Security & Cryptography in Computer Networks

Outline

- Introduction
  - Security Services and Mechanisms, Security Attacks
  - Model for Internet Security
- Cryptography
  - Symmetric Key algorithms: DES, 3DES, RC4, etc.
  - Asymmetric Key algorithms: Public-keys, Hash Algorithms, Digital signatures
- Security Protocols
  - Authentication,
  - IP security (IPSec), SSL(TSL), Mail Security(PGP)
- System Security
  - viruses, intruders, worms
  - Firewalls
- Q&A
- References
  - Course Text
  - William Stalling: Cryptography and Network Security: Principles and Practice, 2nd Ed., Prentice Hall.

Introduction, Security Services

- Confidentiality
  - Protection of transmitted data
- Authentication
  - Assuring that communication is authentic
- Integrity
  - Assuring that received message was not duplicated, modified, reordered, and replayed
- Non-repudiation
  - Proving that message was in fact sent by the alleged sender. Access Control
- Access Control
  - Ability to limit and control access to system
- Availability
  - Loss of or reduction of availability(denial of service)

Introduction, Security Mechanisms

- Encryption
  - DES, RC4, AES
- Hash algorithms
  - MD5, SHA
- Public key algorithms
  - RSA
- Digital signatures
- Trusted 3RD parties
- Authentication algorithms
  - Kerberos

Introduction, Security Attacks

- Interruption
  - System is destroyed or becomes unavailable or usable, blocking the communication. Link high-jacking
- Interception
  - Unauthorized party gains access to communication, attack on confidentiality, decrypting communication, traffic analysis
- Modification
  - Unauthorized party not only gains access but also tampers with communication. Changing value in data file
- Fabrication
  - Unauthorized party inserts counterfeit information into communication, attack on integrity. Creating artificial messages.

Security Treats

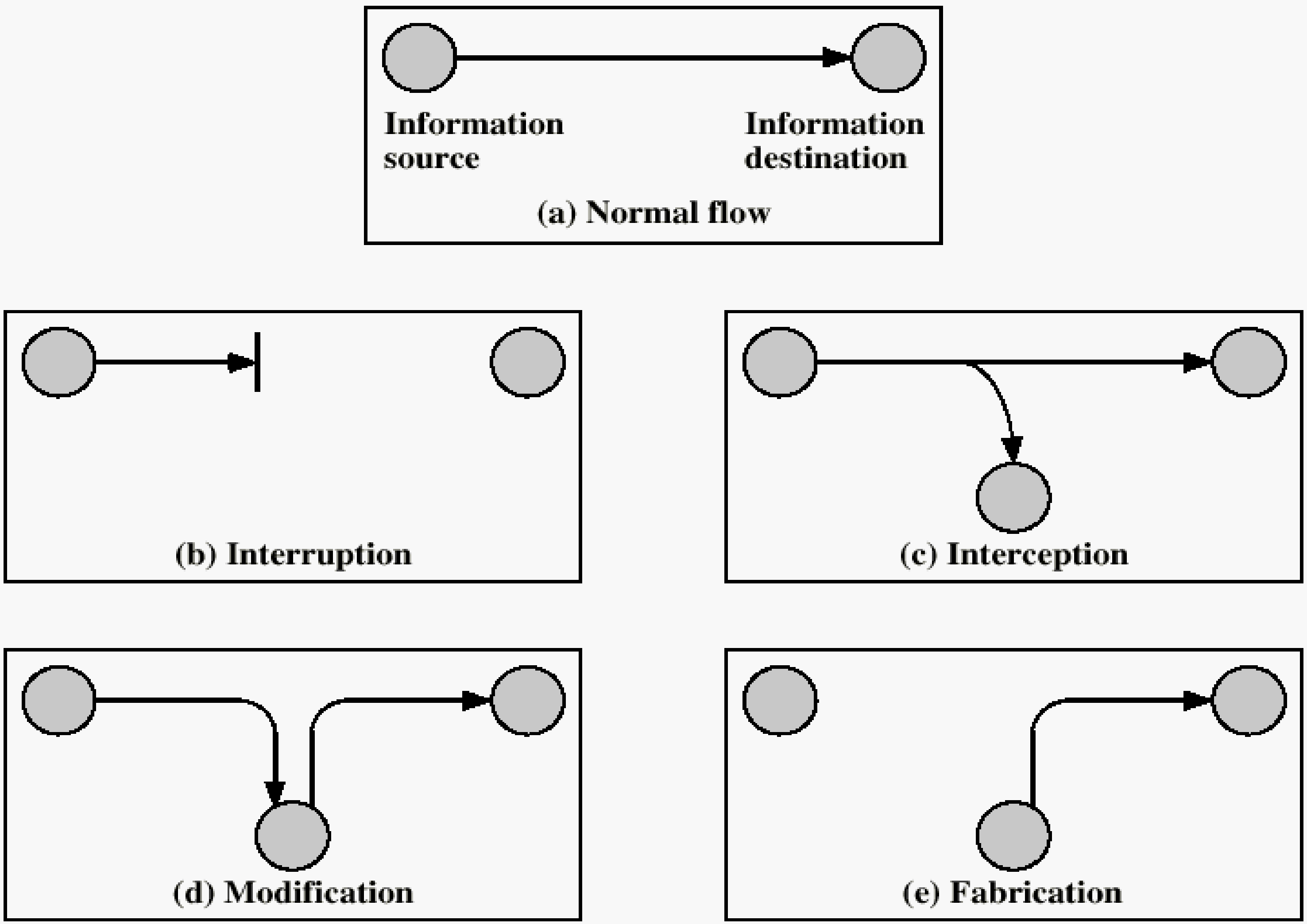


Figure 1.1 Security Threats

Security Treats

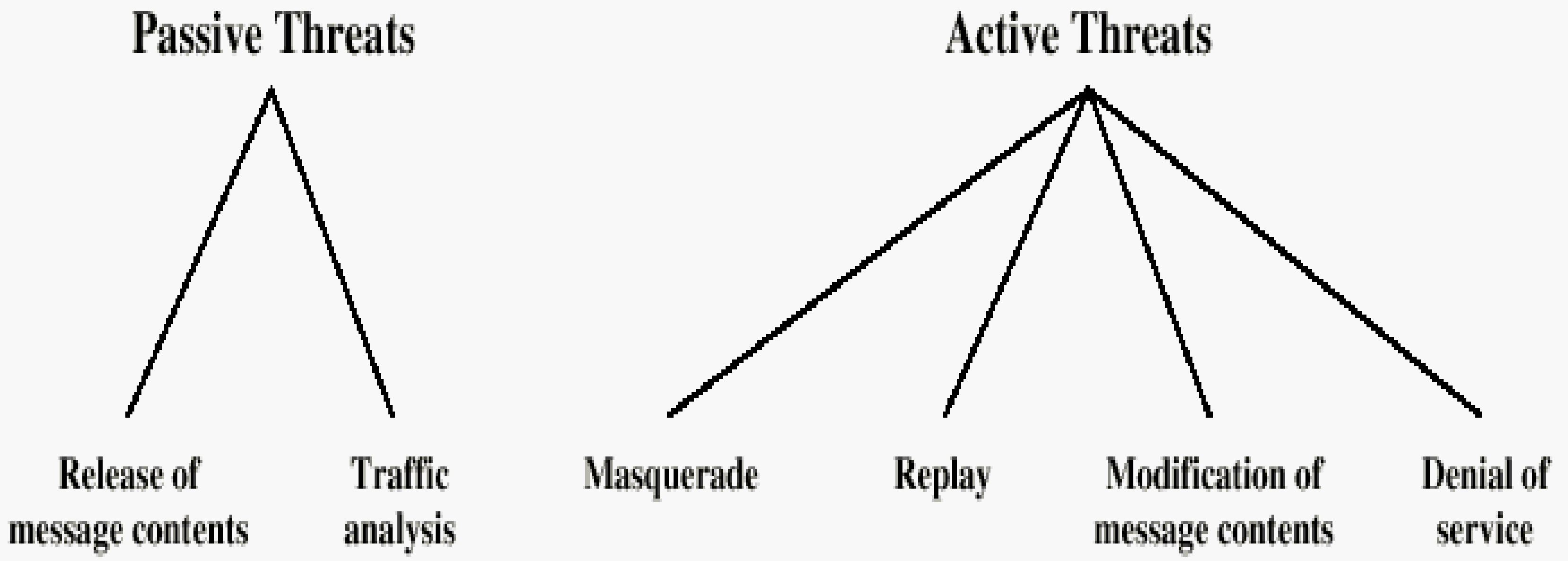


Figure 1.2 Active and Passive Security Threats

Cryptography, Conventional Encryption Model

- Cryptography:
  - Operation used for transforming plaintext to ciphertext
    - Substitution: elements in plaintext are mapped into another element
    - Transposition: elements in plaintext are rearranged
  - Number of key used
    - Both sender and receiver use the same key, system is symmetric single-key, secret-key or conventional encryption
    - Sender and receiver each uses a different key, system is asymmetric key
  - Way in which the plaintext is processed
    - Block cipher, input data processed block by block
    - Stream cipher, input data processed continuously
- Cryptanalysis
  - Process (science) to break encryption

Conventional Encryption

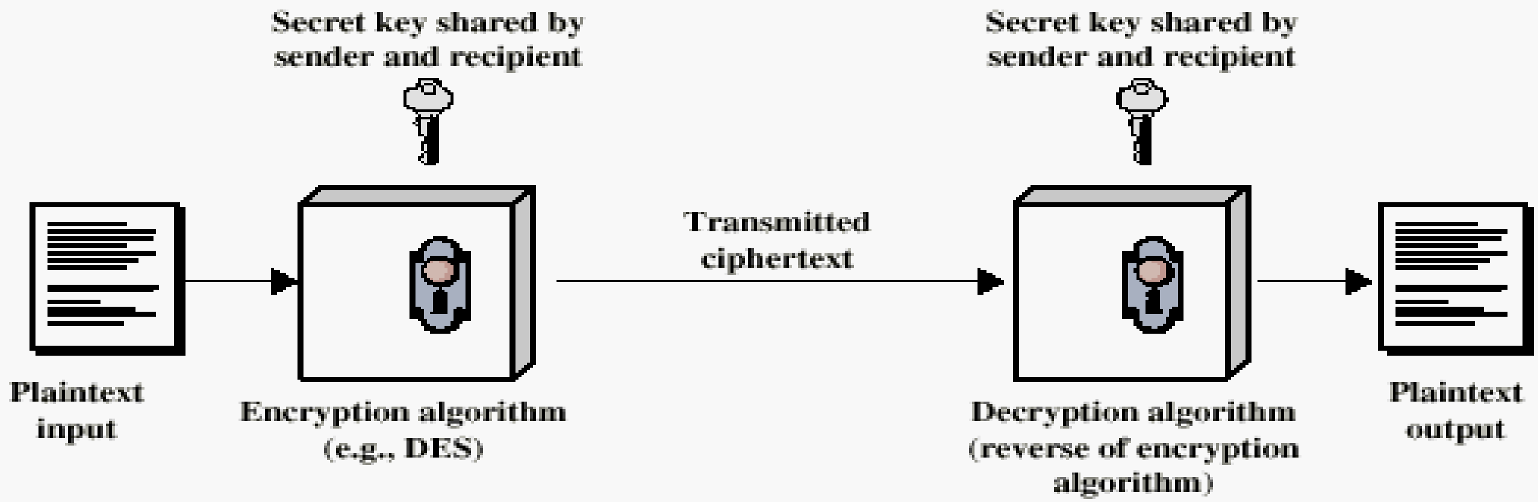


Figure 2.1 Simplified Model of Conventional Encryption

$$\text{Ciphertext} = \text{Plaintext} \oplus \text{Key}$$

$$\begin{aligned}\text{Plaintext} &= \text{Ciphertext} \oplus \text{Key} \\ &= (\text{Plaintext} \oplus \text{Key}) \oplus \text{Key} \\ &= \text{Plaintext} \oplus (\text{Key} \oplus \text{Key}) \\ &= \text{Plaintext}\end{aligned}$$

Classical Encryption Techniques

- Cesar Cipher
  - Plain: `meet me after the party`
  - Cipher: `PHHW PH DIWHU WKH SDUWB`

  C=E(m)=(m+4) mod(26)=P

  P=m+4 (m, m+1=N, m+2=L, m+3=O, "P")
- Polyalphabetic Cipher
  - Key: `deceptiondeceptiond`
  - Plain: `meetmeafterthe party`
  - Cipher: `qjhxcyjuhiwwkujjghc`

  C=E(k⊕p), ⊕ is exclusive-or(XOR)
- Rotor Machines: Famous "ENIGMA"

These techniques became very weak around and after World War II with introduction of computers

Modern Cryptographic Algorithms

Cryptography Algorithms

Secret Key

- Symmetric key
- Block cipher

  (DES, AES)
- Stream ciphers

  (RC4)

Hash algorithms

Authentication and integrity checking

(MD5, SHA)

Public Key

- Asymmetric key
- Public-Private keys

(Diffie-Hellman RSA)

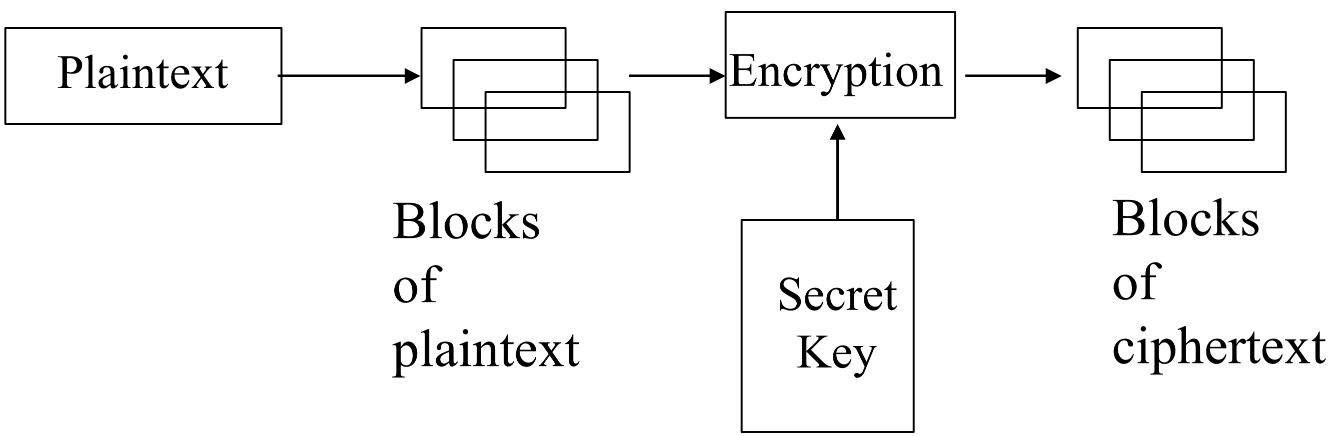
What Cryptography Does?

- Diffusion:
  - Statistical structure of the plaintext is dissipated into long range, each plaintext digit affect the many ciphertext digits.
- Confusion:
  - Seeks to make the relationship between the statistics of ciphertext and the value of encryption as complex as possible.

