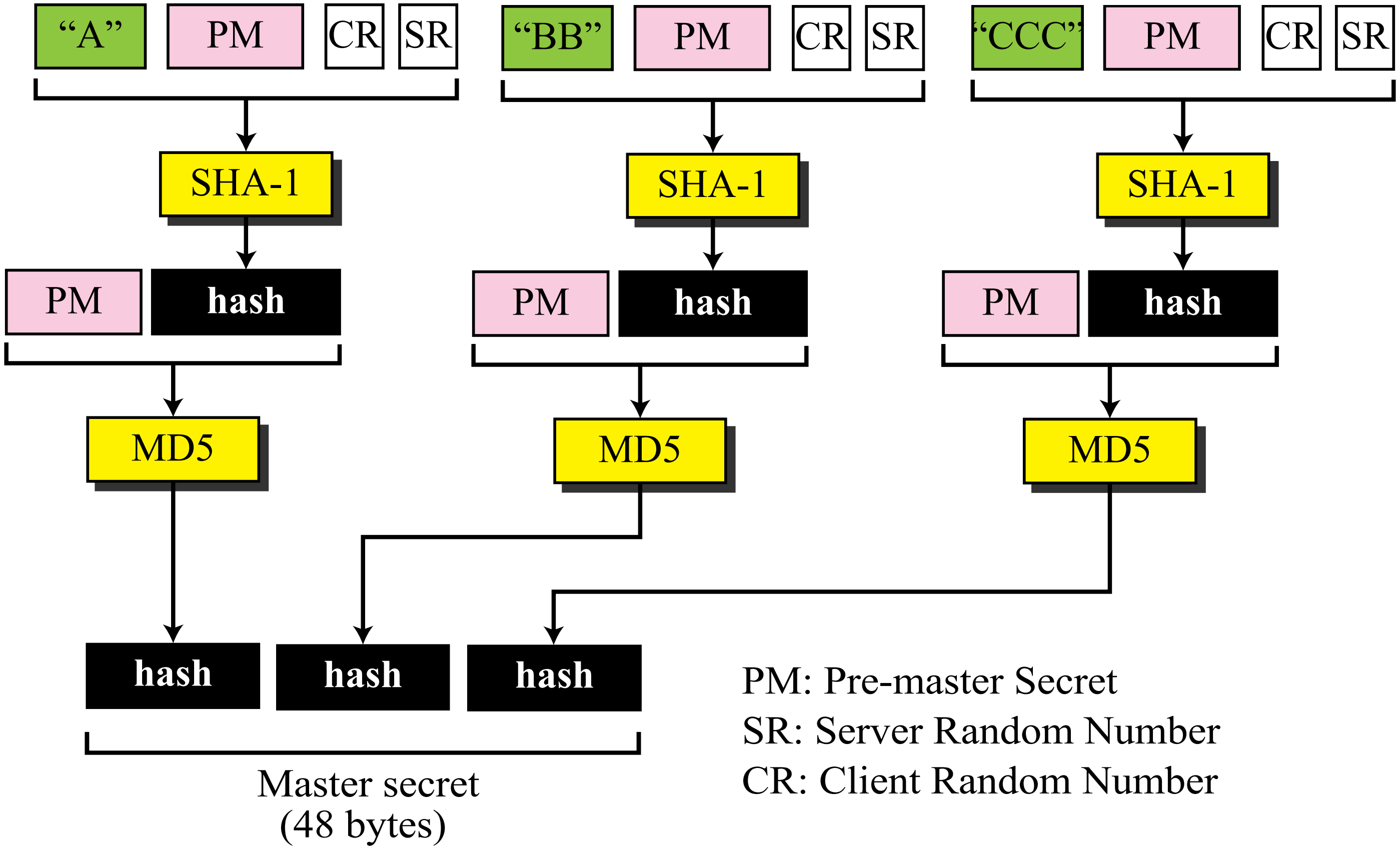
Topics Discussed in the Section

- ✓ SSL Architecture
- ✓ Four Protocols

.15 *Location of SSL and TSL in the Internet mode*

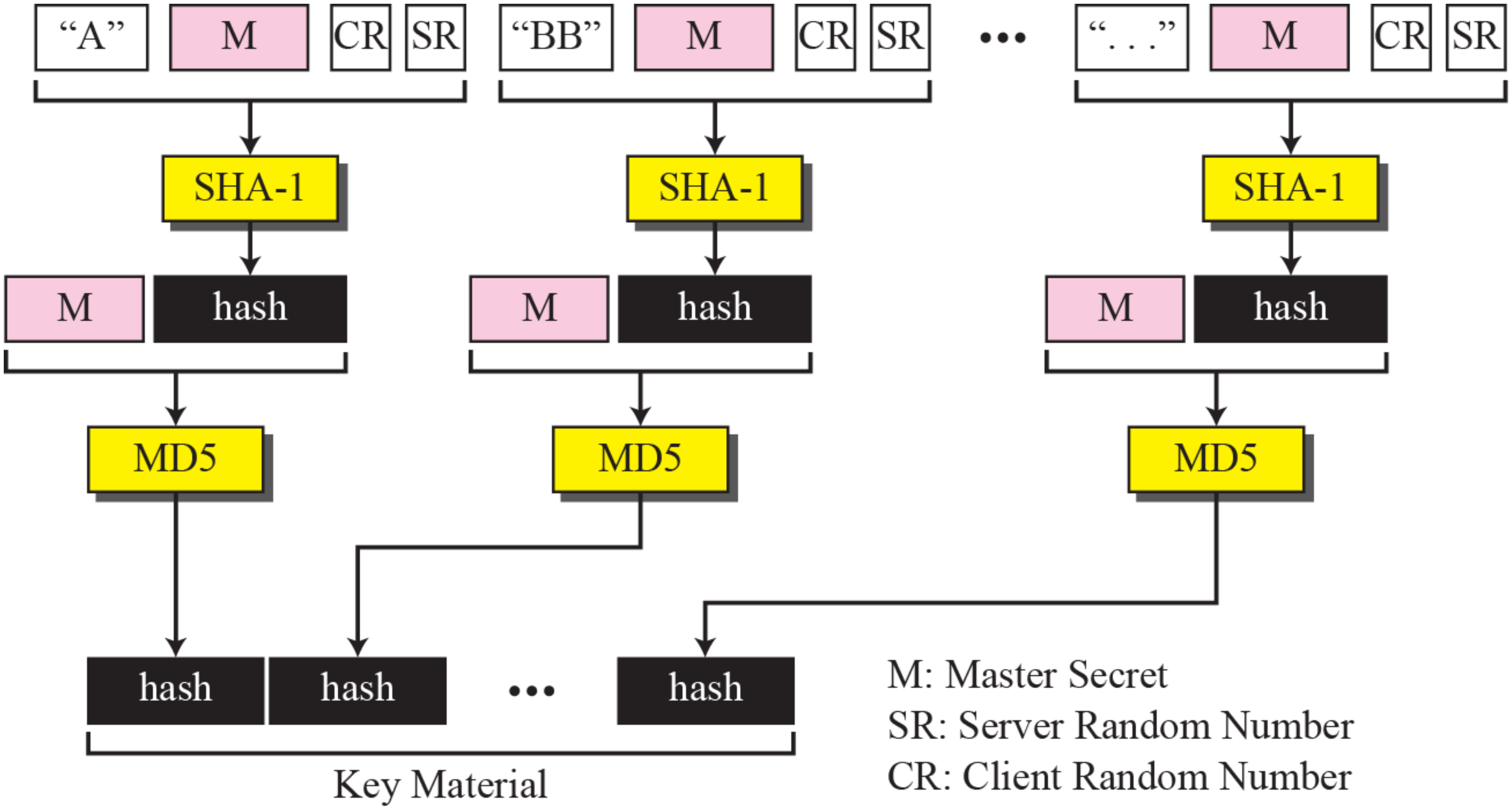


.16 *Calculation of maser key from pre-master secret*



PM: Pre-master Secret
SR: Server Random Number
CR: Client Random Number

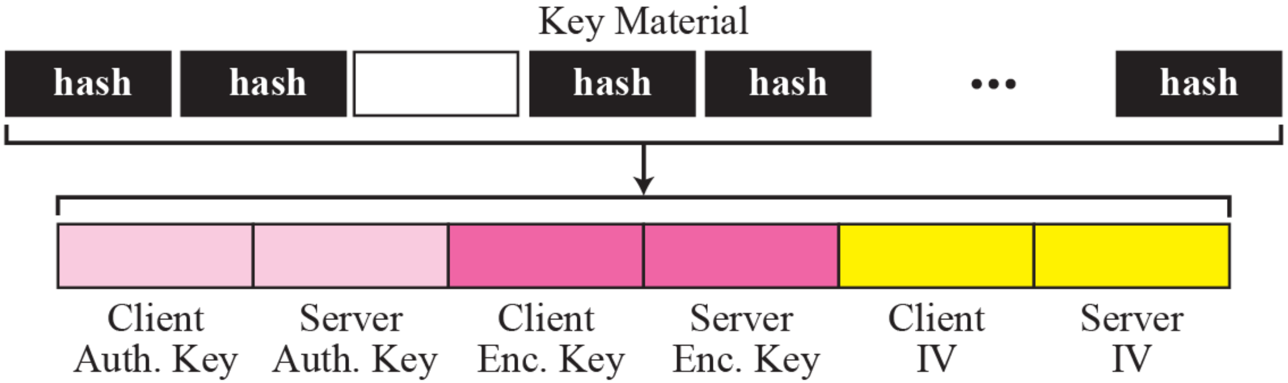
.17 *Calculation of the key materials from master secret*



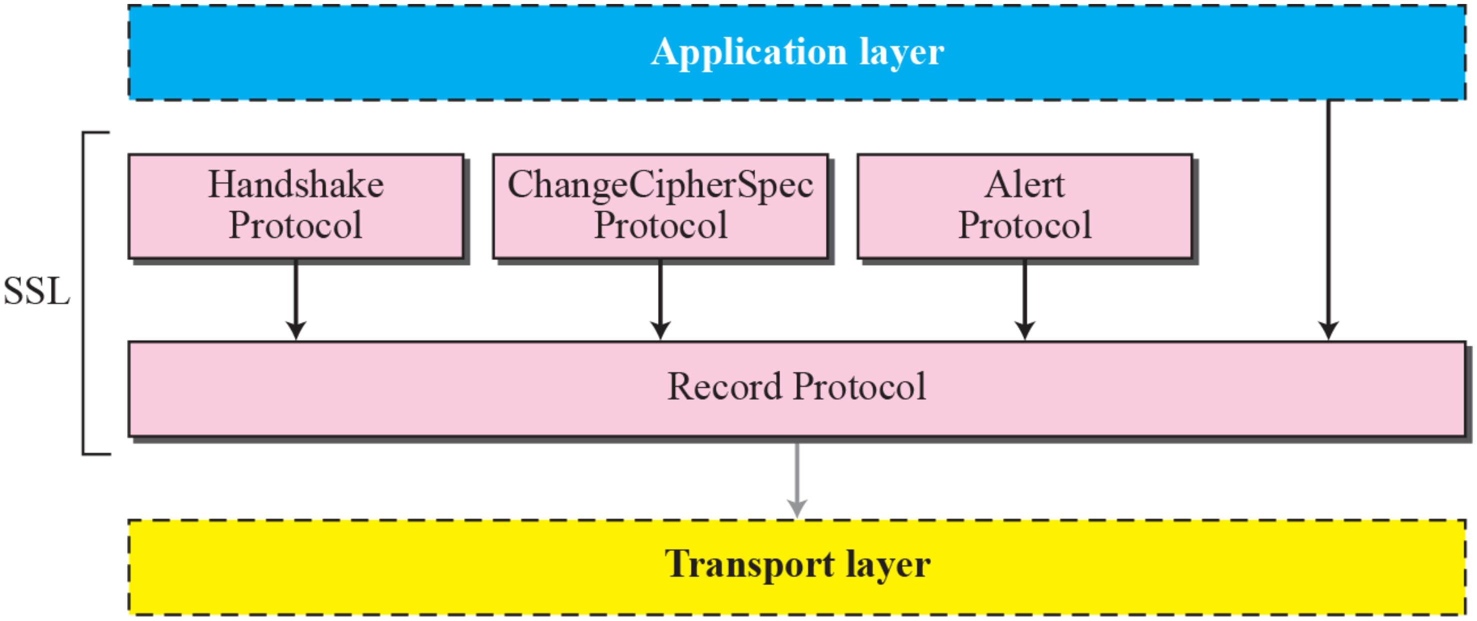
M: Master Secret
SR: Server Random Number
CR: Client Random Number

.18 *Extraction of cryptographic secrets from key materials*

