Dept. of Computer Science and Engineering

Computer Networks and Security – 18CS52

MODULE – IV

Network Security

Module Content

- Overview of Network Security
- Elements of Network Security
- Classification of Network Attacks
- Overview of Security Methods
- Symmetric-Key Cryptography
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
- Public-Key Cryptography
  - RSA Algorithm
  - Diffie-Hellman Key-Exchange Protocol
- Authentication
  - Hash Function
  - Secure Hash Algorithm (SHA)
  - Digital Signatures
- Firewalls
- Packet Filtering
- Proxy Server .

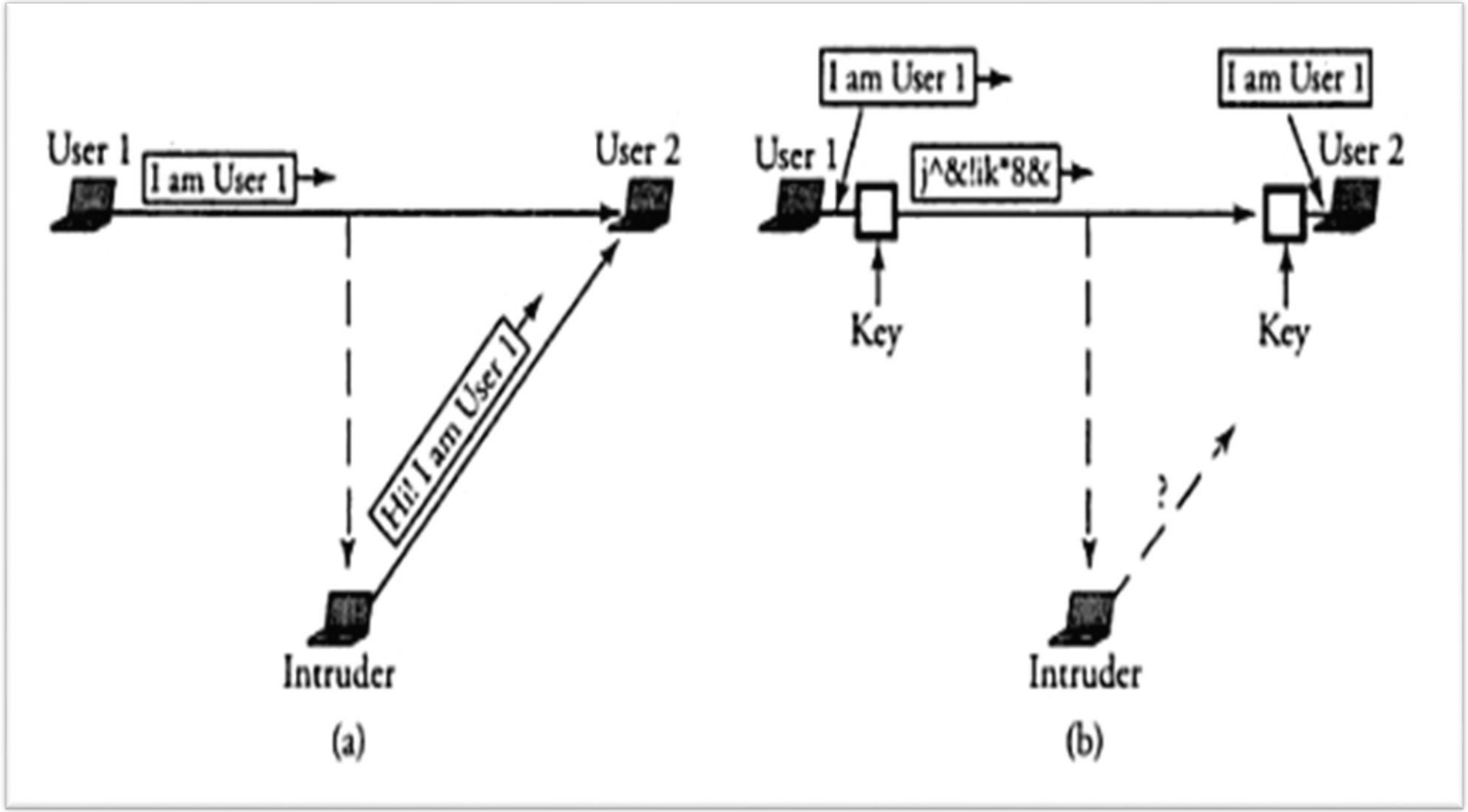
Overview of Network Security and its Elements

Network security is a top priority issue in data networks.