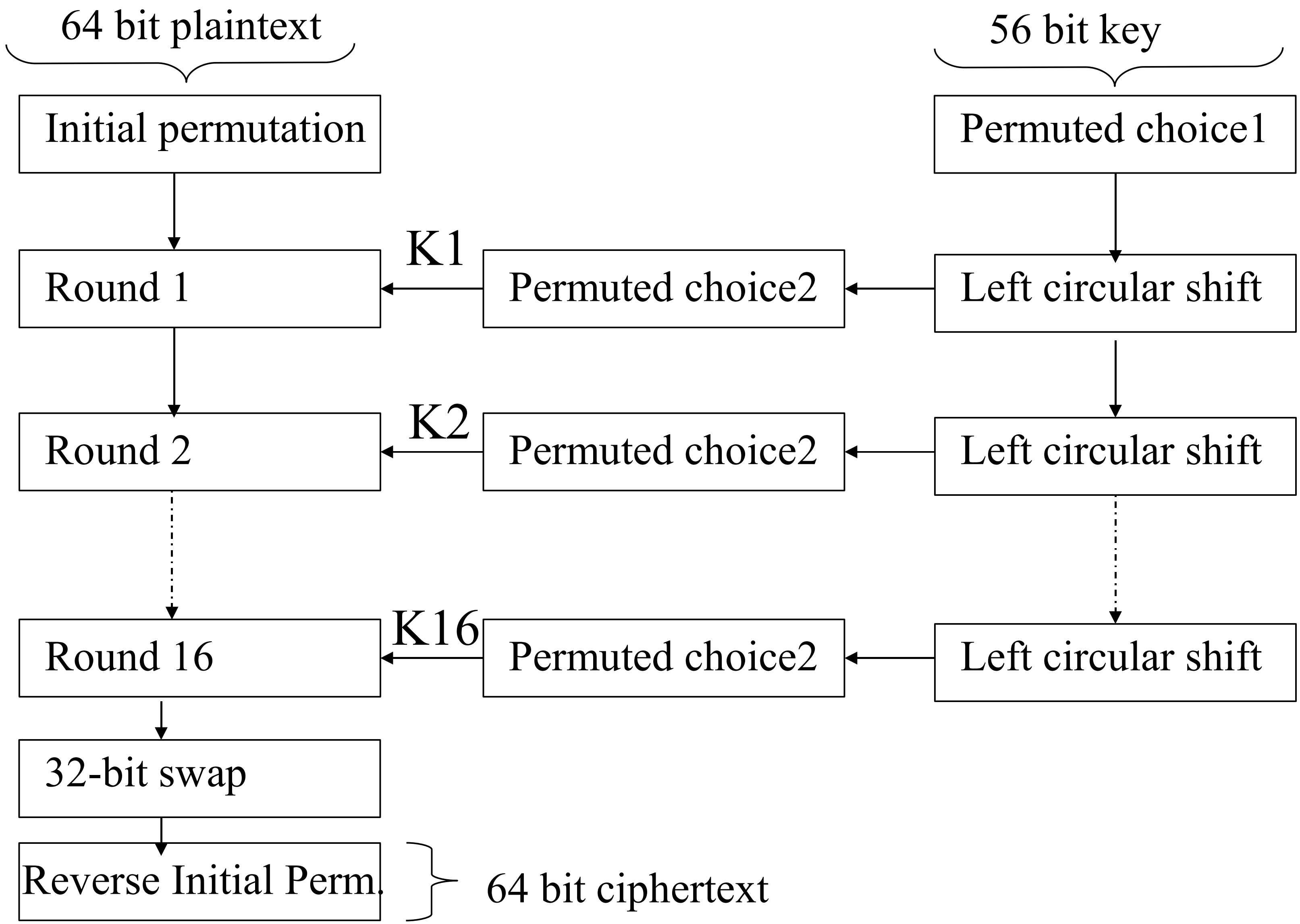
Key sizes and Brute Force Attacks

Block Ciphers

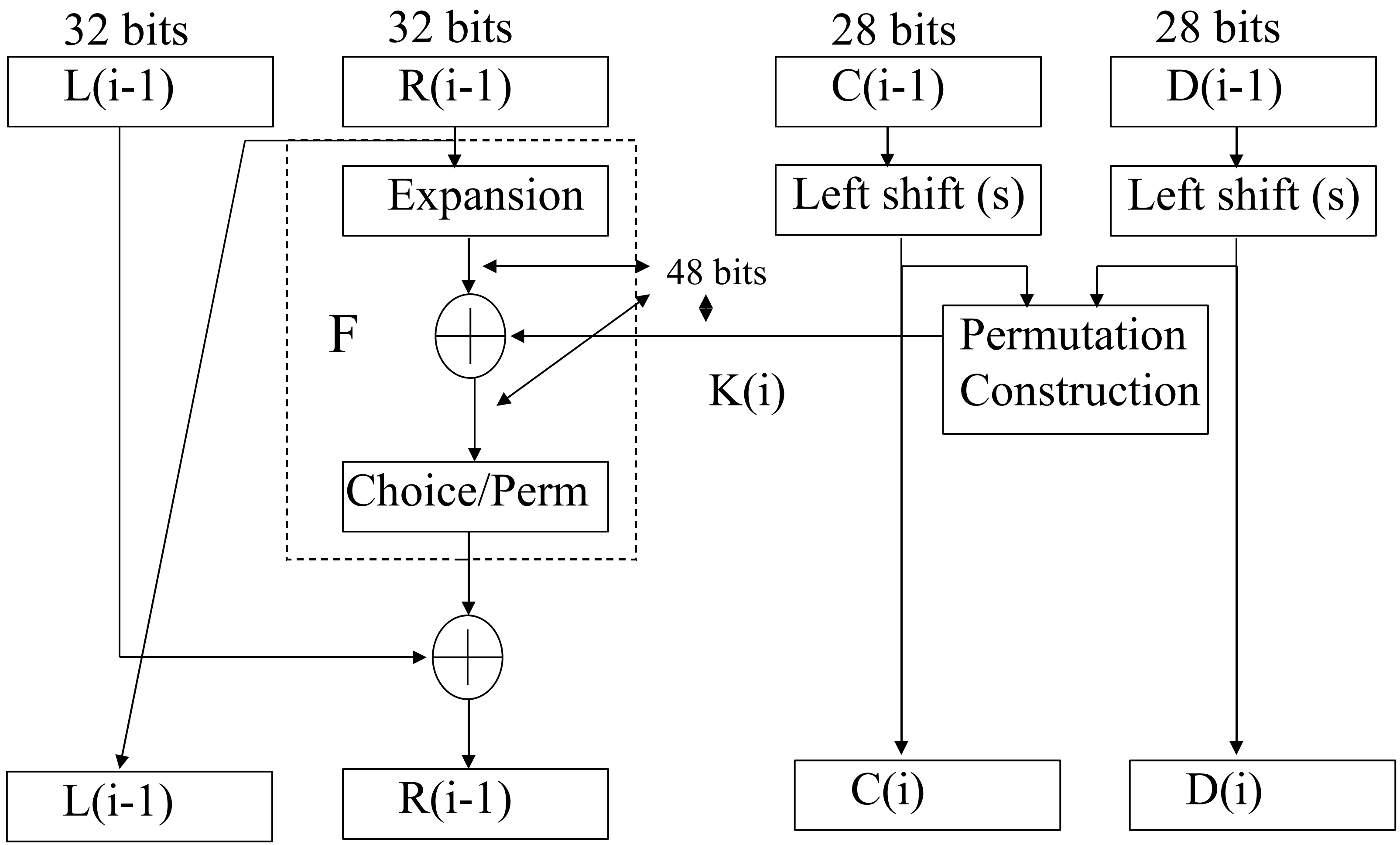
- Block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Example: DES(Data Encryption Standard), AES(Advance Encryption Technique)



General DES Encryption Algorithm



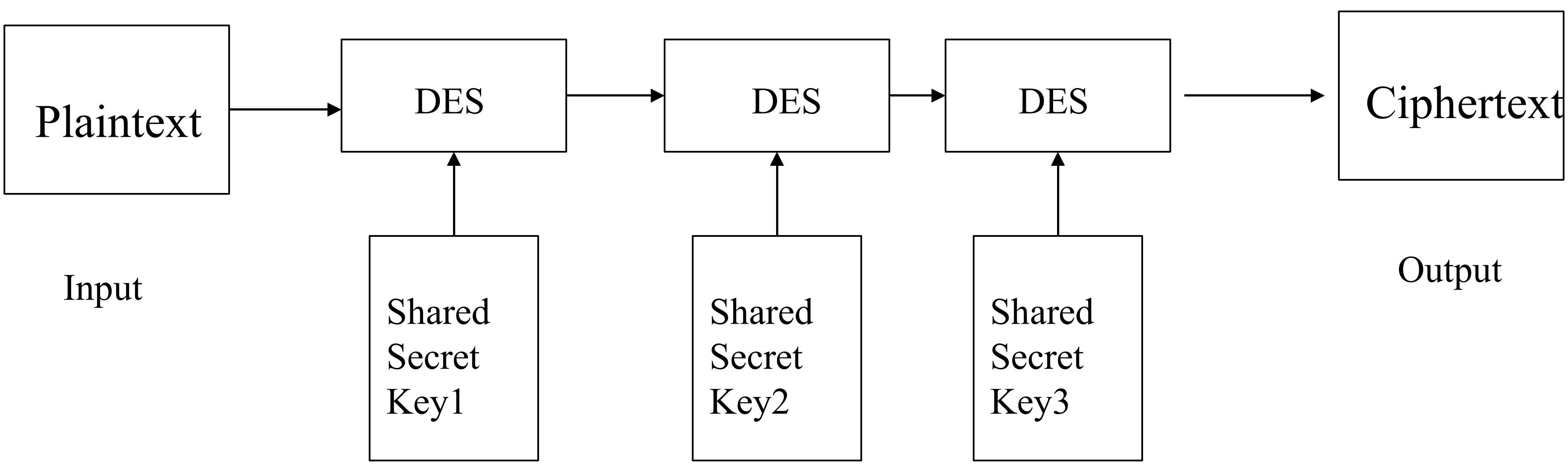
Single Round of DES Algorithm



$$L(i)=R(i-1),\ R(i)=L(i-1) \oplus F(R(i-1),K(i))$$

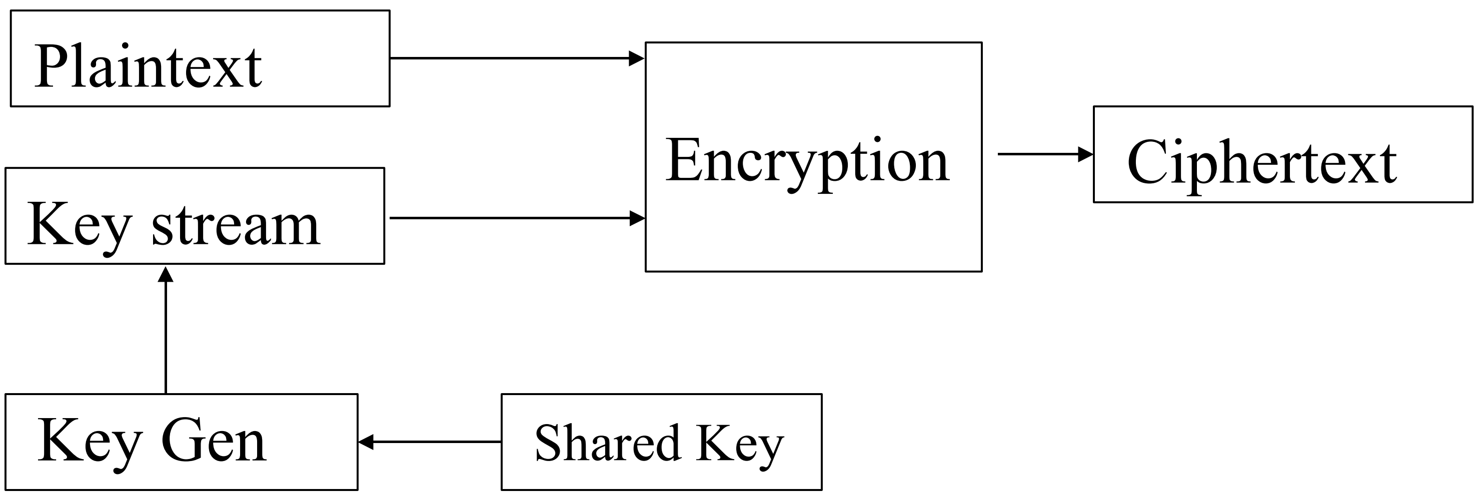
3DES

- DES key is 56 bit, not good enough, but widely available in HW and SW, so use three times with different keys.



Stream Ciphers

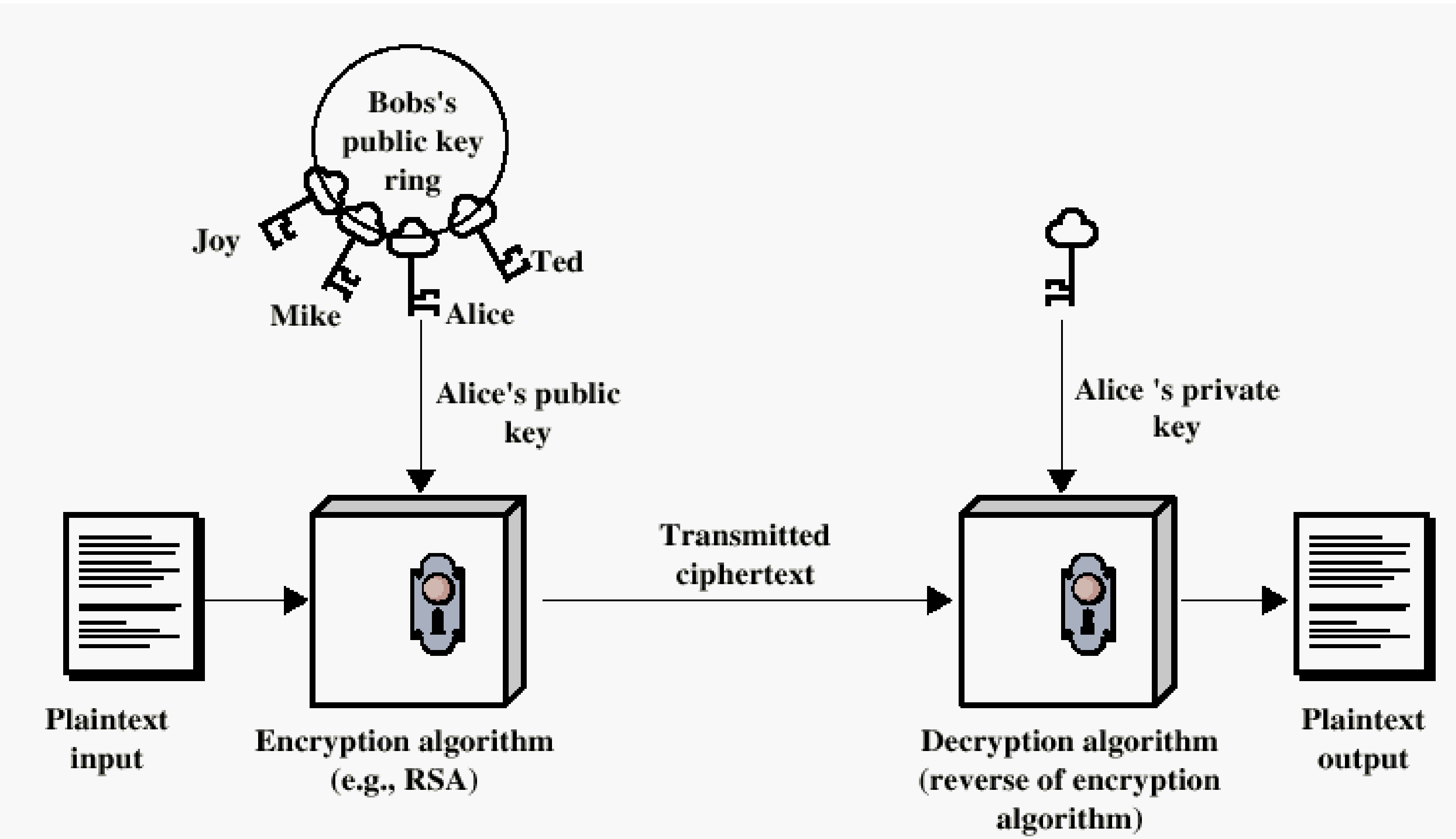
- Encrypt a digital data stream one bit or one byte at a time
- Example: RC4(Rivest Cipher-4)



Key Distribution

- Key could be selected by A and physically delivered to B.
- Third party could select the key and physically deliver it to A and B.
- If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.
- If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

View of Public Key Scheme



Public Key Ciphers
Diffie-Hellman Key Exchange

- Enable two users to exchange keys
- Depends on difficulty of computing discrete logarithms
  - P is prime number, A is its primitive root of P; so numbers A mod(P), A^2 mod(P), …..,A^{P-1} mod(P) are distinct and consists of integers from 1 through p-1 in some permutation.