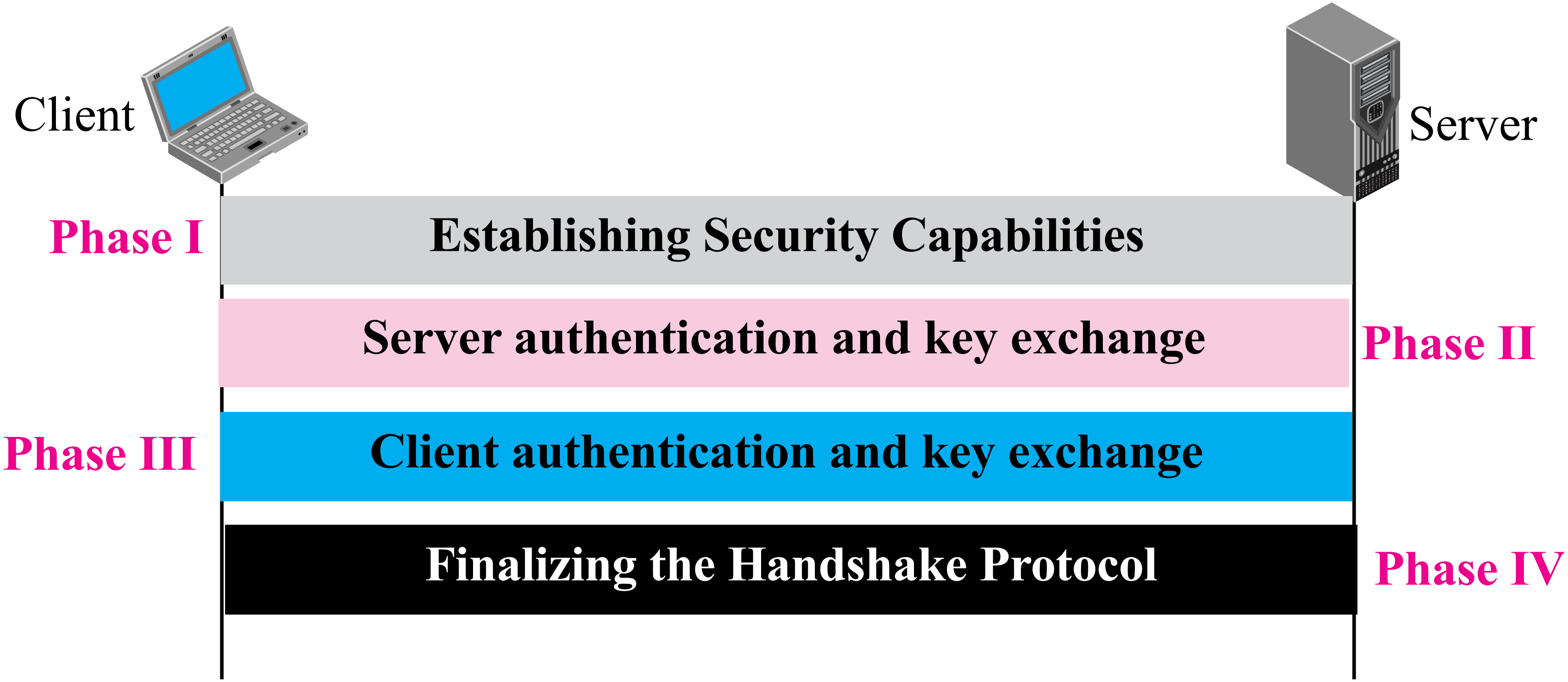
Auth. Key: Authentication Key
Enc. Key: Encryption Key
IV: Initialization Vector



.19 *Four SSL protocols*



.20 *Handshake protocol*



Client

Server

Phase I

Establishing Security Capabilities

Server authentication and key exchange

Phase II

Phase III

Client authentication and key exchange

Finalizing the Handshake Protocol

Phase IV

Note

After Phase I, the client and server know the version of SSL, the cryptographic algorithms, the compression method, and the two random numbers for key generation.