Elements of network security are

- ***Confidentiality :*** Information should be available only to those have rightful access to it.
- ***Authenticity and Integrity:*** The sender of the message and the message itself should be verified at the receiving point.

Figure *a. message content and sender identity falsified by intruder; b. A method of applied security*



Threats to Network Security

Internet infrastructure attacks are broadly classified into four categories.

1. DNS hacking
2. Routing table poisoning
3. Packet mistreatment
4. Denial of service

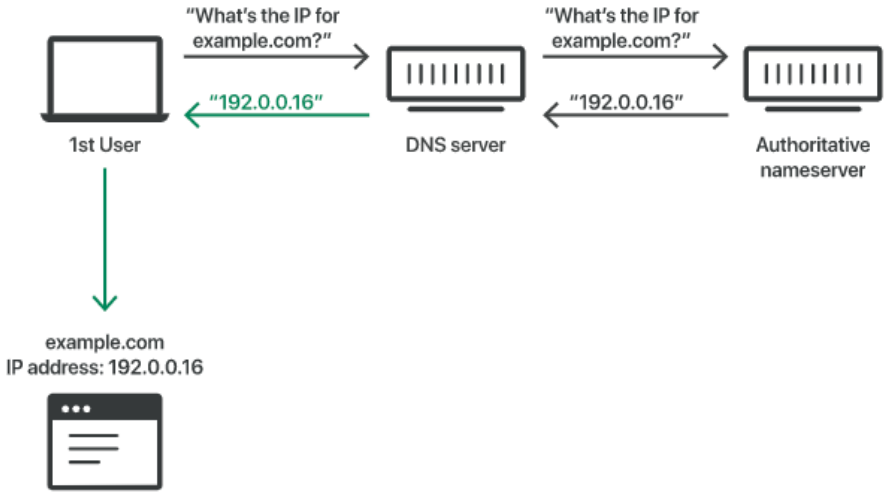
Among these threats , the first three attacks are related to network infrastructure; fourth one is related to end systems

DNS hacking attacks

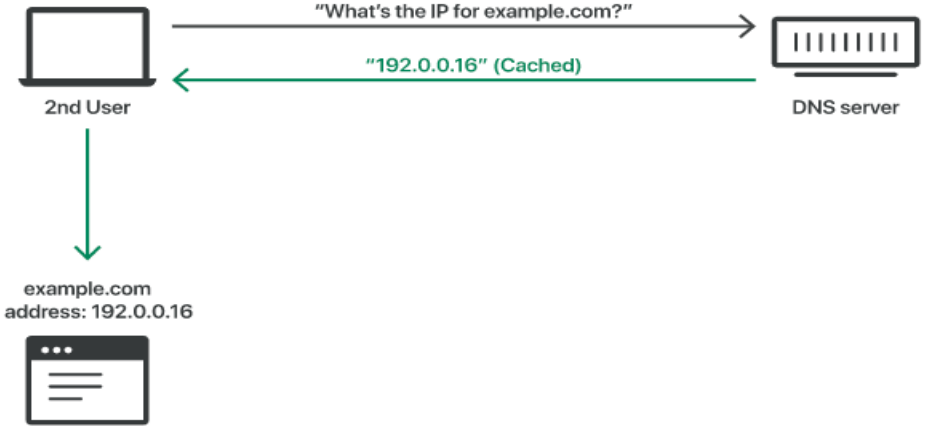
1. An information level attack
   - Cache Poisoning
2. Masquerading attack or middle-man attack
   - Attacker can stop or change the content of packet.
3. Information leakage attack
   - Identifies unused IP address to attack
4. Domain high-jacking attack
   - Forced to enter attackers web site