  - If P=11, then A=2 is primitive root with respect to P

2^1 mod(11)=2, 2^2mod(11)=4, 2^3mod(11)=9, 2^4mod(11)=5, … ……,2^{10}mod(11)=1

Diffie-Hellman

- Global public elements, prime number P, and E primitive root and E< P
- User A selects private XA where XA <P,

  Calculates public YA $YA = E^{XA} mod(P)$
- User B selects private XB where XB <P,

  Calculates public YB $YB = E^{XB} mod(P)$

- User A calculates K, $K=(YB)^{XA} mod(P)$
- User B calculates K, $K=(YA)^{XB} mod(P)$

Diffie-Hellman(example)

- Global public elements, prime number and primitive root
  P=97 and E=5
- User A selects private XA=36 where XA <P,

  Calculates public YA YA $=5^{36} \bmod(97)=50$
- User B selects private XB=58 where XB <P,

  Calculates public YB YB $=5^{58} \bmod(P)=44$

- User A calculates K, $K=(YB)^{XA} \bmod(97)$

  $= 44^{36} \bmod(97)=75$
- User B calculates K, $K=(YA)^{XA} \bmod(97)$

  $= 50^{58} \bmod(97)=75$

Public Key Ciphers

- RSA(Rivest, Shamir, Adelman)
  - Similar to Diffie-Hellman, uses large exponentials, plaintext is encrypted in blocks having a binary value N.
  - M is plaintext block, e is exponent then,
    - $C=M^e \bmod(n)$ C, ciphertext so encryption
    - $M=C^d \bmod(n)= (M^e)^d \bmod(n)= M^{ed} \bmod(n)$
- Public key (e,n), Private key (d,n)
- Requirements
  - Possible to find values of e,d,n to satisfy above calculations
  - Relatively easy to calculate M^e and C^d for all values of $M<n$
  - Infeasible to determine d given e and n

The RSA Algorithm – Key Generation

1. Select *p,q* — *p* and *q* both prime
2. Calculate $n = p \times q$
3. Calculate $\Phi(n) = (p-1)(q-1)$
4. Select integer *e* $\gcd(\Phi(n), e) = 1;\ 1 < e < \Phi(n)$
5. Calculate *d* $d = e^{-1} \bmod \Phi(n)$
6. Public Key KU = {e,n}
7. Private key KR = {d,n}

Example of RSA Algorithm

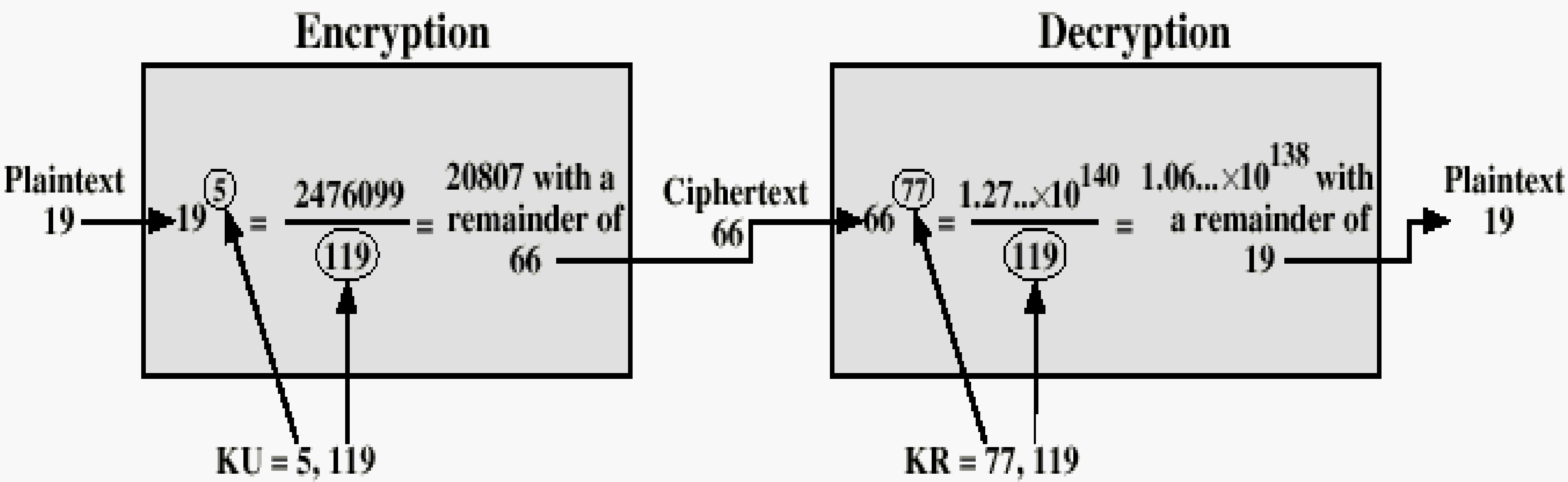
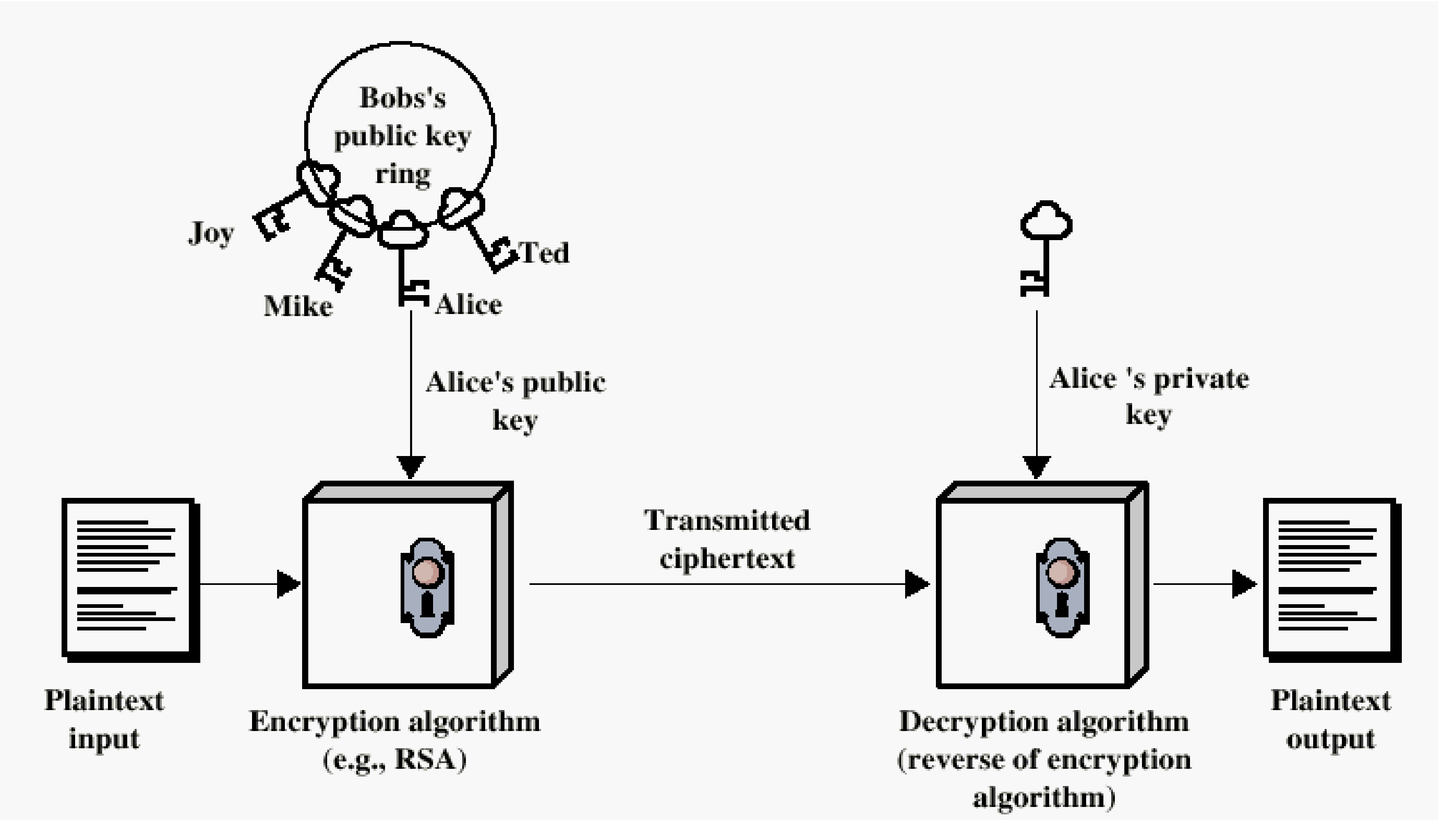
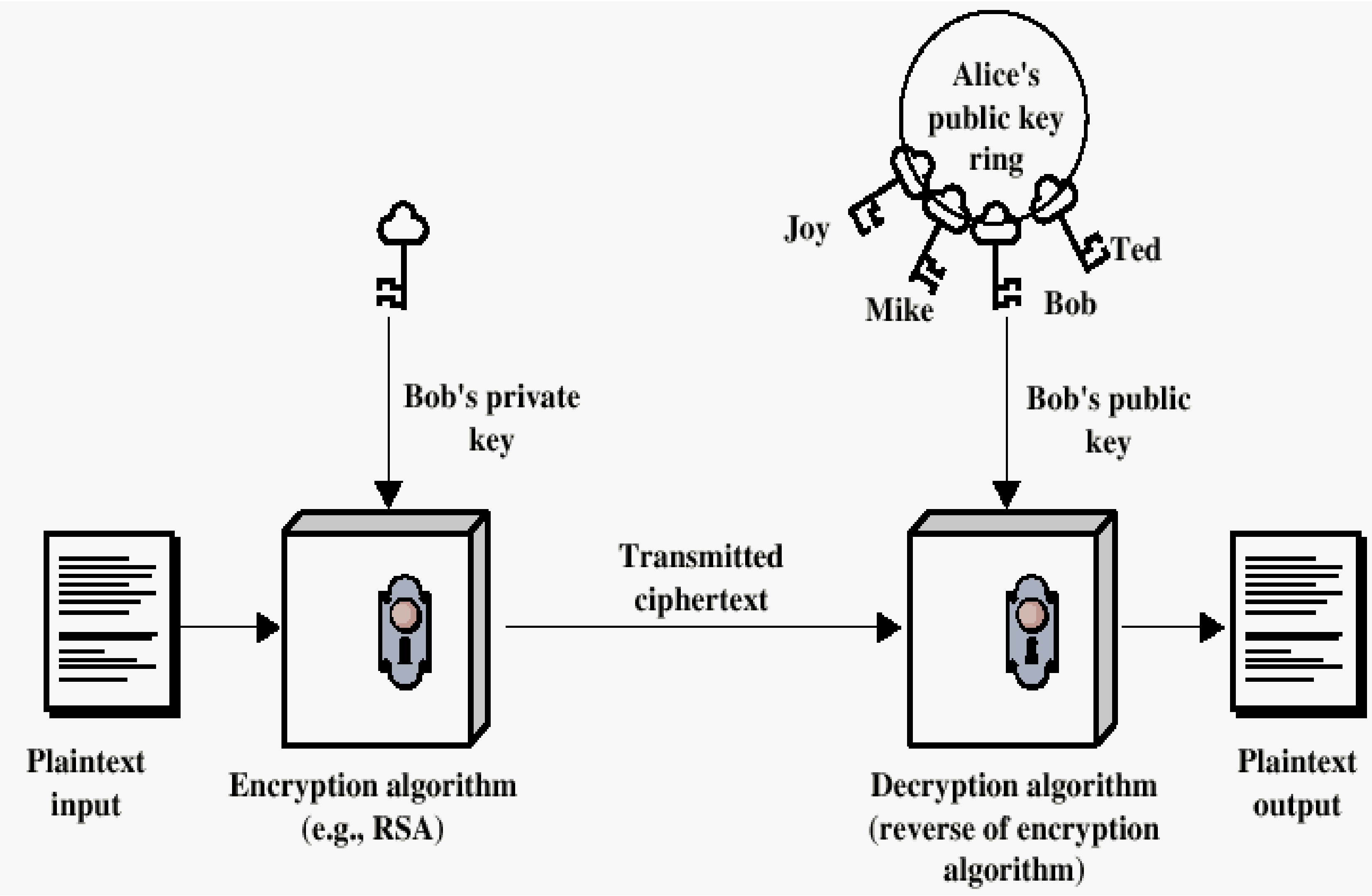


Figure 3.9 Example of RSA Algorithm

Encryption with Public Keys



Authentication with Public Keys



Hash Algorithms (requirements)

Produce a FINGERPRINT of the message or entity

- Can be applied to a block of data of any size
- Produces fixed length output
- Relatively easy to compute both HW and SW
- It should be infeasible to compute message from hash (one-way property)
- Computationally infeasible to get same hash value for different messages (weak collision resistance), protect from modification
- Computationally infeasible to find any message pair whose have same hash values (strong collision resistance), protect duplications

Hash Algorithms(one-way functions)

- Integrity checking, authentication of the message

```
Message => MD5 output (128bit)
1234567890 => 7c12772809c1c0c3deda6103b10fdfa1
1234567891 => eac9407dc999ae35ba5e6851e28d7c53
```