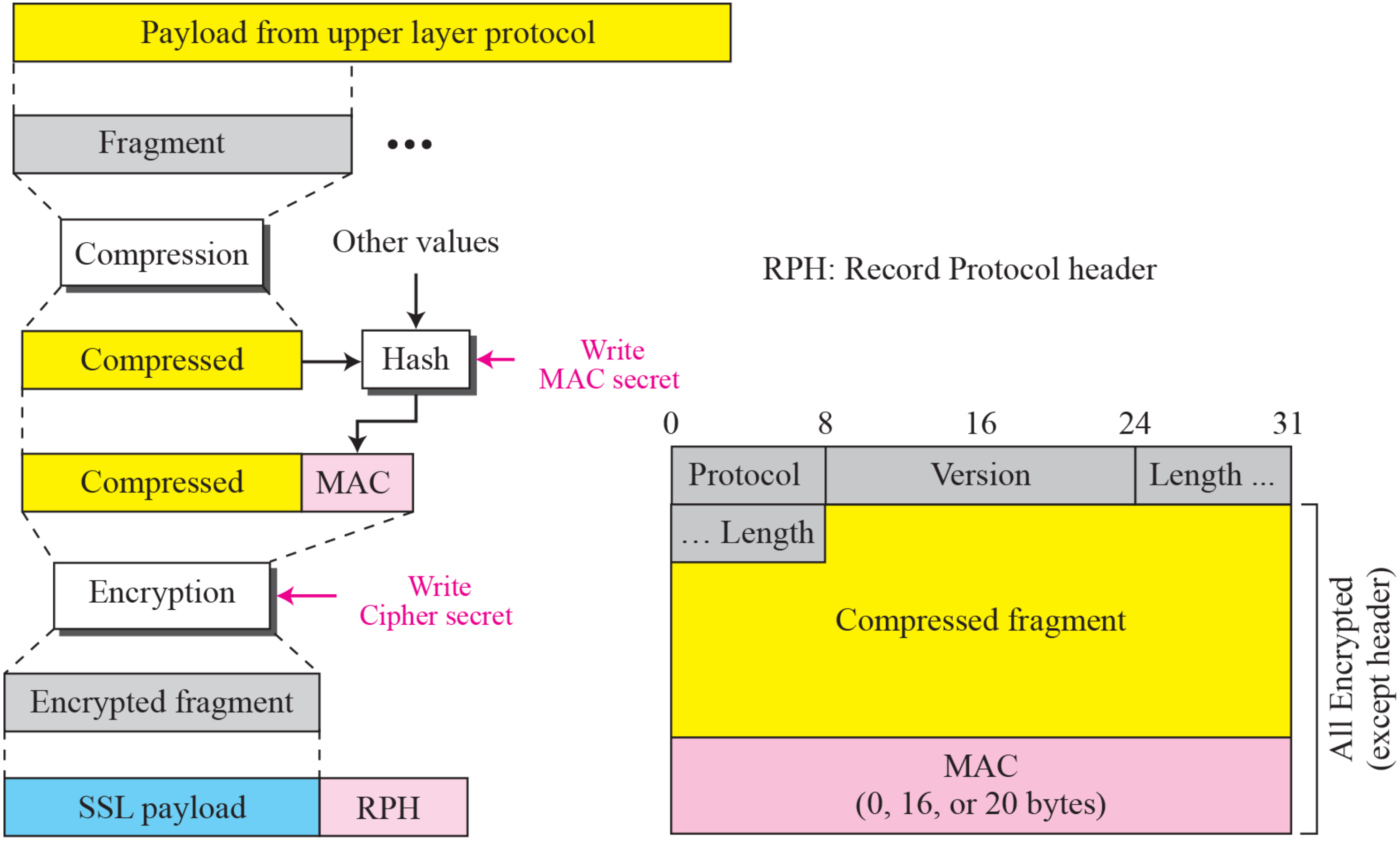
Note

After Phase II, the server is authenticated to the client, and the client knows the public key of the server if required.

Note

After Phase III, The client is authenticated for the serve, and both the client and the server know the pre-master secret.

.21 *Processing done by the record protocol*



a. Process

b. Encapsulation

30-3 APPLICATION LAYER SECURITY

This section discusses two protocols providing security services for e-mails: Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME).

Topics Discussed in the Section

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

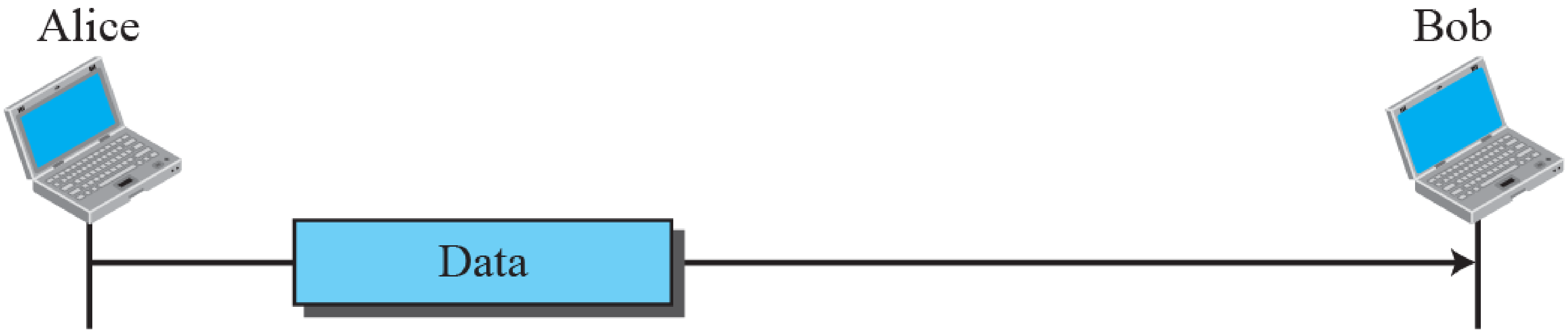
Note

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

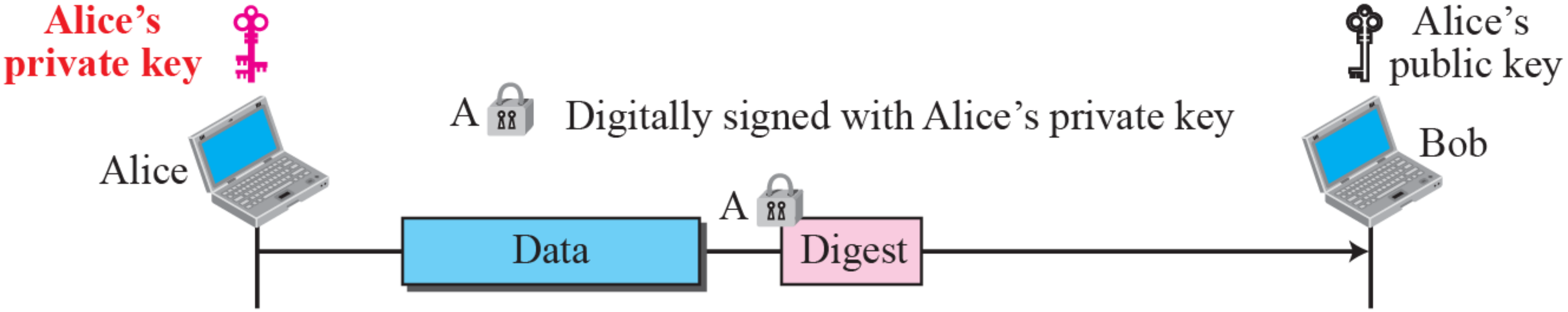
Note

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.