Cache Poisoning

DNS Uncached Response:

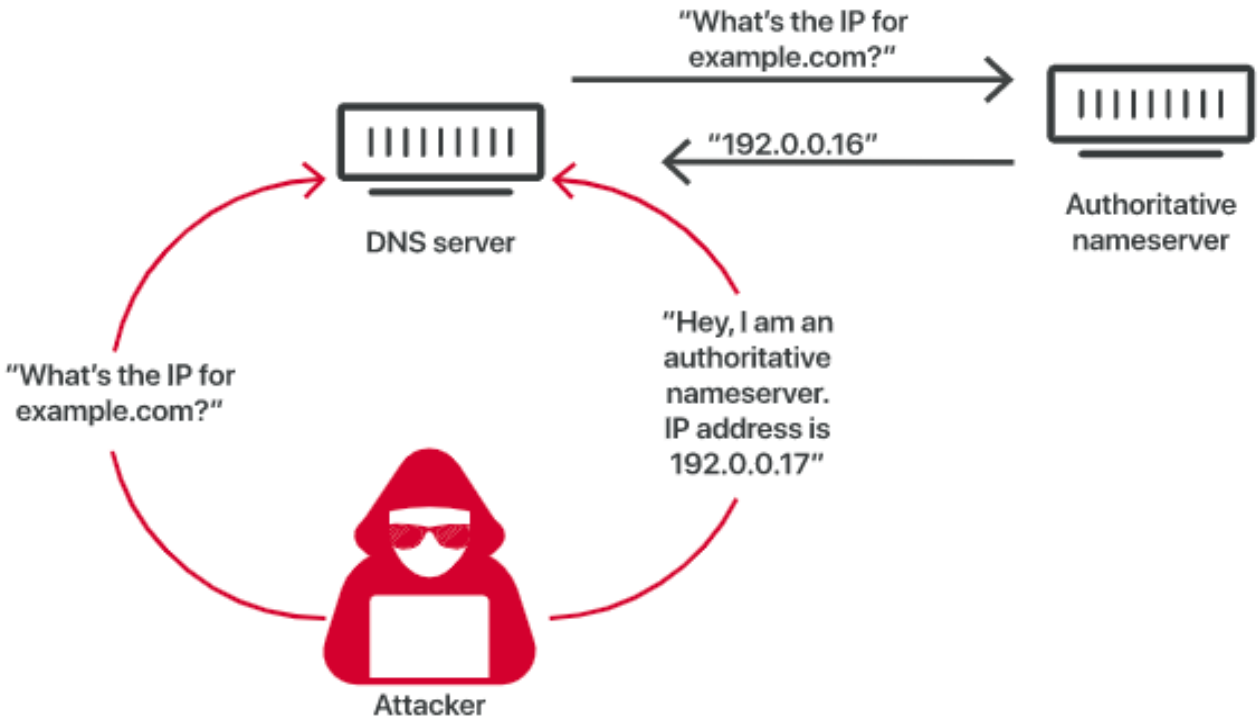


DNS Cached Response:

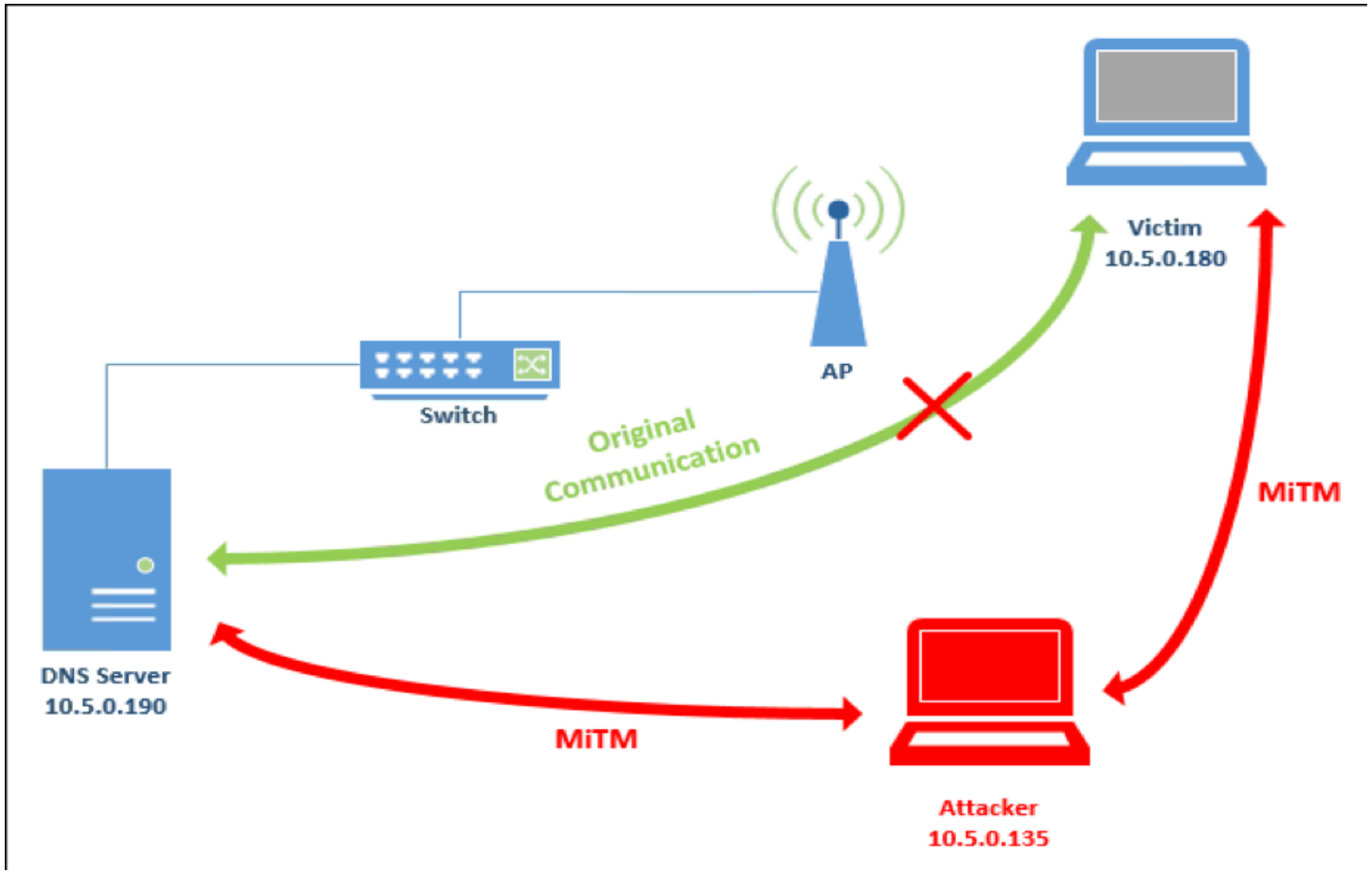


Cache Poisoning

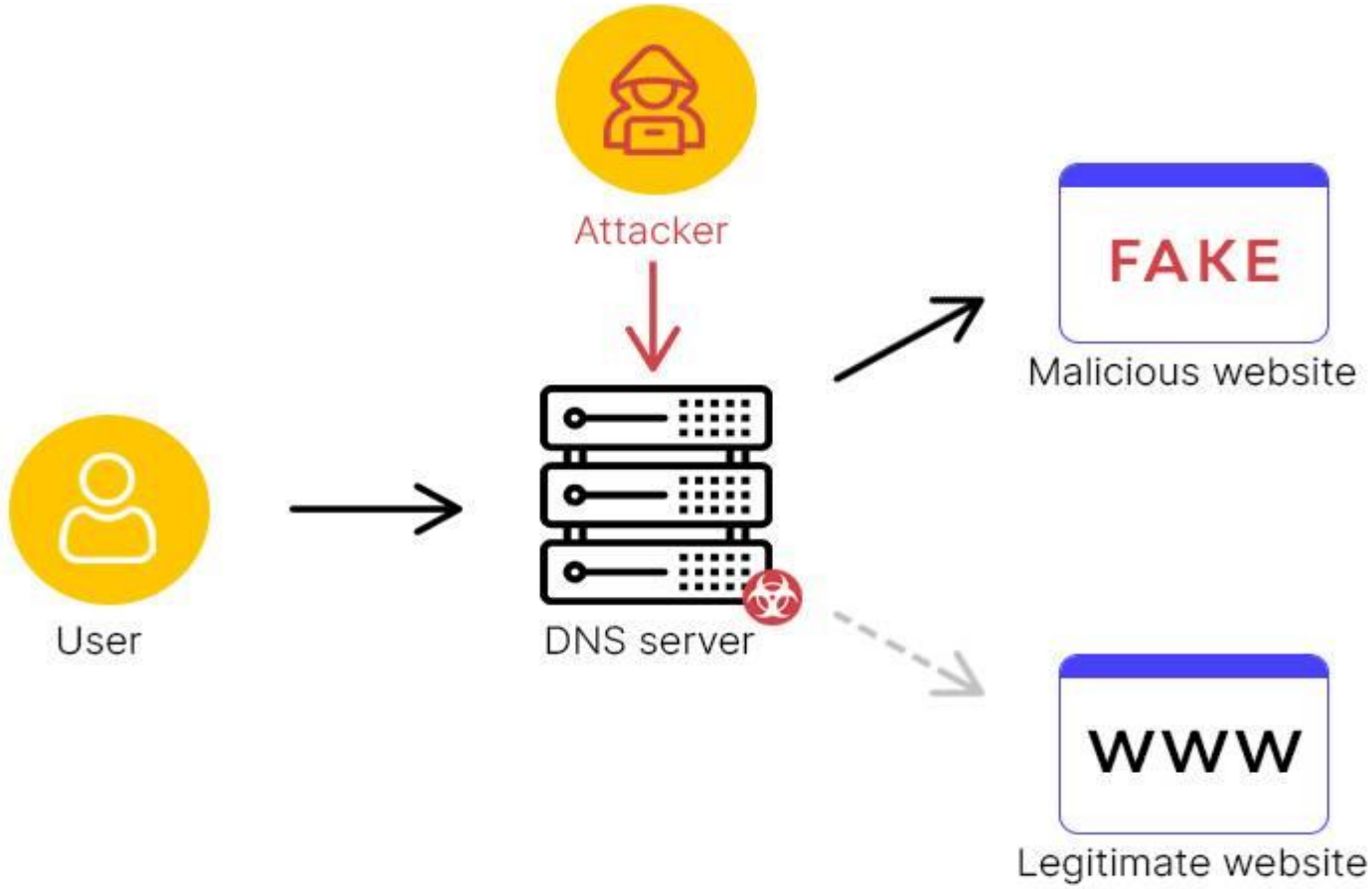
DNS Cache Poisoning Process:



Masquerading attack



Domain high-jacking attack



Routing table poisoning attacks

It is the undesired modification of routing tables. This can be done through maliciously modifying the routing information update packets sent by routers.

Any false entry in a routing table could lead to significant consequences, such as congestion, overwhelmed host, looping, illegal access to data and network partition.

Two types of routing table poisoning attacks are

1. The Link attack and
2. The router attack

Routing table poisoning attacks

1. The Link attack

- Occurs when a hacker gets access to a link and there by intercepts, interrupts, or modifies routing messages on packet

2. The router attack

- It may add a non existing link to a routing table, delete an existing link, or even change the cost of a link.
- This attack may cause a router to simply ignore the updates sent by its neighbors, leading to serious impact on the operability of the network traffic flow

Packet mistreatment attacks

It can occur during any data transmission.

A hacker may capture certain data packets and mistreat them.