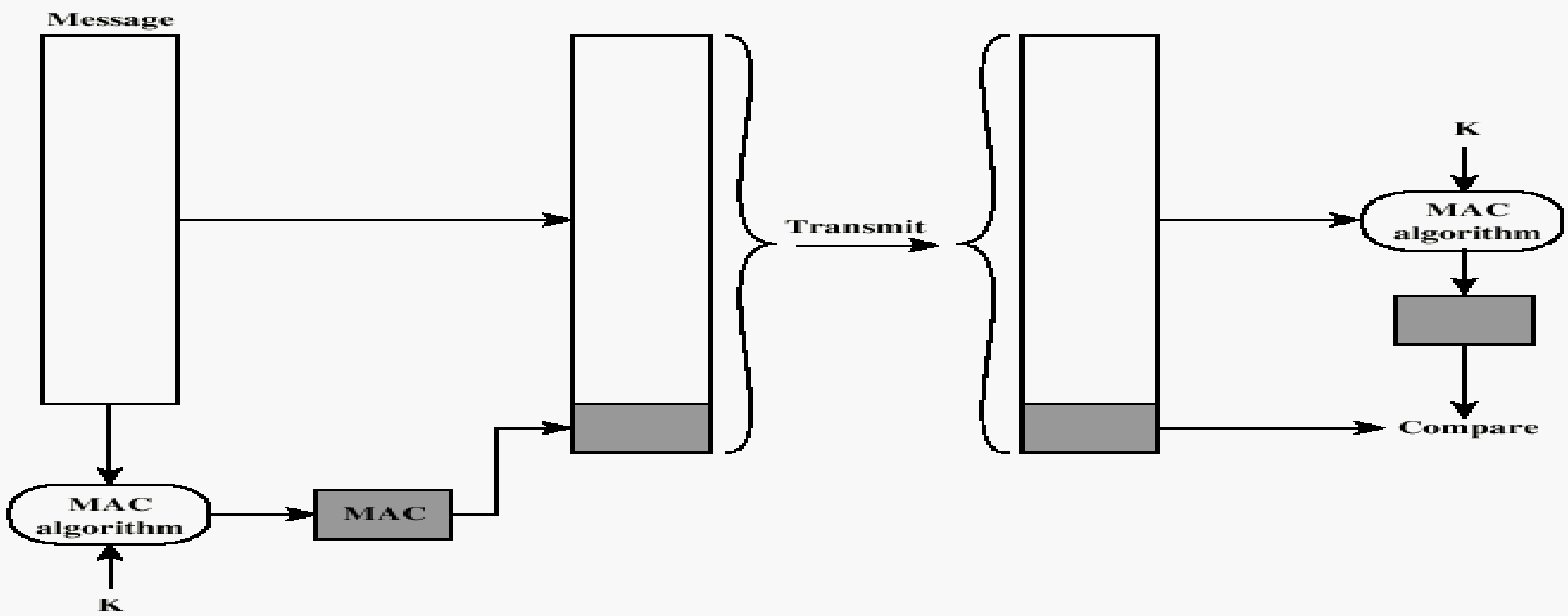
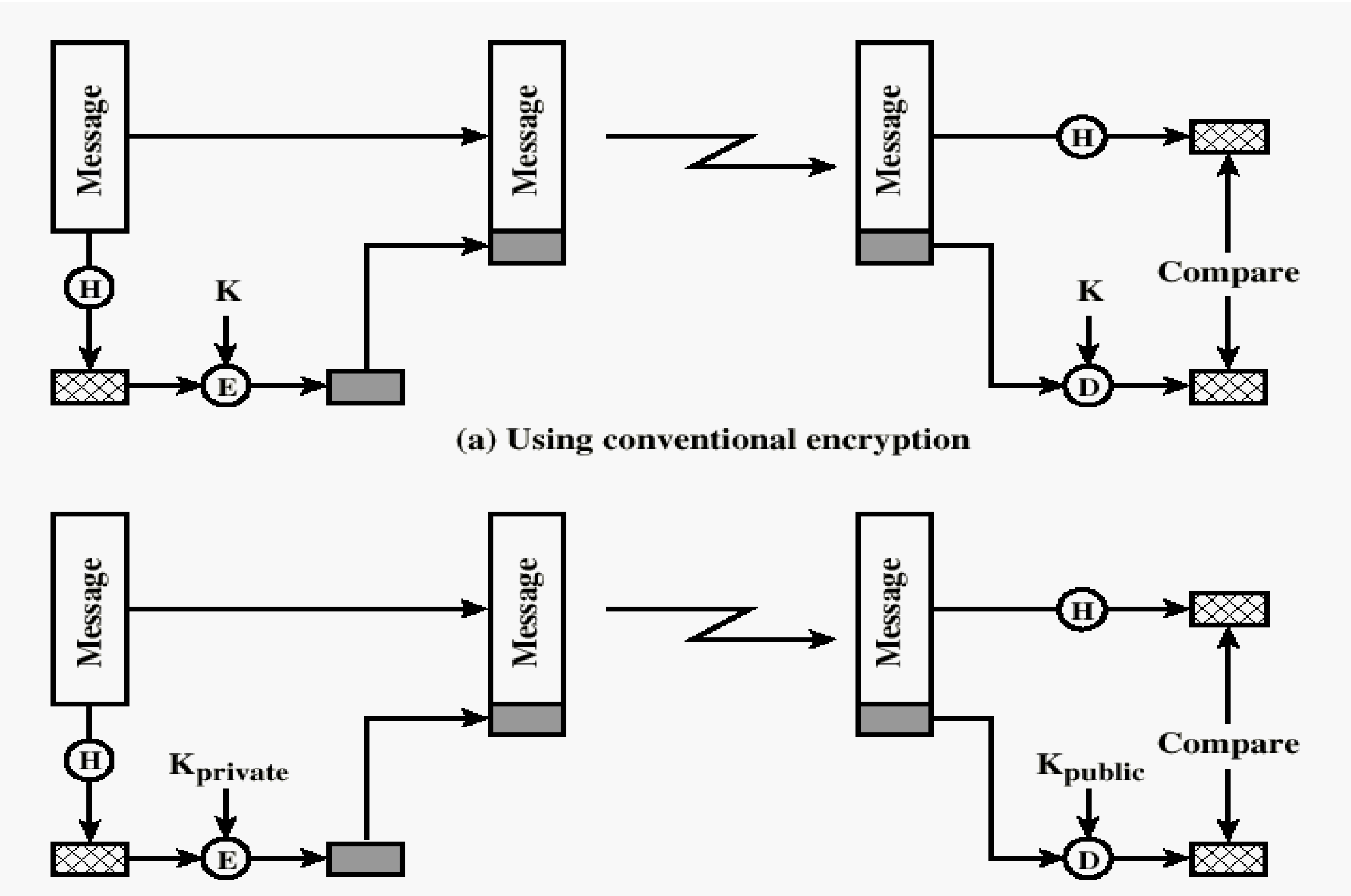


Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Using Hash Algorithm

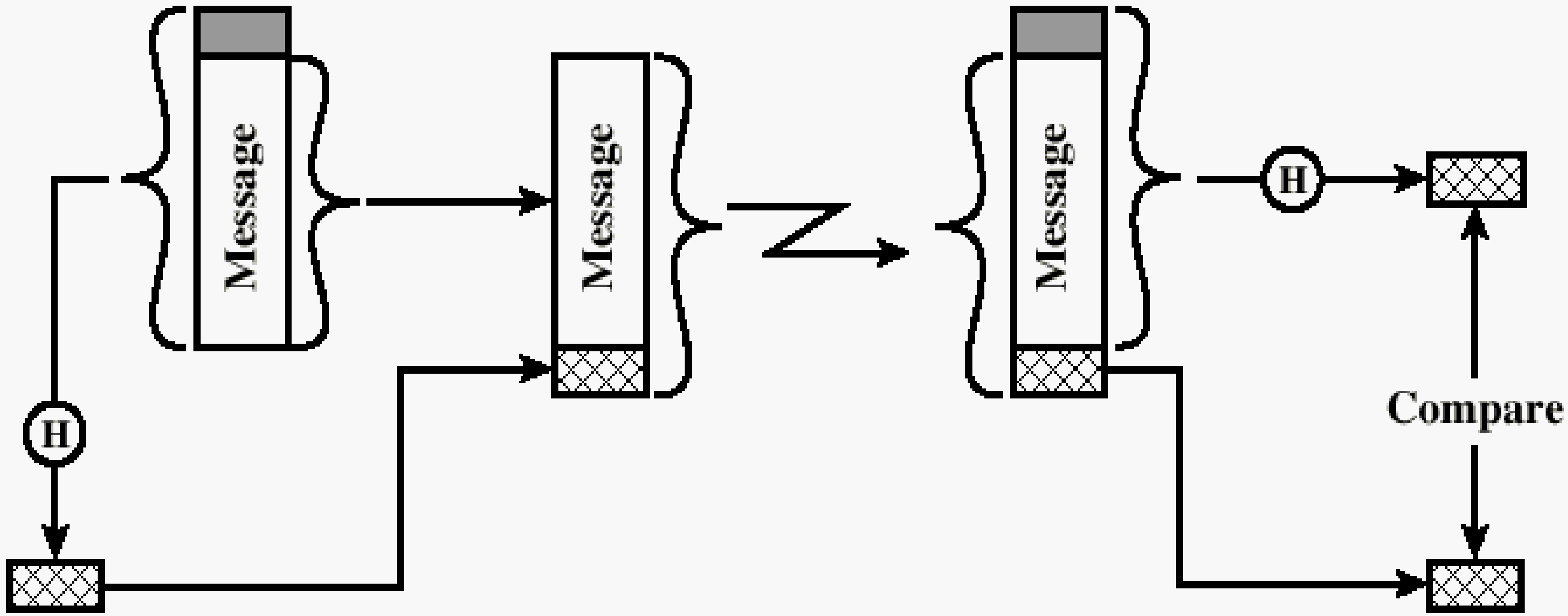


(a) Using conventional encryption

(b) Using public-key encryption

Using Hash Algorithm-2

- Secret value is added before the hash and removed before transmission.

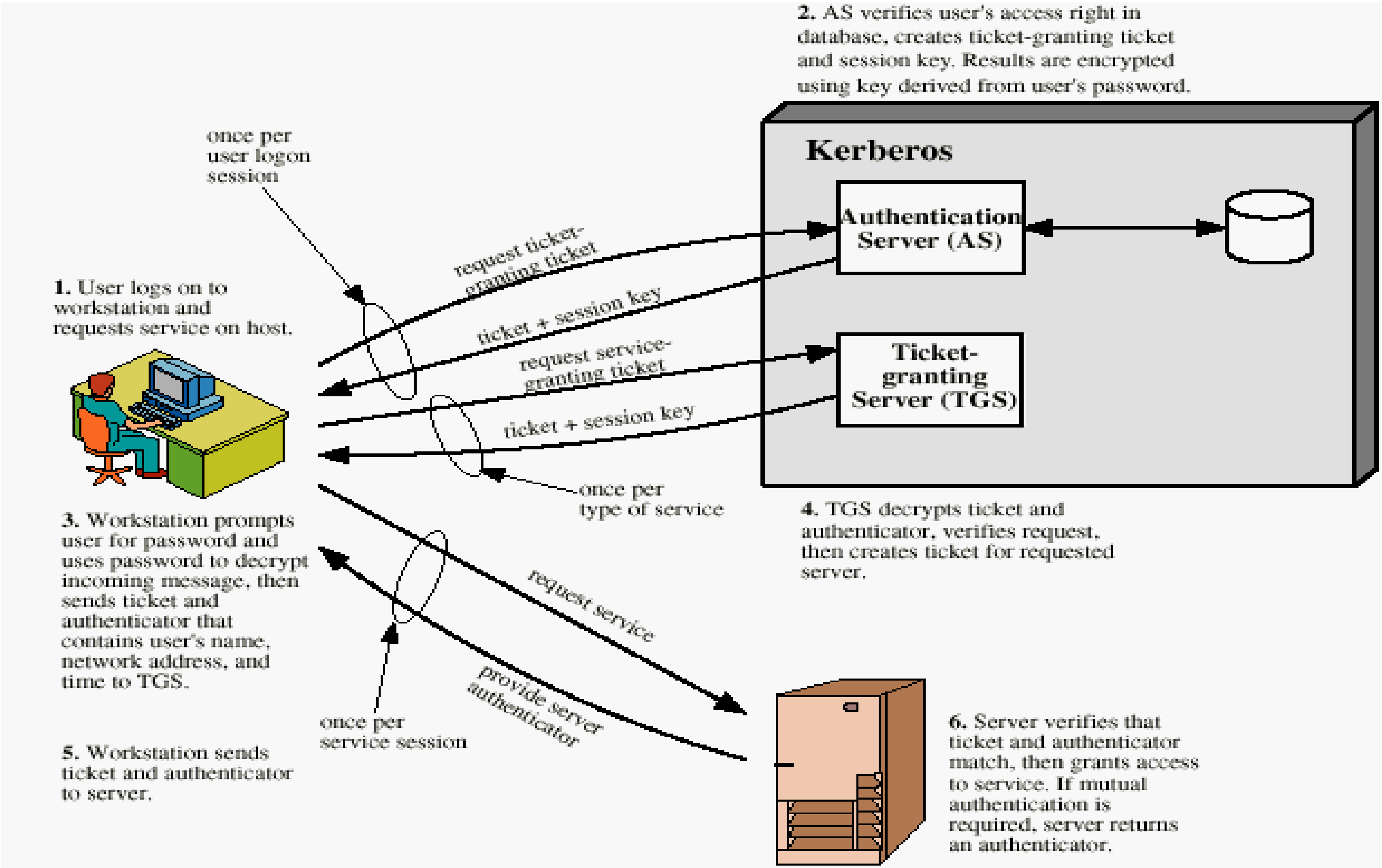


(c) Using secret value

Security Protocols

- Authentication
  - Three-way hand shake, client and server have shared secret key
  - Trusted third party (as in Kerberos)
  - Public Key Authentication (RSA)
  - Digital signatures

Authentication with KERBEROS



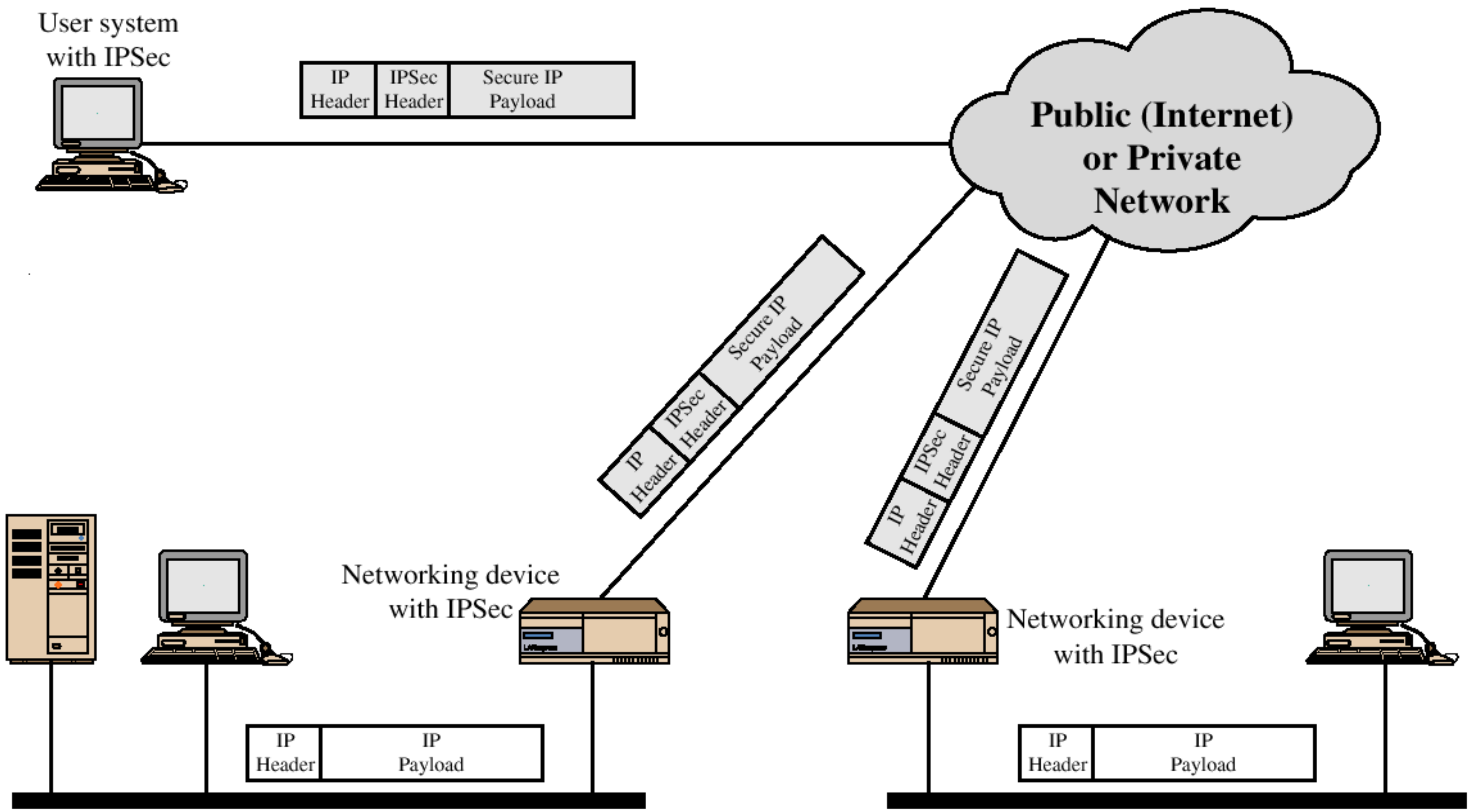
IP Layer Security Protocol (IPSec)