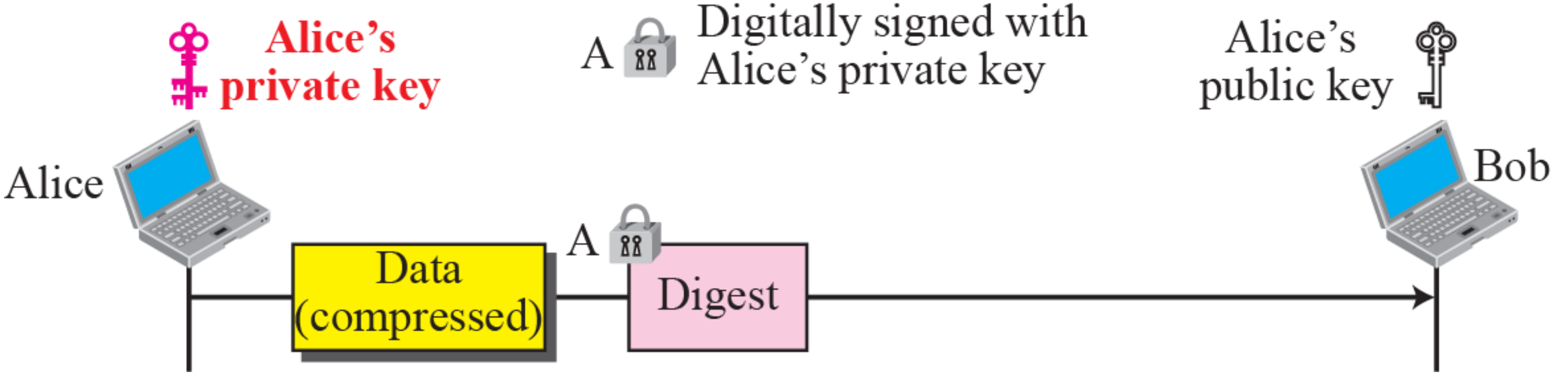
.22 *A plaintext message*



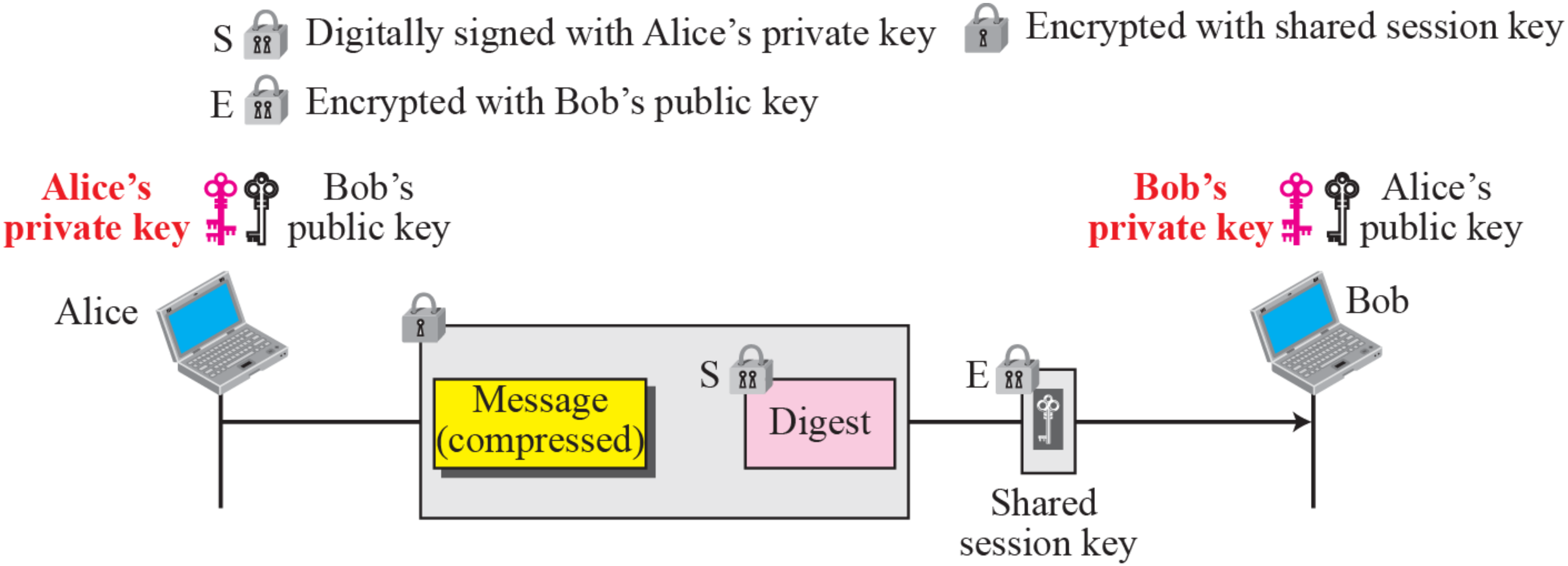
.23 *An authenticated message*



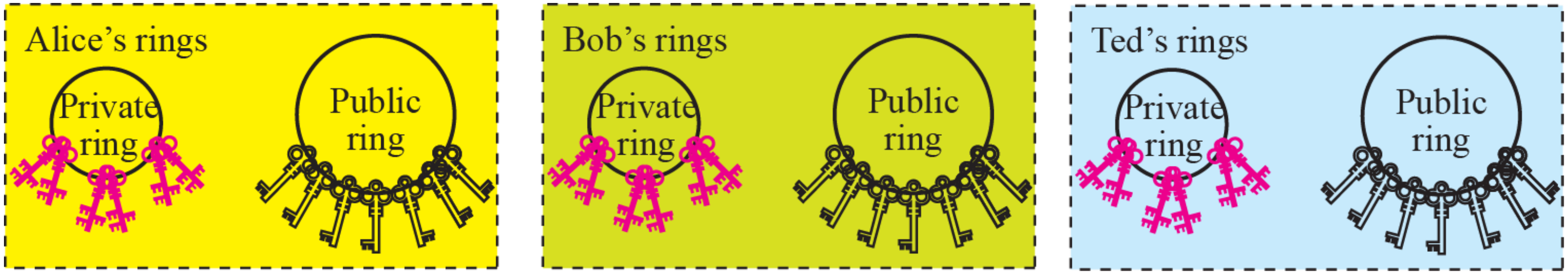
.24 A compressed message



.25 *A confidential message*



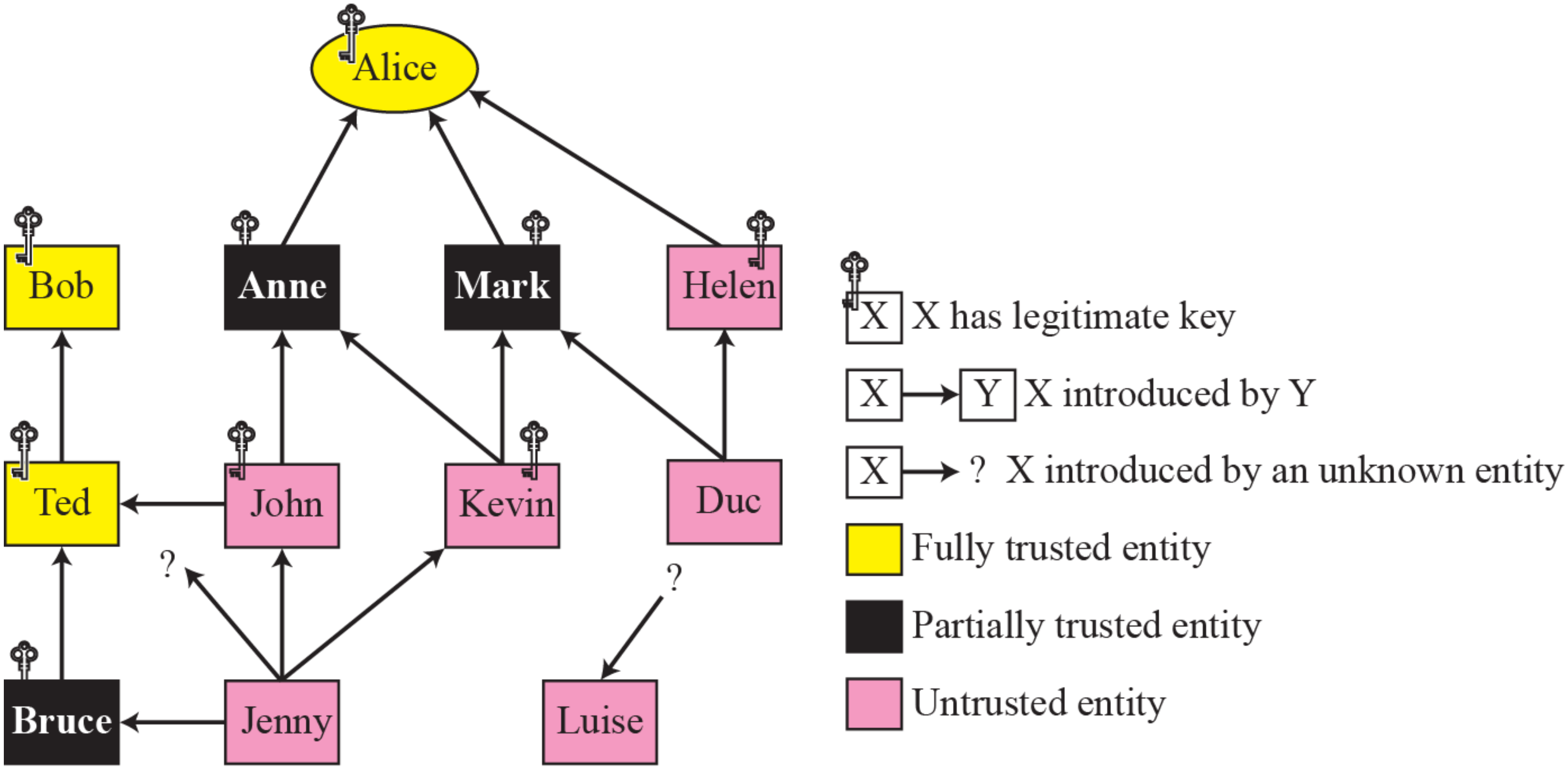