- Suite of protocols developed by IETF to address security at the IP level, and provide secure communications across the Internet
- IPSec supports the following features
  - Two security protocols: 1) Authentication Header (AH), and 2) Encapsulating Security Payload (ESP)
  - Two modes of operation: 1) Transport, and 2) Tunnel
  - Two key management protocols: 1) Internet Key Exchange (IKE), and 2) IP Security Association Key Management Protocol (ISAKMP)
  - Six security services: 1) Access control, 2) Connectionless integrity, 3) Data origin authentication, 4) Rejection of replayed packets, 5) Confidentiality (encryption), and 6) Limited traffic flow confidentiality
  - Security policies that determine how machines communicate via IPSec, and the security services they can access
  - Support for IPSec features is optional (mandatory) for IPv4 (IPv6)

IP Security Overview

- Benefits of IPSec
  - Transparent to applications (below transport layer (TCP, UDP)
  - Provide security for individual users
- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

IP Security Scenario



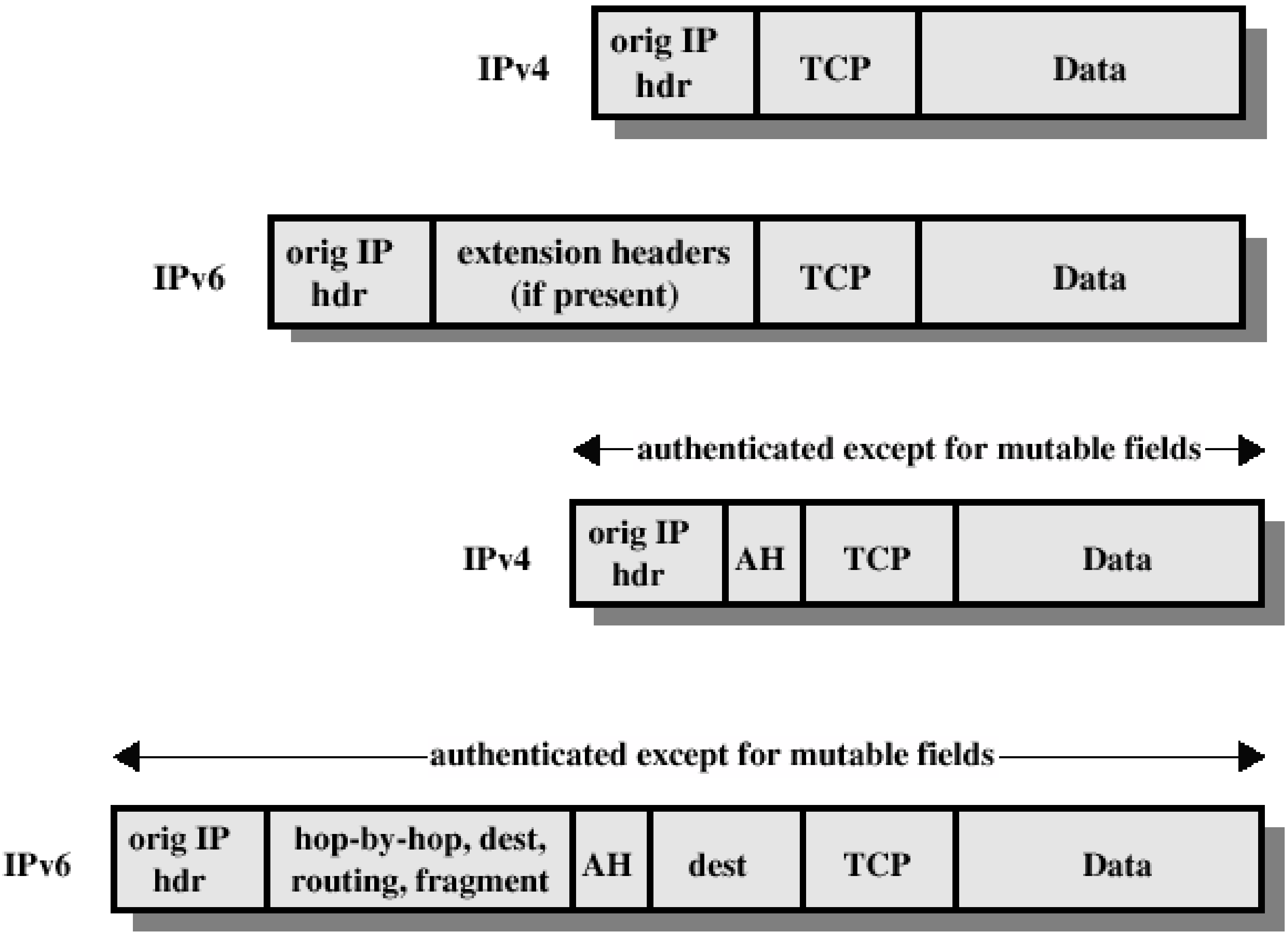
IPSec Modes

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extesion header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

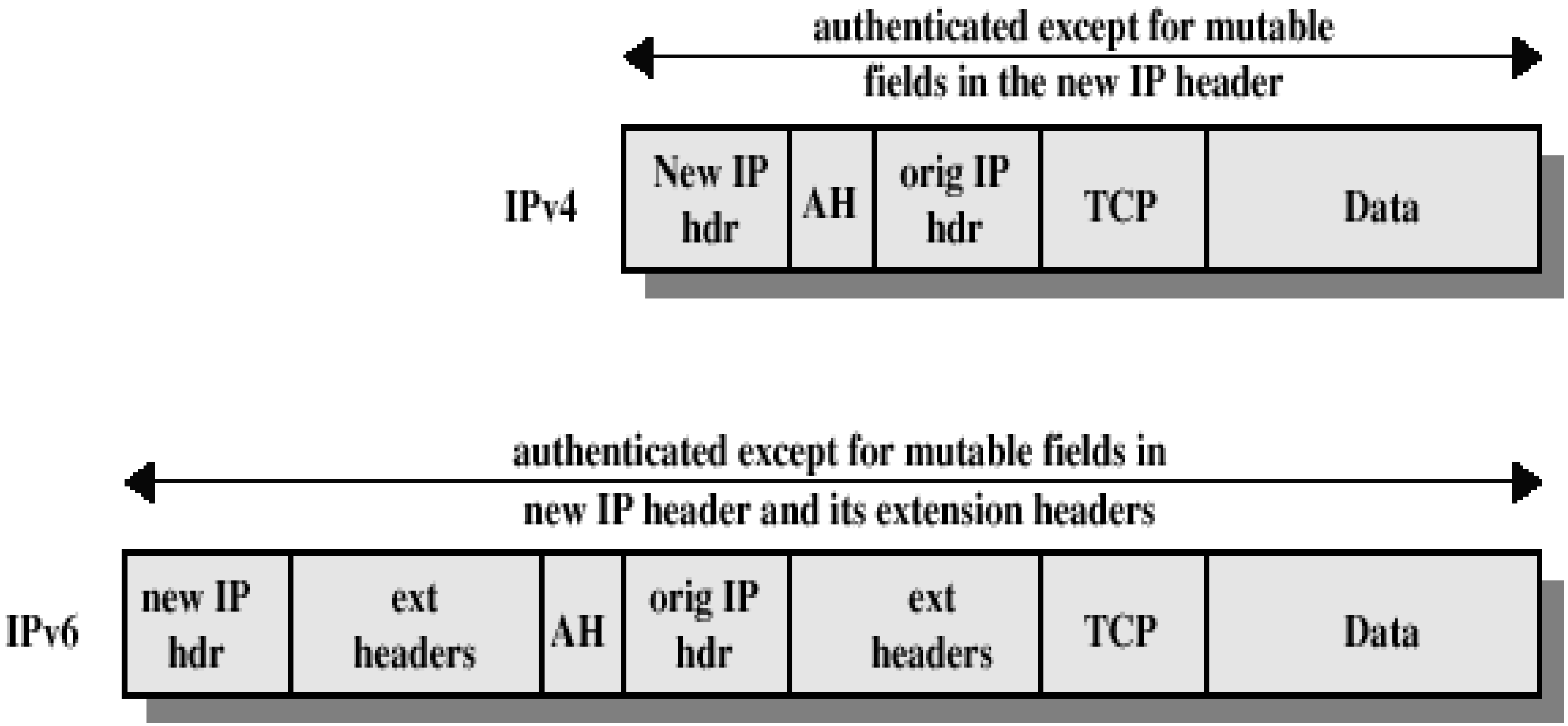
IP Security (IPSec Services)

Services	Security Protocol		
	AH	ESP (Encryption only)	ESP (Encryption plus Authentication)
Access Control	√	√	√
Connectionless Integrity	√		√
Data Origin Authentication	√		√
Rejection of Replayed Attacks	√	√	√
Confidentiality		√	√
Limited Traffic Flow Confidentiality		√	√

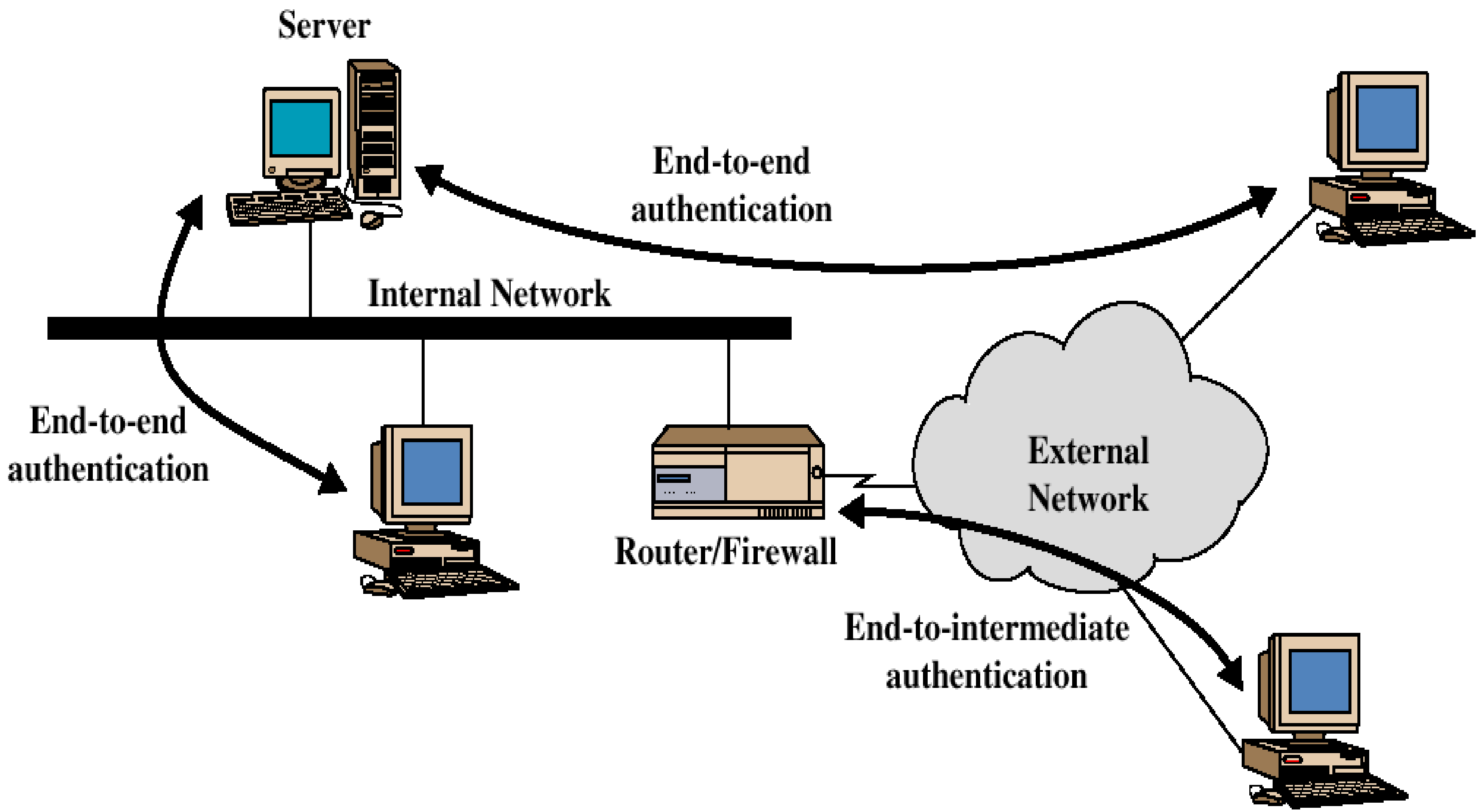
IPSec Headers in AH



Tunnel Mode (AH Authentication)



End-to-end versus End-to-Intermediate Authentication

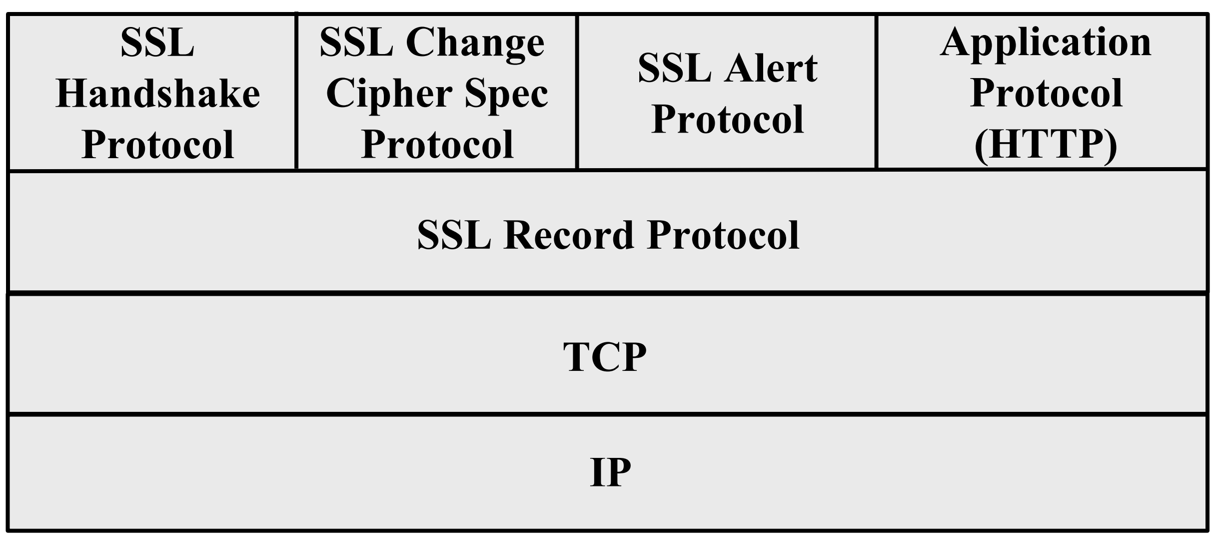


Web-Based Security SSL,TLS and WTLS

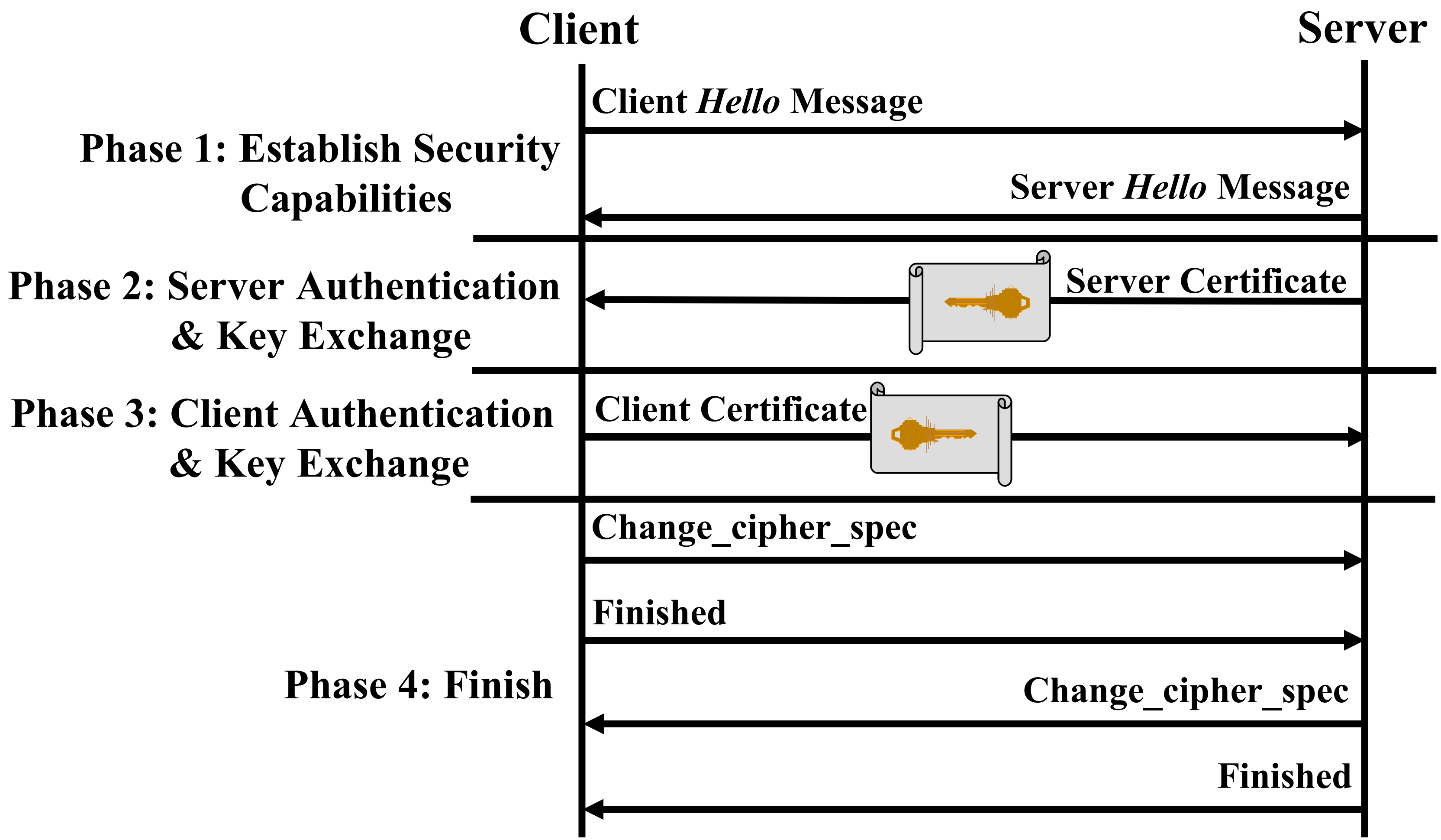
- SSL was originated by Netscape
- TLS working group was formed within IETF
- First version of TLS can be viewed as an SSLv3.1
- Wireless TLS (WTLS) Protocol

Web-Based Security (SSL Protocol)

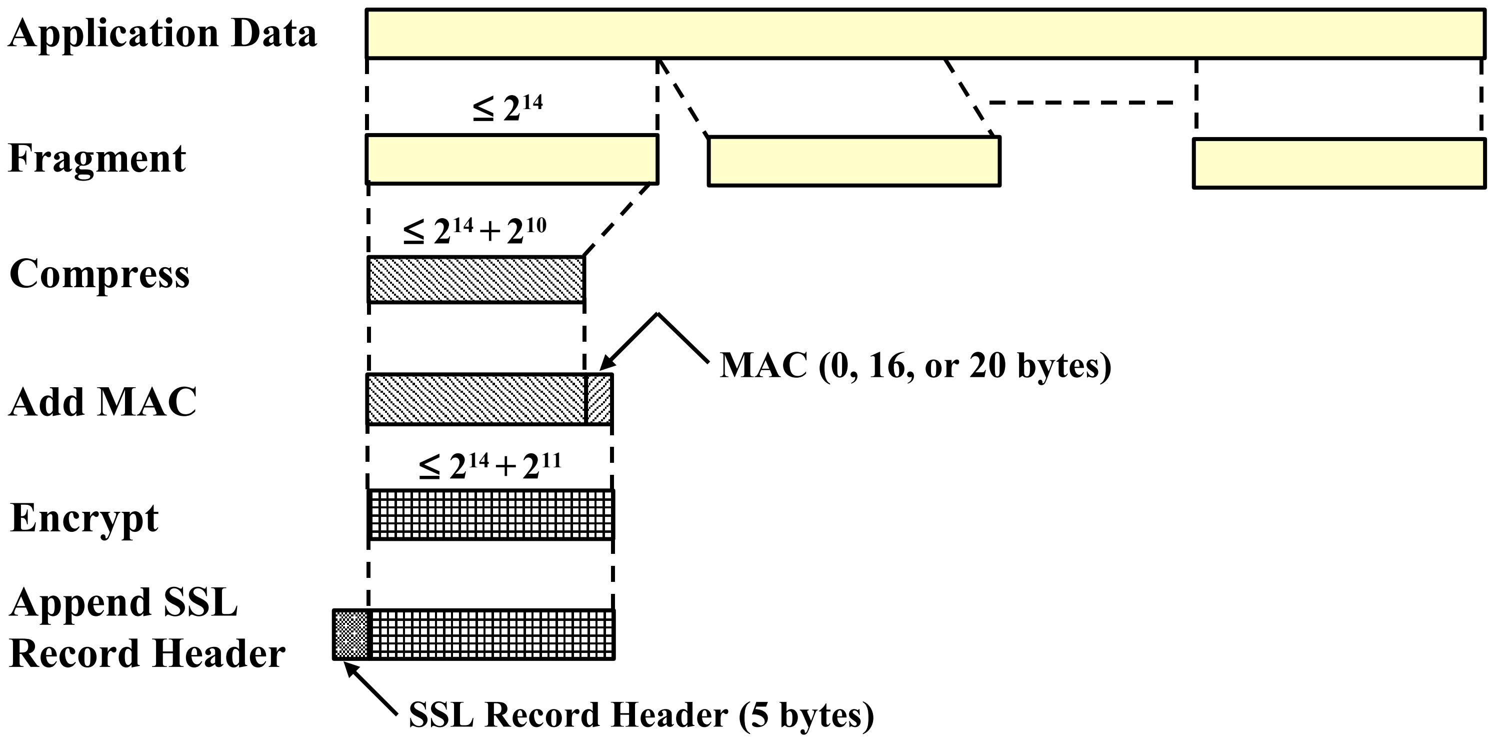
- Secure Sockets Layer (SSL) protocol is an open protocol designed by Netscape, layered between the application protocol (e.g., HTTP) and TCP/IP
- SSL provides data encryption, server authentication, message integrity, and (optionally) client authentication for the TCP/IP connection
- SSL comes in 40-bit and 128-bit strengths (session key lengths)



Web-Based Security (SSL Handshake Protocol)



Web-Based Security (SSL Record Protocol)



Web-Based Security SSL-TLS Protocol

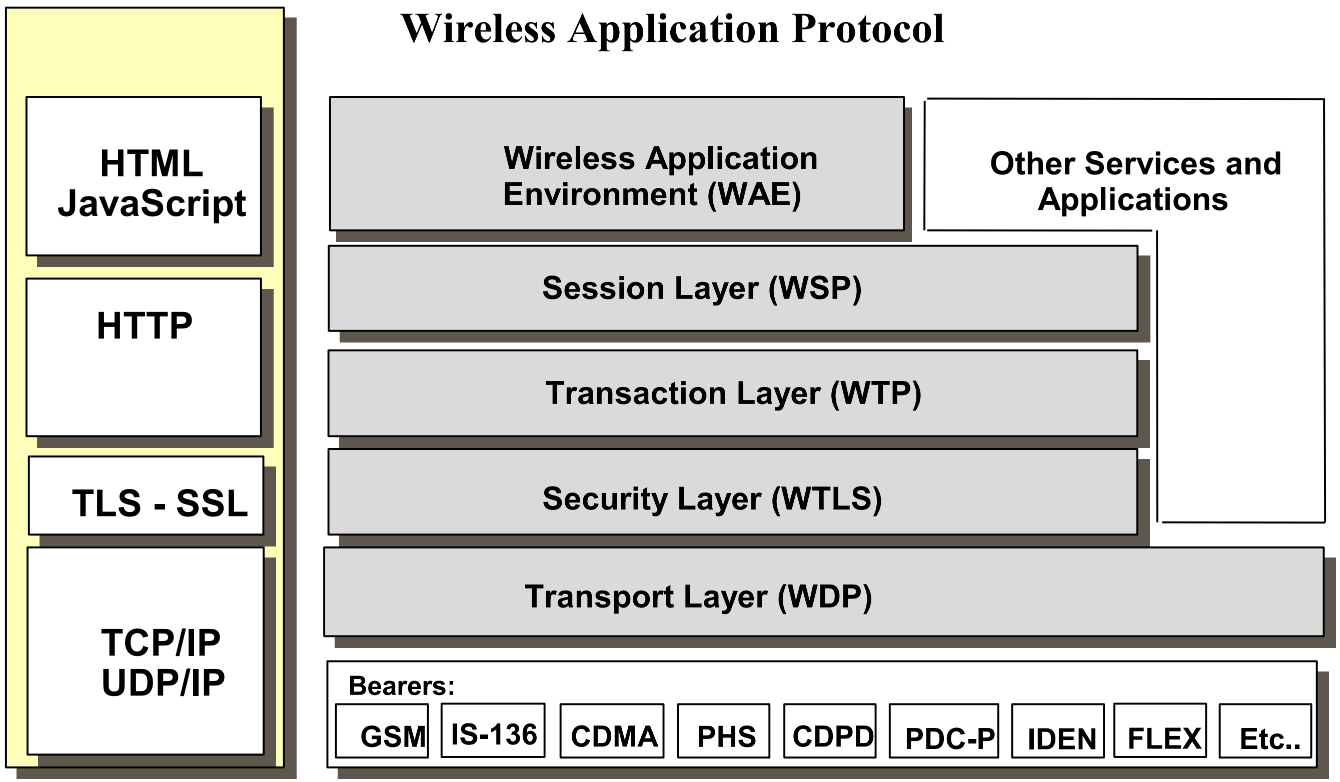
- Transport Layer Security (TLS) is an IETF standard version of SSL (version 3) that is backward compatible with SSLv3
- Differences between TLS 1.0 and SSLv3
  - *MAC Schemes:* Two differences in the actual algorithm and scope of the MAC calculation
  - *PN Function:* TLS uses a PN function to expand the small shared secret keys to protect against Hash function and MAC attacks
  - *Alert Codes:* TLS supports all alert codes defined in SSLv3 (except no_certificate), plus 12 additional codes, 9 of which are always fatal
  - *Cipher Suites:* TLS supports all SSLv3 key exchange techniques, and includes all symmetric encryption algorithms except Fortezza
  - *Client Certificate Types:* TLS does not include the Fortezza scheme or ephemeral DH types
  - Differences also exist in the *certificate-verify* and *finished* messages, *cryptographic computations*, and the *paddings*

Web-Based Security (WTLS Protocol)

- Wireless Application Protocol (WAP) defines set of standard components to enable secure communications between mobile terminals and network servers
  - Similar to Web programming model
  - Leverages existing Web tools, e.g., Web servers, XML tools
  - Micro browser in wireless terminal analogous to standard Web browser

Web-Based Security (WTLS Protocol)

- The Wireless TLS (WTLS) protocol operates at one of six layers of Wireless Application Protocol (WAP), to provide end-to-end wireless link security
- WTLS is based on TLS, optimized for use over narrow-band channels



Web-Based Security (WTLS Protocol)

- WTLS employs special adaptation mechanisms for mobile and wireless usage
- The following WTLS features highlight the main differences with TLS
  - WLTS record layer does not fragment information blocks
  - WTLS is optimized for low-bandwidth bearer networks
  - Long lived secure sessions
  - Optimized handshake procedures
  - Use of a single hash algorithm to secure data secrecy
  - Dynamic key refreshing
  - Simple data reliability scheme for operation over datagram bearers
  - Sequence number mode identifies scheme used to communicate sequence numbers

Overview of PGP(Pretty Good Privacy)

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

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	-

E-mail Security(PGP)