.26 *Key rings in PGP*



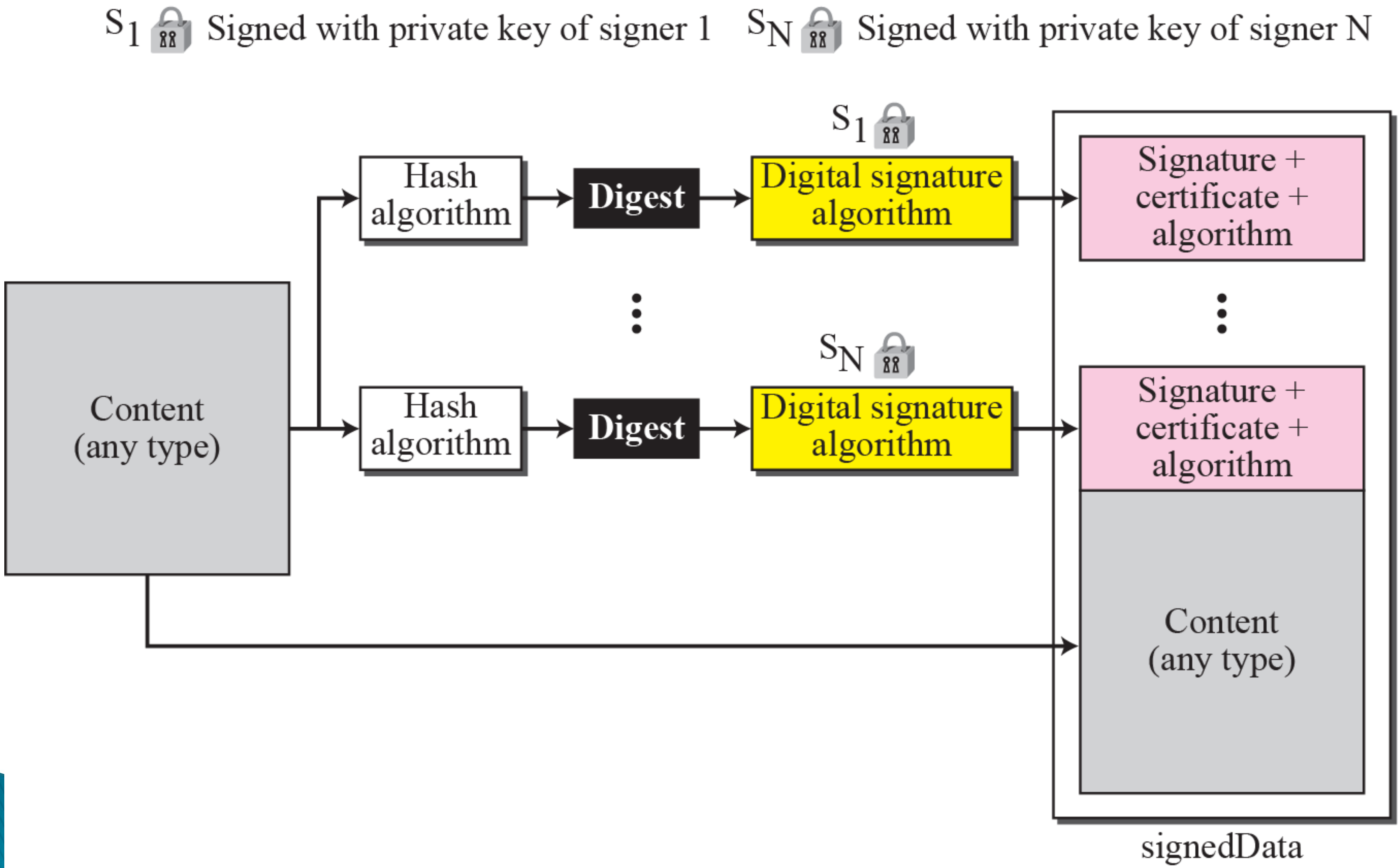
Note

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

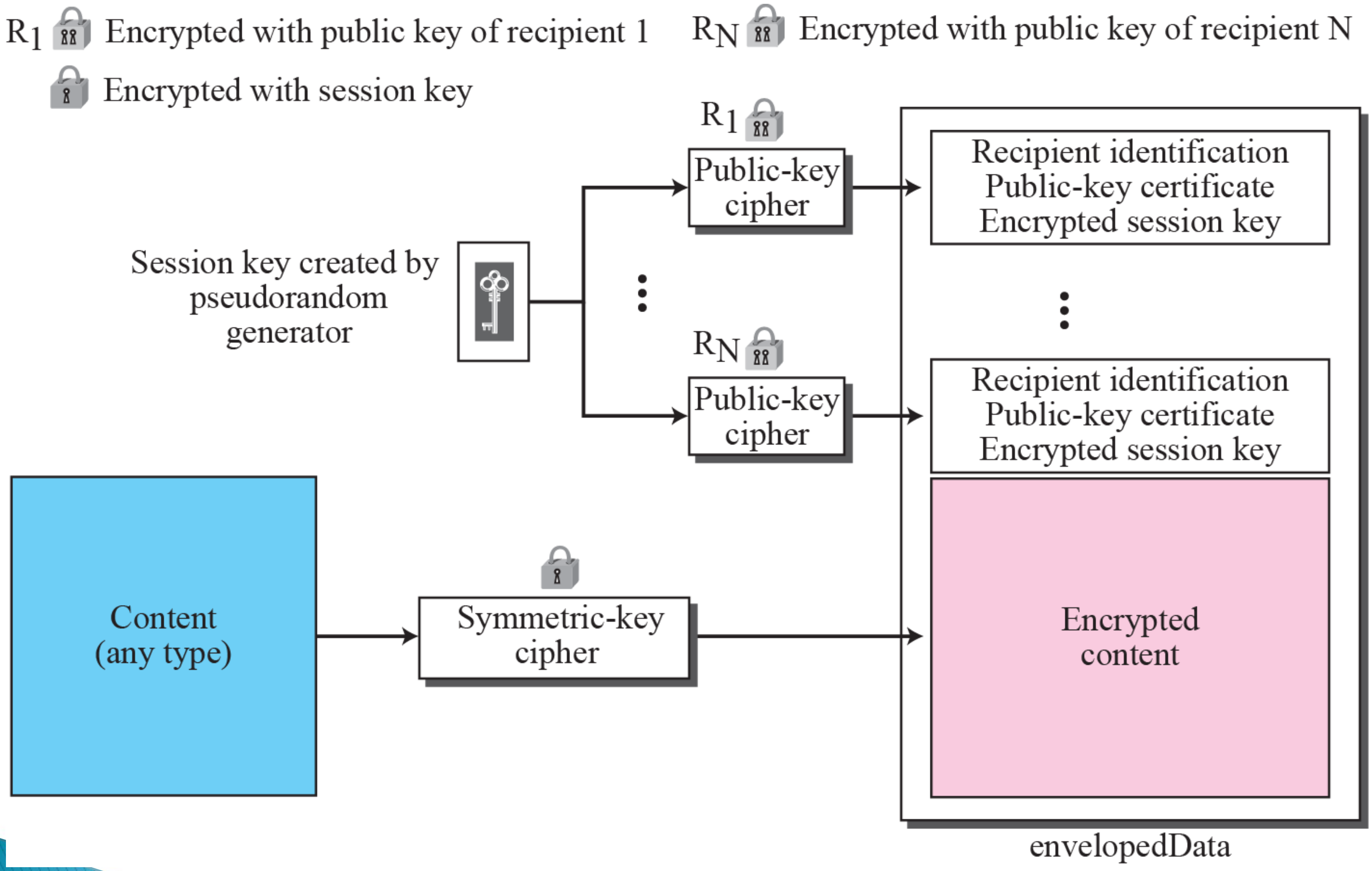
.27 Trust model



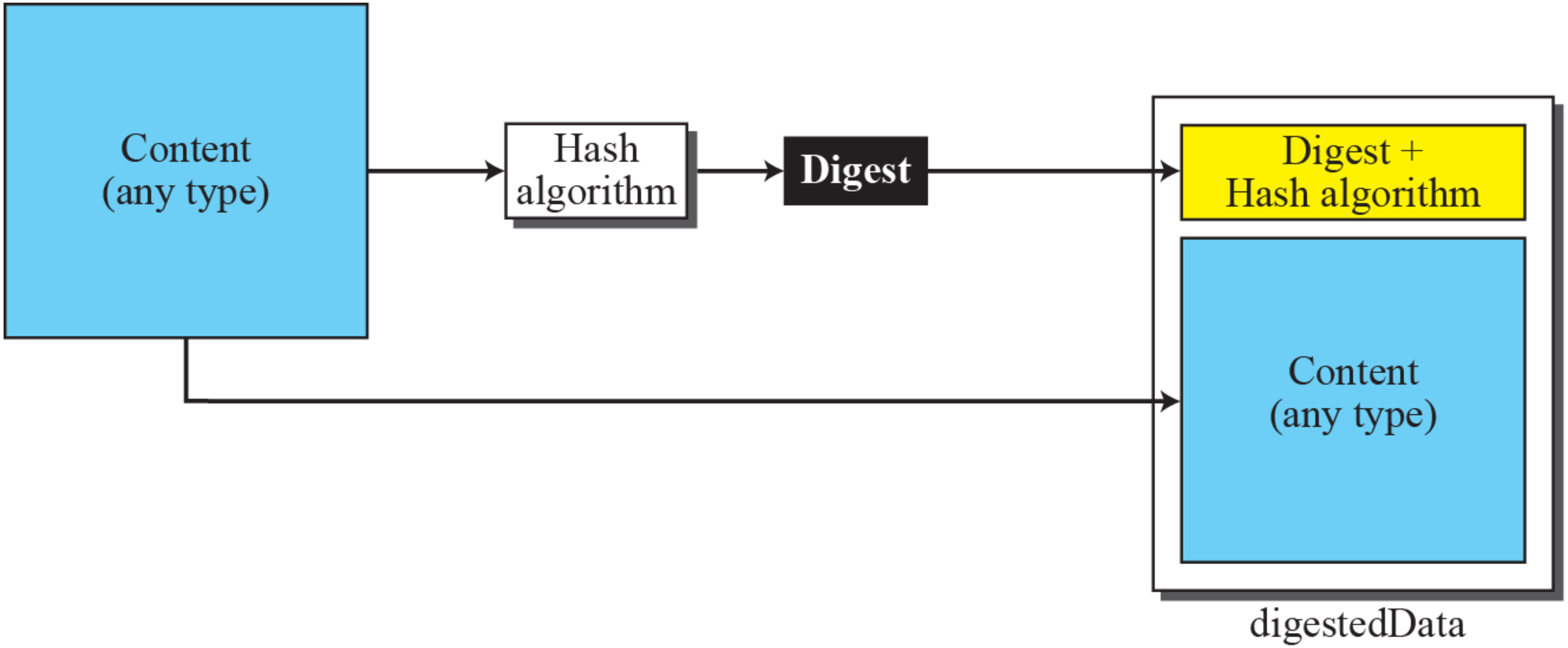
.28 *Signed-data content type*


S1 Signed with private key of signer 1
SN Signed with private key of signer N
Content (any type)
Hash algorithm
Digest
S1
Digital signature algorithm
Hash algorithm
Digest
SN
Digital signature algorithm
Signature + certificate + algorithm
Signature + certificate + algorithm
Content (any type)
signedData

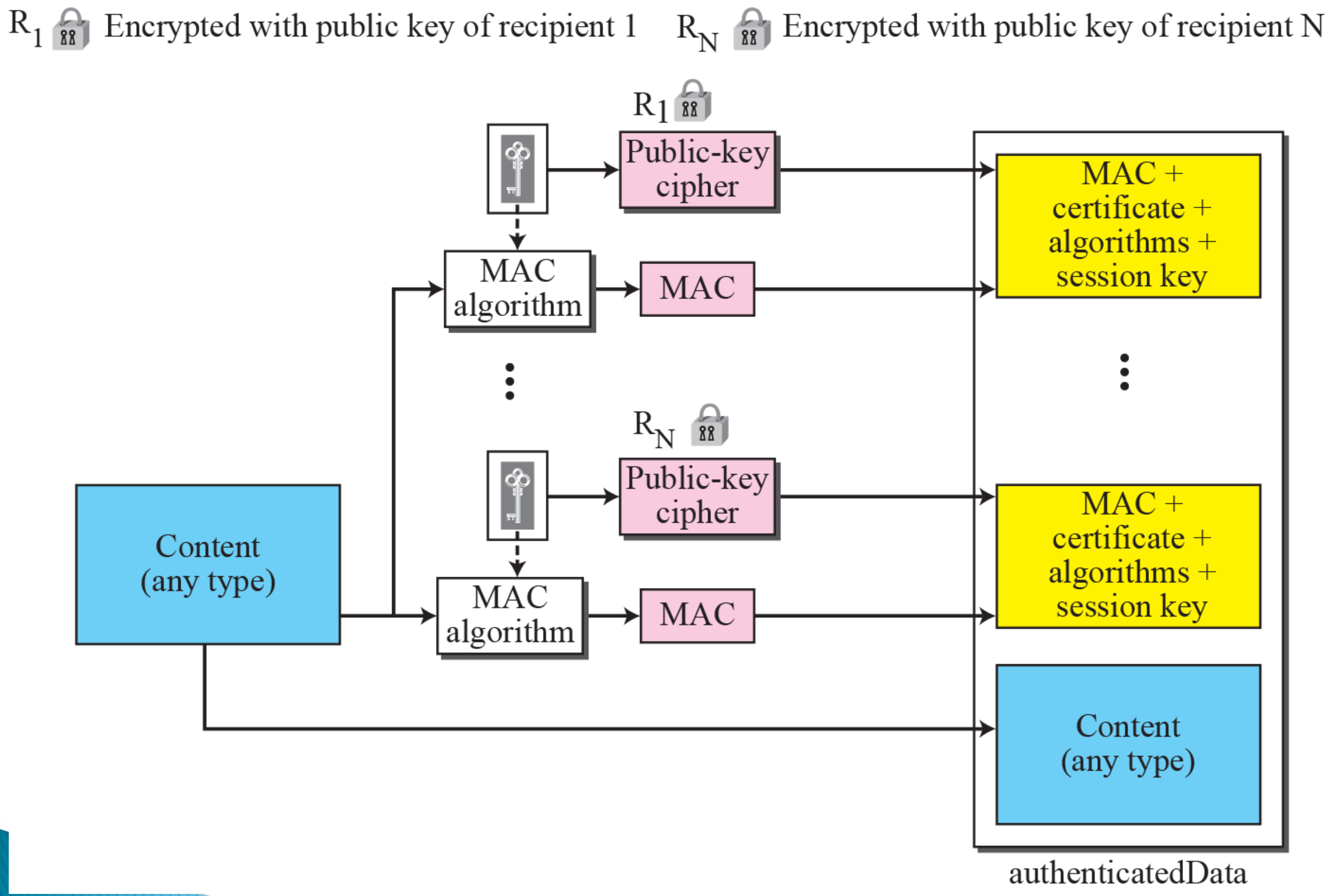
.29 Encrypted-data content type



.30 *Digest-data content type*

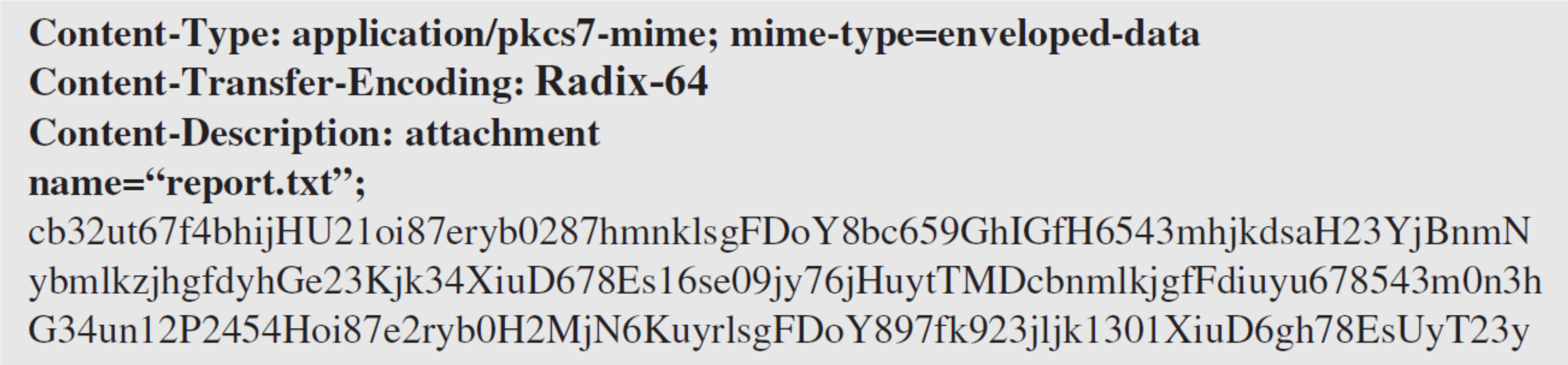


.31 *Authenticated-data content type*


R1 Encrypted with public key of recipient 1
RN Encrypted with public key of recipient N
R1
Public-key cipher
MAC algorithm
MAC
RN
Public-key cipher
MAC algorithm
MAC
Content (any type)
MAC + certificate + algorithms + session key
MAC + certificate + algorithms + session key
Content (any type)
authenticatedData