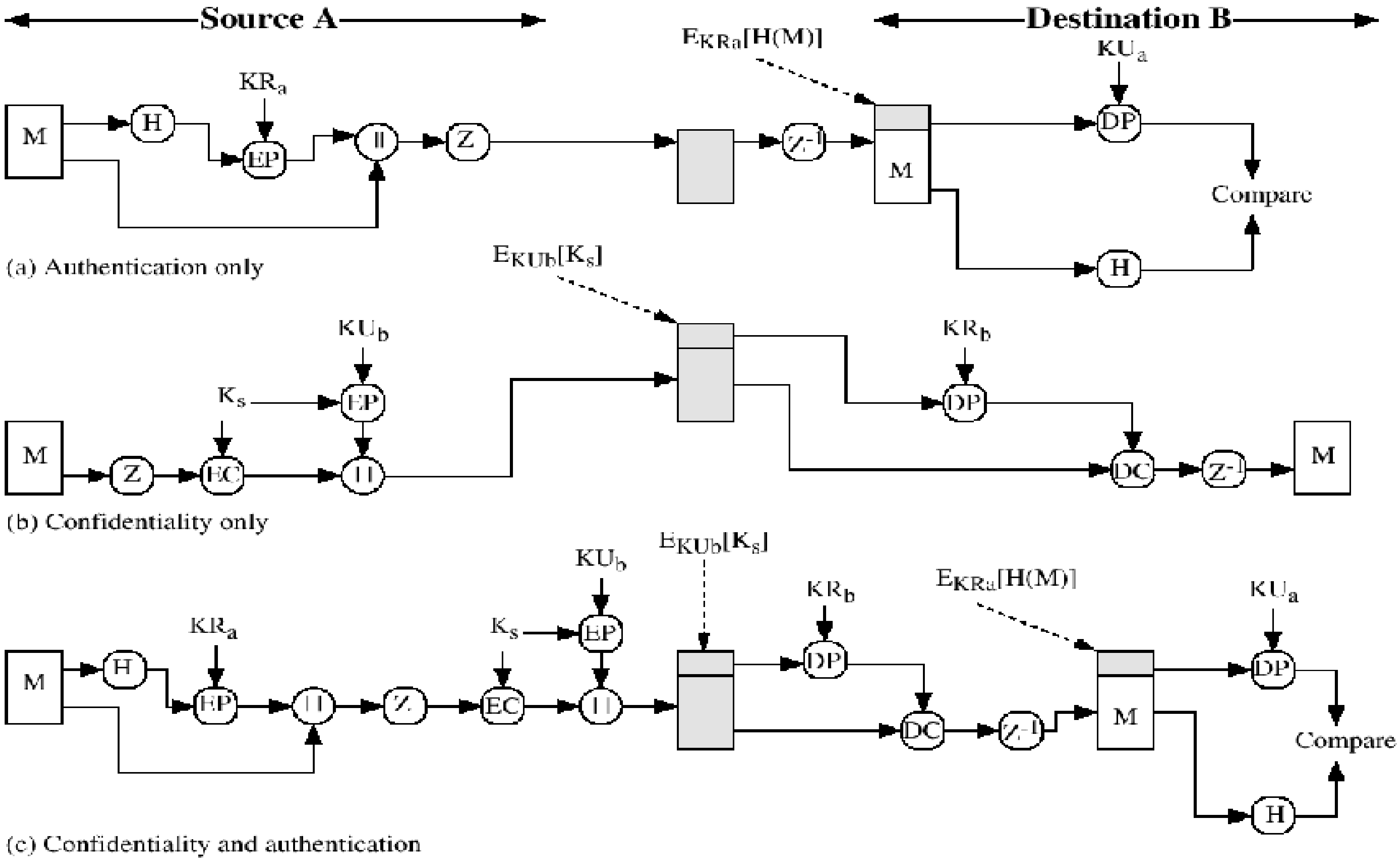


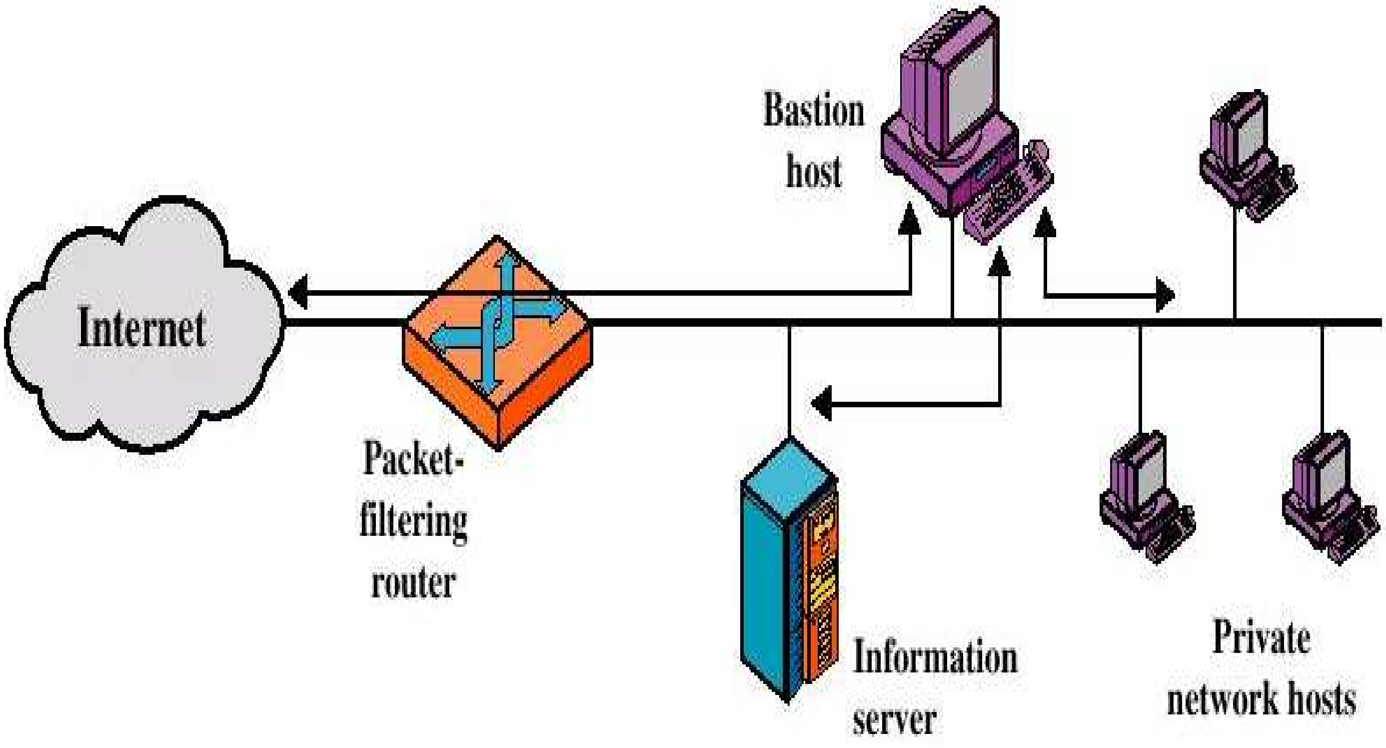
Figure 5.1 PGP Cryptographic Functions

Firewalls

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet
- Special router sits between a site and the rest of the network.
- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security police) will be allowed to pass

Firewall Configurations

- Screened host firewall system (single-homed bastion host)



Firewall Design Principles

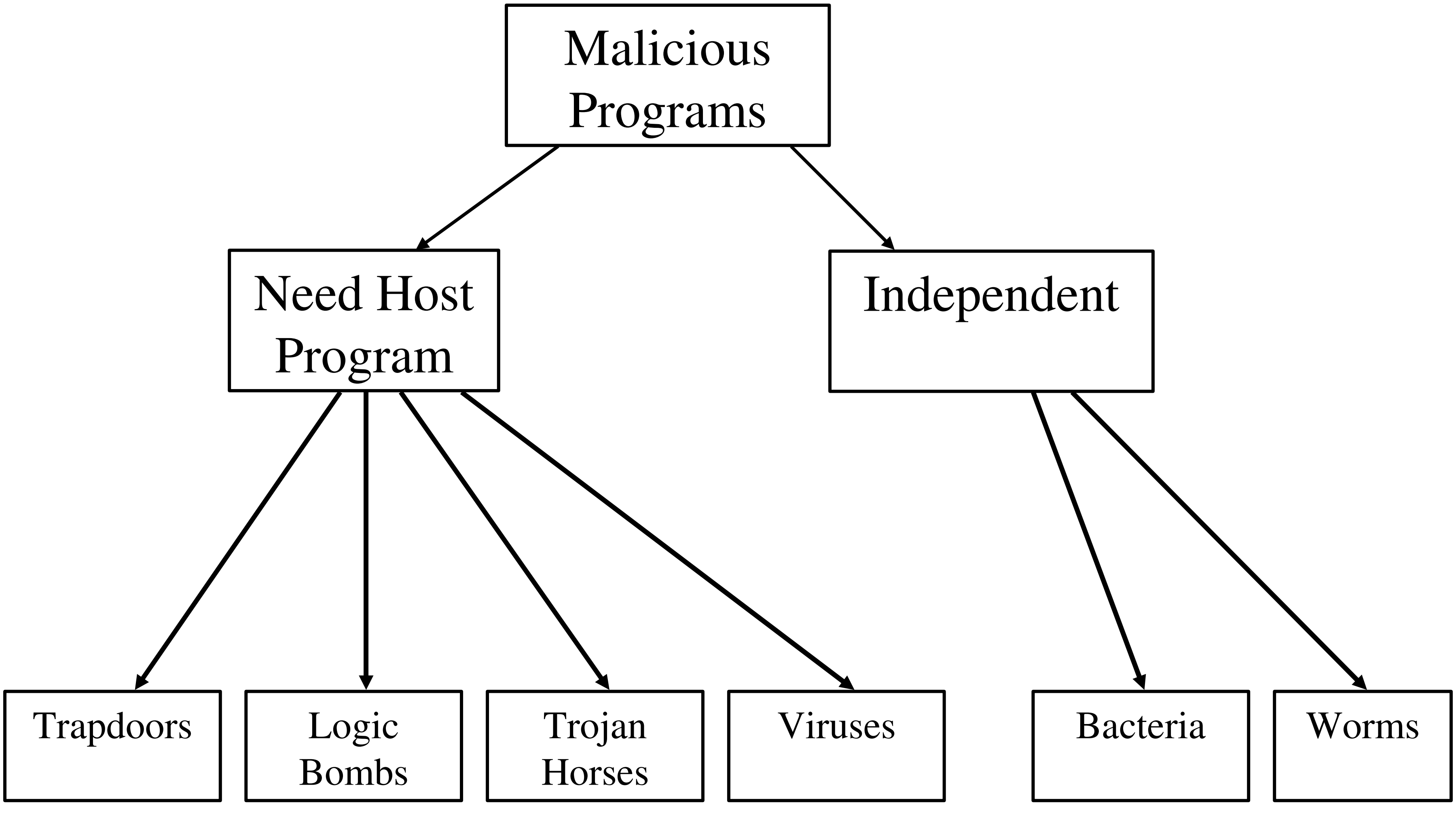
- Information systems undergo a steady evolution (from small LAN`s to Internet connectivity)
- Strong security features for all workstations and servers not established
- The firewall is inserted between the premises network and the Internet
- Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point

Viruses and ”Malicious Programs”

- Computer “Viruses” and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a “Worm”).

- Other “Malicious Programs” may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Taxanomy of Malicious Programs



Definitions

- Virus - code that copies itself into other programs.
- A "Bacteria" replicates until it fills all disk space, or CPU cycles.
- Payload - harmful things the malicious program does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.
- Easter Egg - extraneous code that does something "cool." A way for programmers to show that they control the product.

References

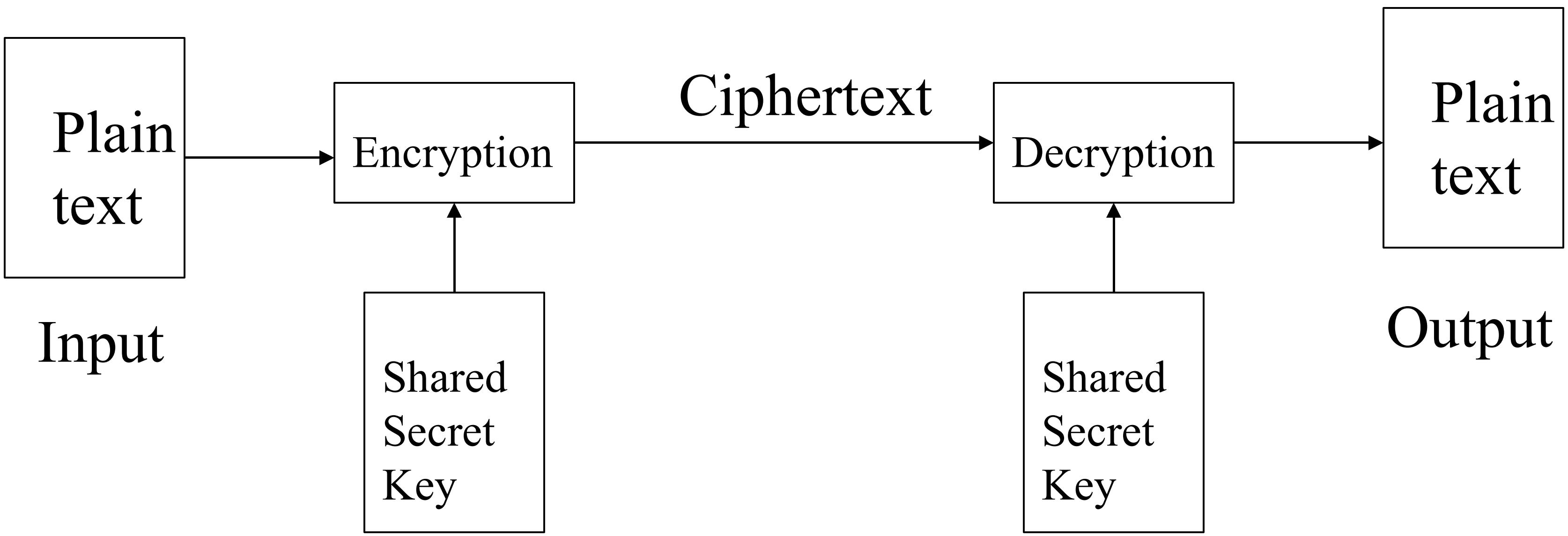
- Textbook
- Cryptography and Network Security, William Stallings, Prentice Hall
- Internet Security, Richard E. Smith, Addisson-Wesley
- http://www.WilliamStallings.com/
- IETF RFCs
- http://www.freeswan.org/ (Linux free IPSec implementation and useful document)

BEYOND is BACKUP SLIDES

Bluetooth Security Algorithms

- Security modes
- Authentication
- Encryption

Model of Encryption



Encryption

$$\text{Ciphertext}=\text{Plaintext} \oplus \text{Key}$$

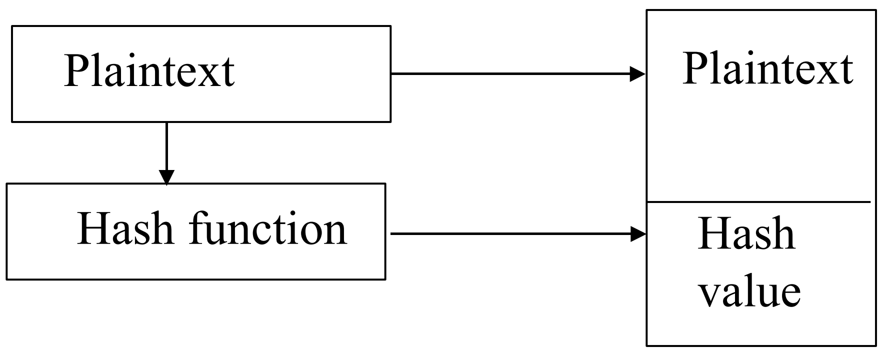
Decryption

$$\begin{aligned}\text{Plaintext}&=\text{Ciphertext} \oplus \text{Key}\\ &= (\text{Plaintext} \oplus \text{Key}) \oplus \text{Key}\\ &= \text{Plaintext} \oplus (\text{Key} \oplus \text{Key})\\ &= \text{Plaintext}\end{aligned}$$

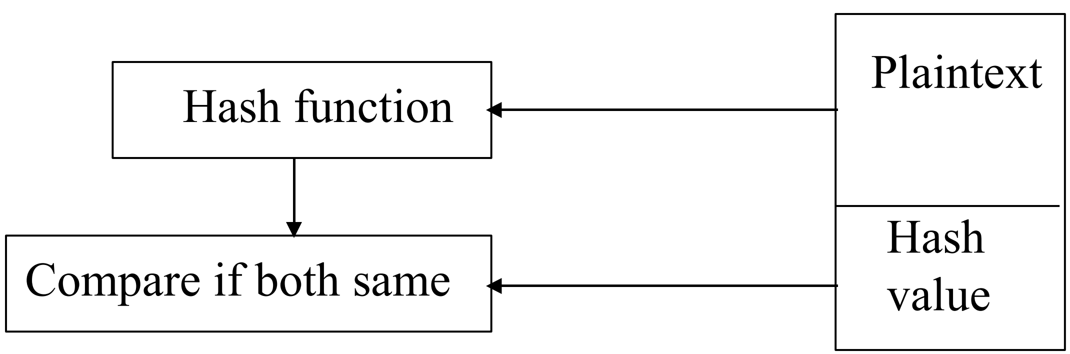
Hash Algorithms(one-way functions)