Example 30.1

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
```

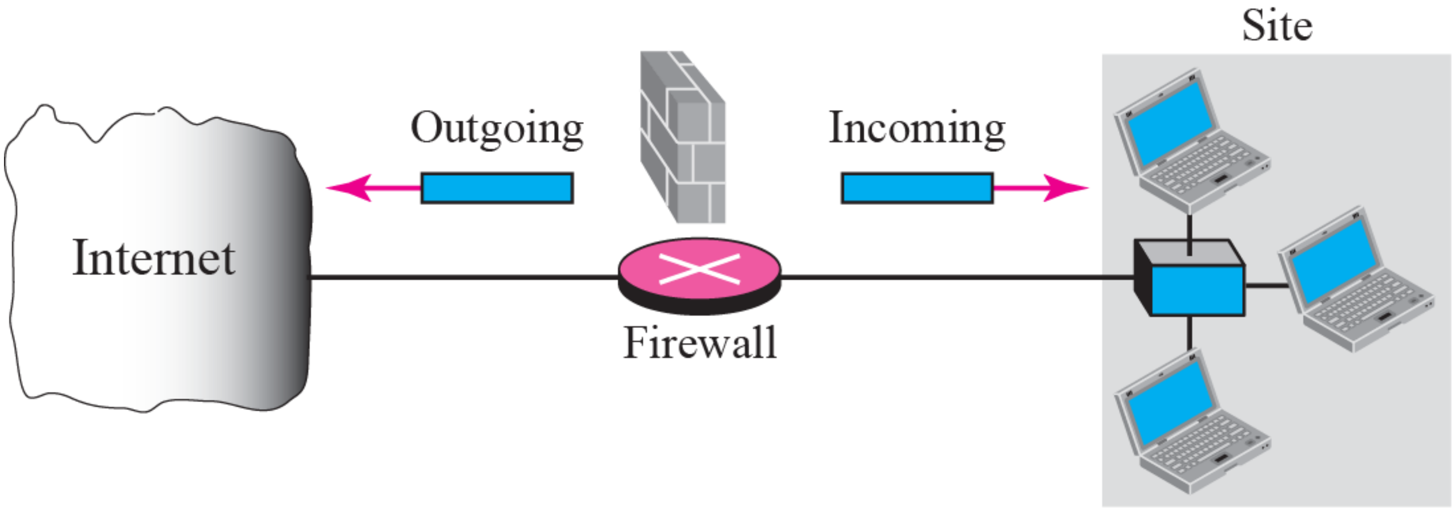
30-4 FIREWALLS

All previous security measures cannot prevent Eve from sending a harmful message to a system. To control access to a system we need firewalls. A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others. .32 shows a firewall.

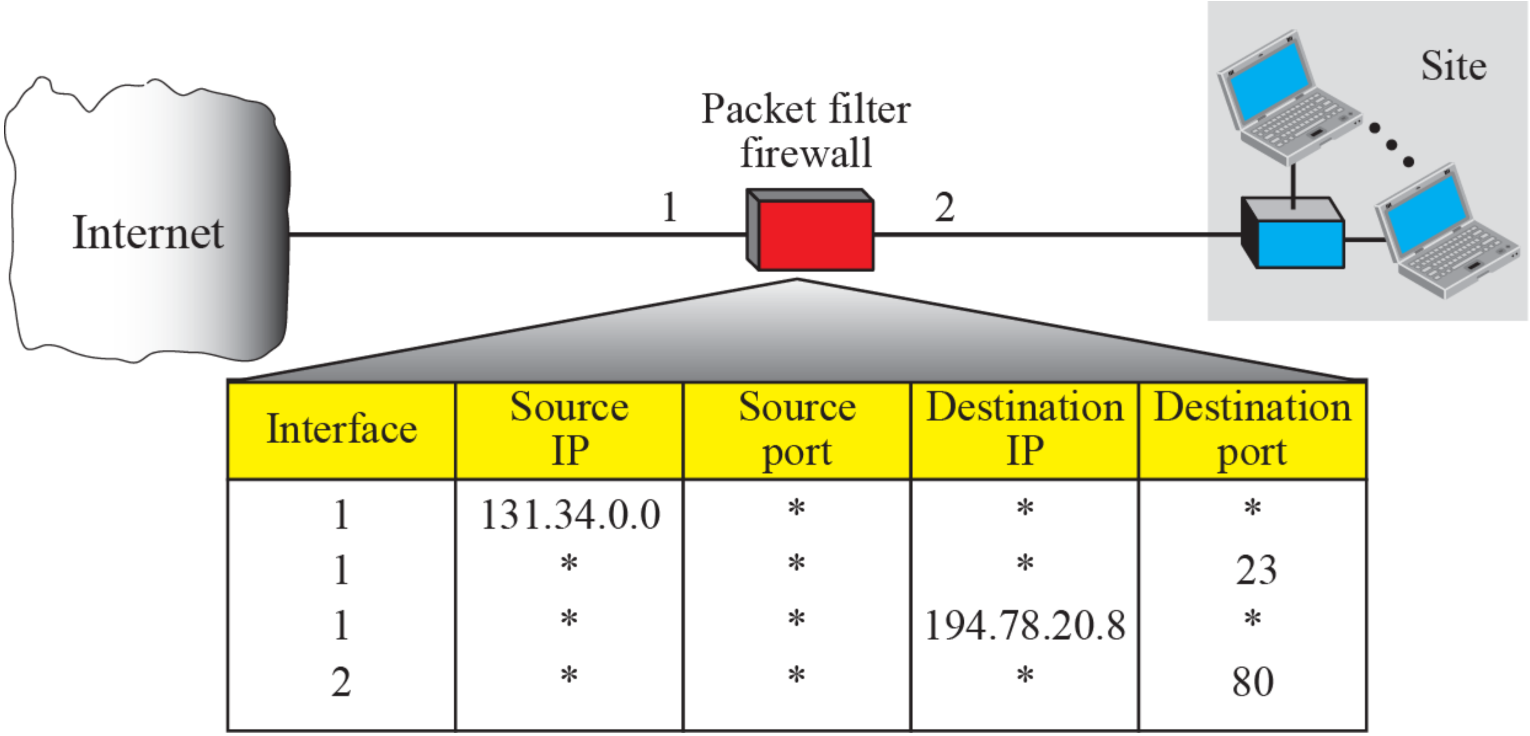
Topics Discussed in the Section

- ✓ **Packet-Filter Firewall**
- ✓ **Proxy Firewall**

.32 Firewall



.33 *Packet-filter firewall*

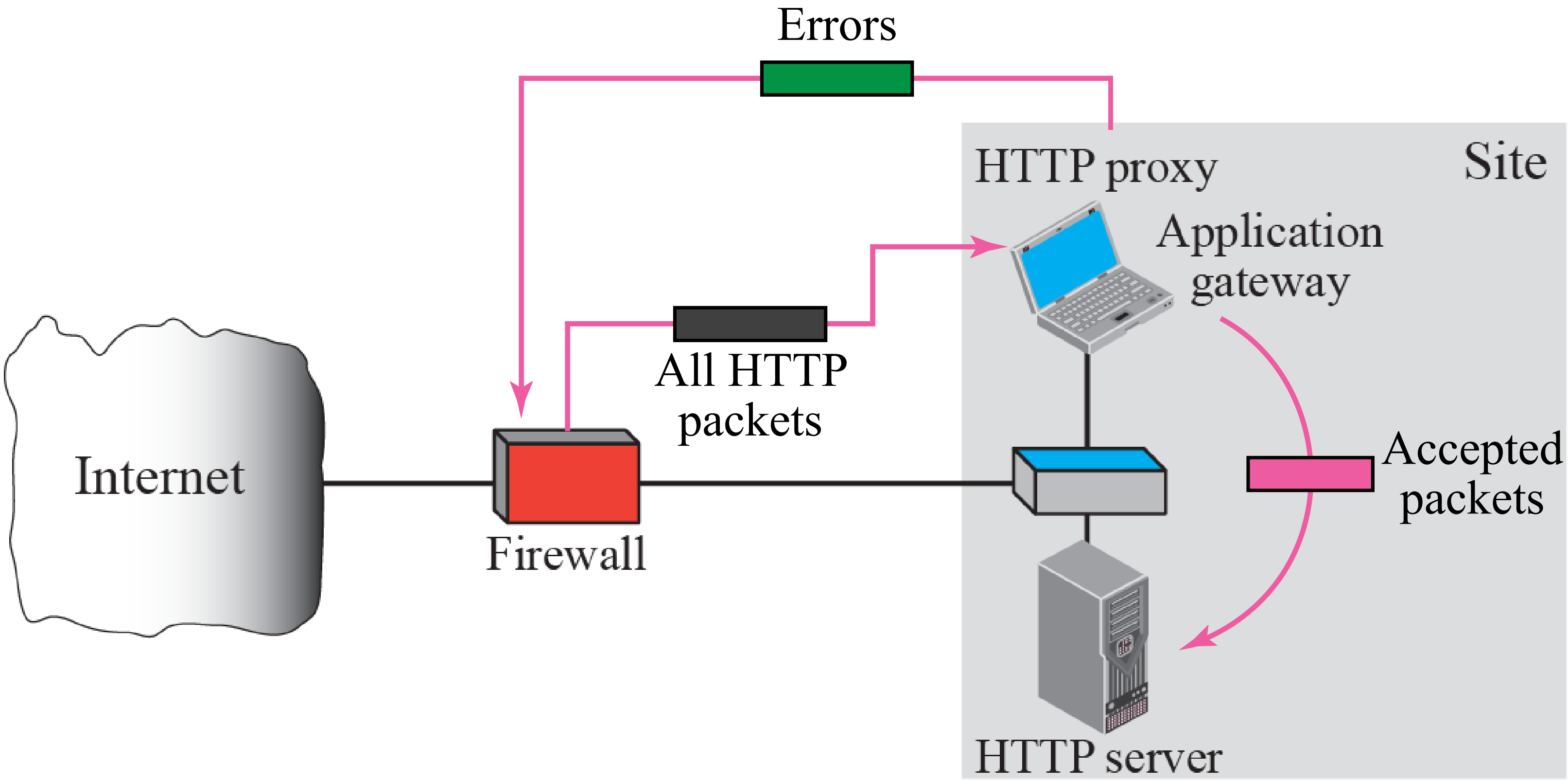


Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

Note

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

.34 *Proxy firewall*



Note

A proxy firewall filters at the application layer.