- Integrity checking, authentication of the message

```
Message => MD5 output (128bit)
1234567890 => 7c12772809c1c0c3deda6103b10fdfa1
1234567891 => eac9407dc999ae35ba5e6851e28d7c53
```



At source

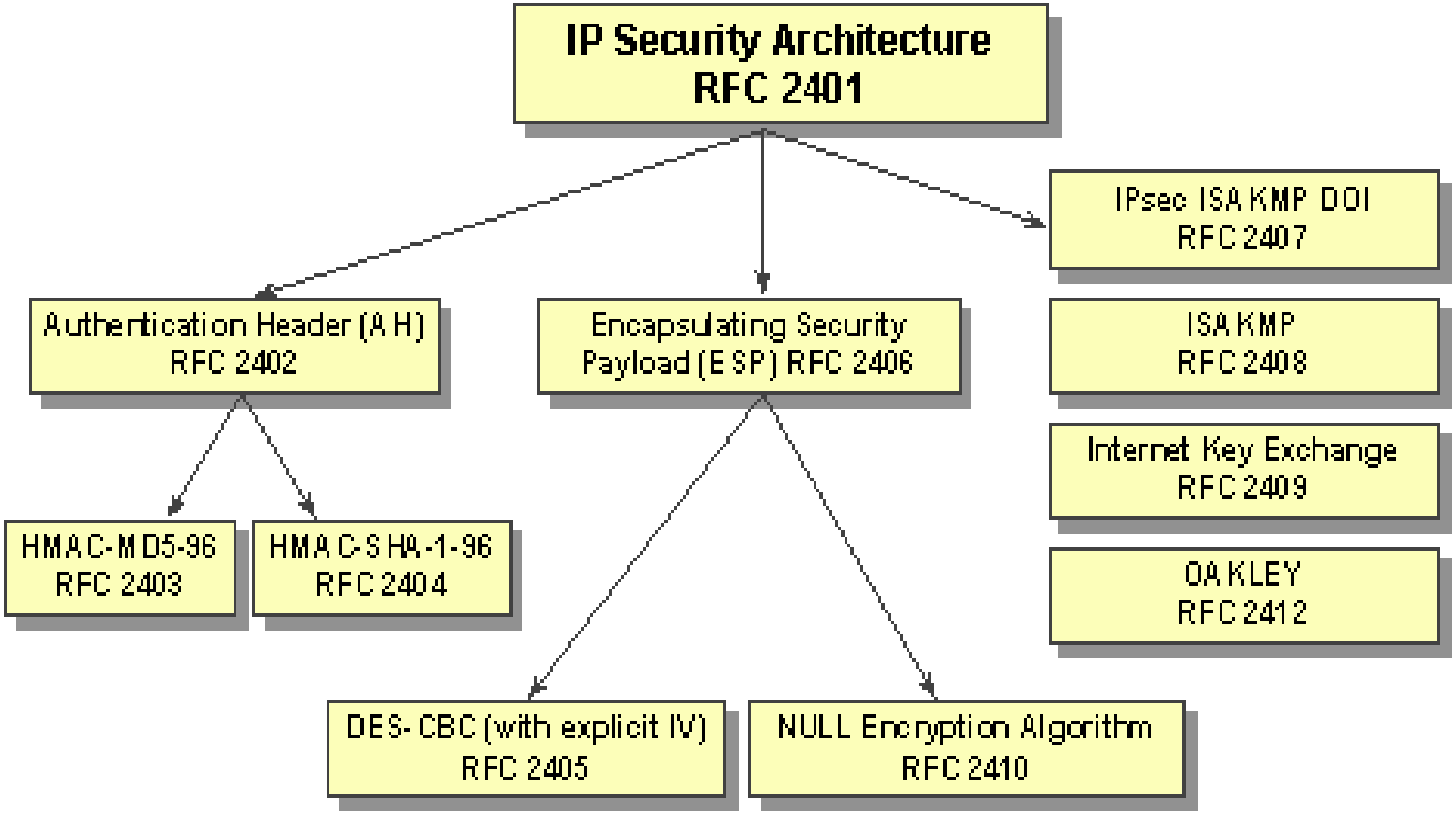


At destination

Comparison between Secret and Public Key algorithms

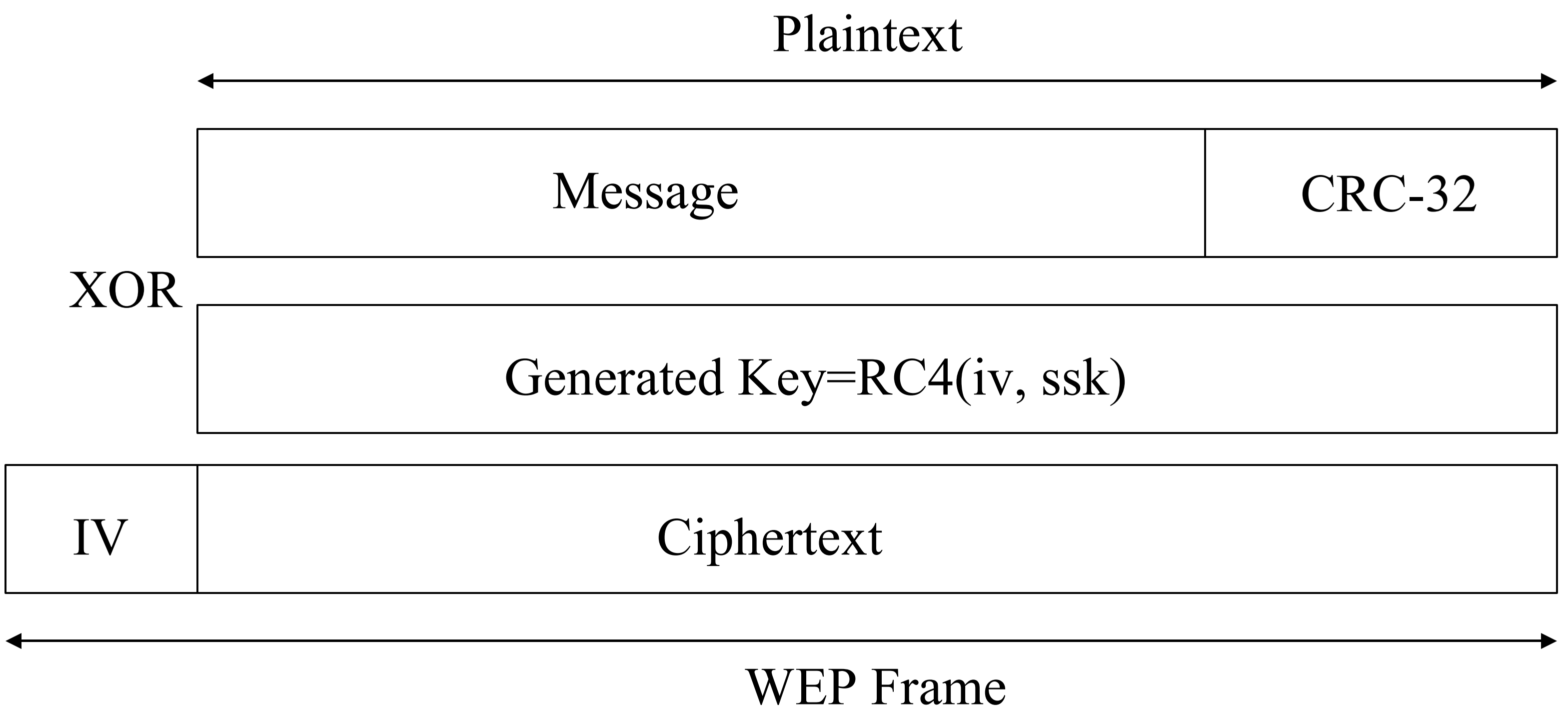
E-mail Security(PEM)

IP Security (IPSec RFC's

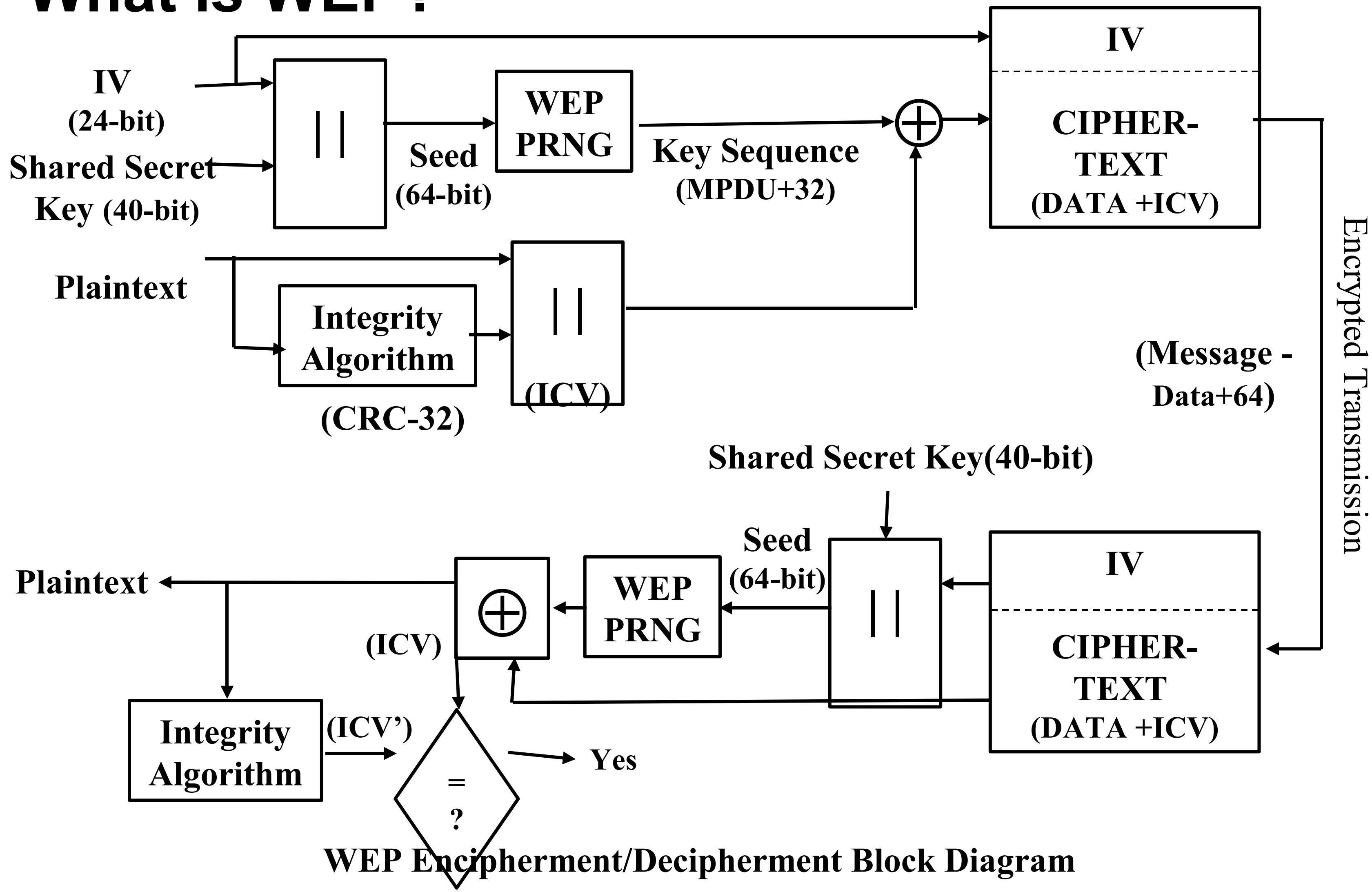


IEEE 802.11b Security, WEP

- Wired equivalent privacy(WEP)
  - -Designed to provide link layer security for IEEE 802.11networks



What is WEP?



WEP Encipherment/Decipherment Block Diagram

Security services provided with WEP

•Privacy: RC4 with 40-bit SSK (or 104-bit SSK in WEP2)

•Integrity: CRC-32

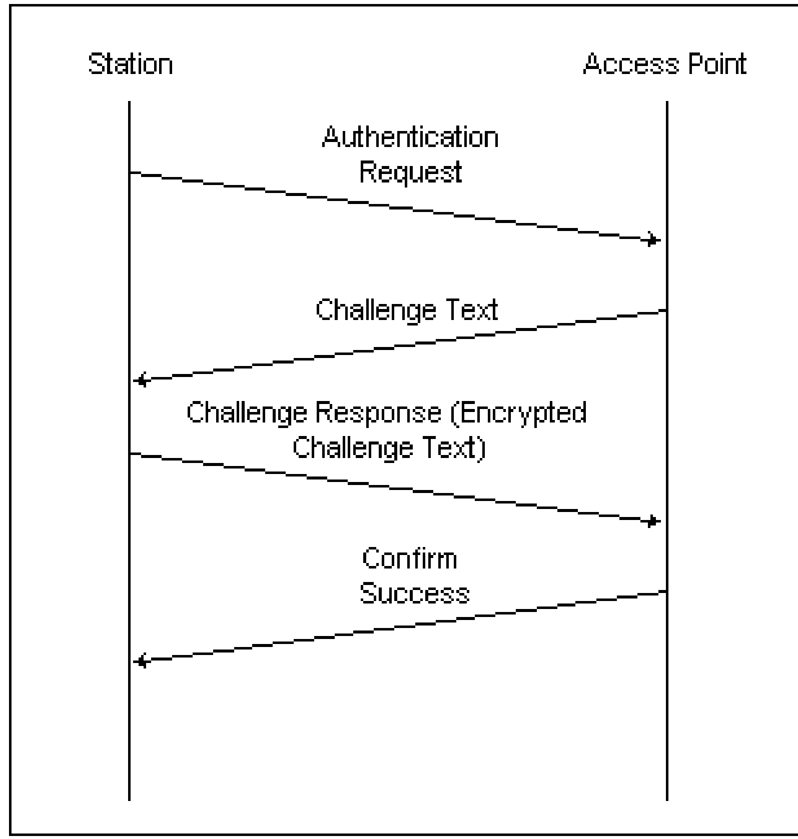
•Authentication:

Open system or SSK based

•Access Control: SSK based

•Non-repudiation: None

•Replay: None



SSK Authentication Mechanism

Weaknesses of existing WEP

- RC4 is stream cipher with 40-bit (or 104-bit) SSK
  - 40-bit is short, 104 bit long but not secure
  - 24-bit IV can be exhausted(at 16M packet)
  - Produces equivalent ciphertext from equivalent plaintext streams, IP packets have many common data streams
- CRC-32 is linear, CRC(X+Y)=CRC(X)+CRC(Y)
- No automatic key distribution mechanism, no scalability
- No user authentication

Too much faith in “**shared secret key**”

Proposed solutions

•Better encryption algorithm: Advanced Encryption Standard(AES), 128-bit block cipher

•Better integrity checking: AES in offset code book (OCB)

•Better authentication protocols

•Authentication services which includes the user as well: "**upper layer**" authentication in addition to open system and shared secret key

-Upper layer does not specify a specific authentication mechanism at MAC layer, but leaves the authentication services to upper layer, so that some of the following authentication schemes can initiated: 802.1X/EAPOL (Extended Authentication Protocol, RADIUS), Kerberos V, IAKERB

Upper layer authentication