Example of packet-mistreatment attack

- Interruption
- Modification
- Replication
- Ping of death
- Malicious misrouting of packets

Denial-of-Service (DoS) attacks

- This is a type of security breach that prohibits a user from accessing normally provided services.
- This can cost the target person a large amount of time and money.
- This affects the destination rather than a data-packet or router.
- They take important servers out of action for few hours, thereby denying service to all users.
- DoS attacks are of two types
  1. Single source
  2. Distributed

Module Content

- Overview of Network Security
- Elements of Network Security
- Classification of Network Attacks
- Overview of Security Methods
- Symmetric-Key Cryptography
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
- Public-Key Cryptography
  - RSA Algorithm
  - Diffie-Hellman Key-Exchange Protocol
- Authentication
  - Hash Function
  - Secure Hash Algorithm (SHA)
  - Digital Signatures
- Firewalls
- Packet Filtering
- Proxy Server .

Overview of Security Methods

Common solutions that can protect computer communication networks from attacks are classified as:

- Cryptographic techniques
- Authentication Techniques(Verification)

Cryptographic techniques

Cryptography is the process of transforming a piece of information or message shared by two parties into some sort of code.

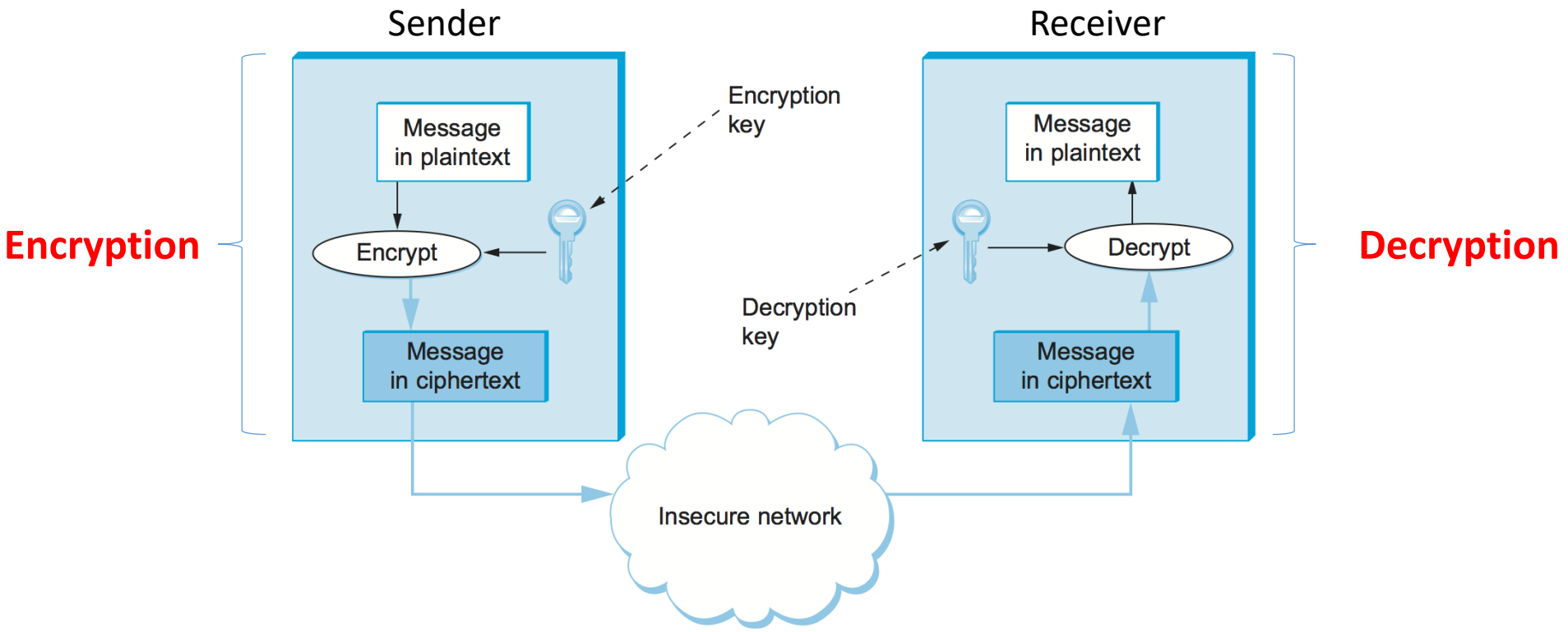
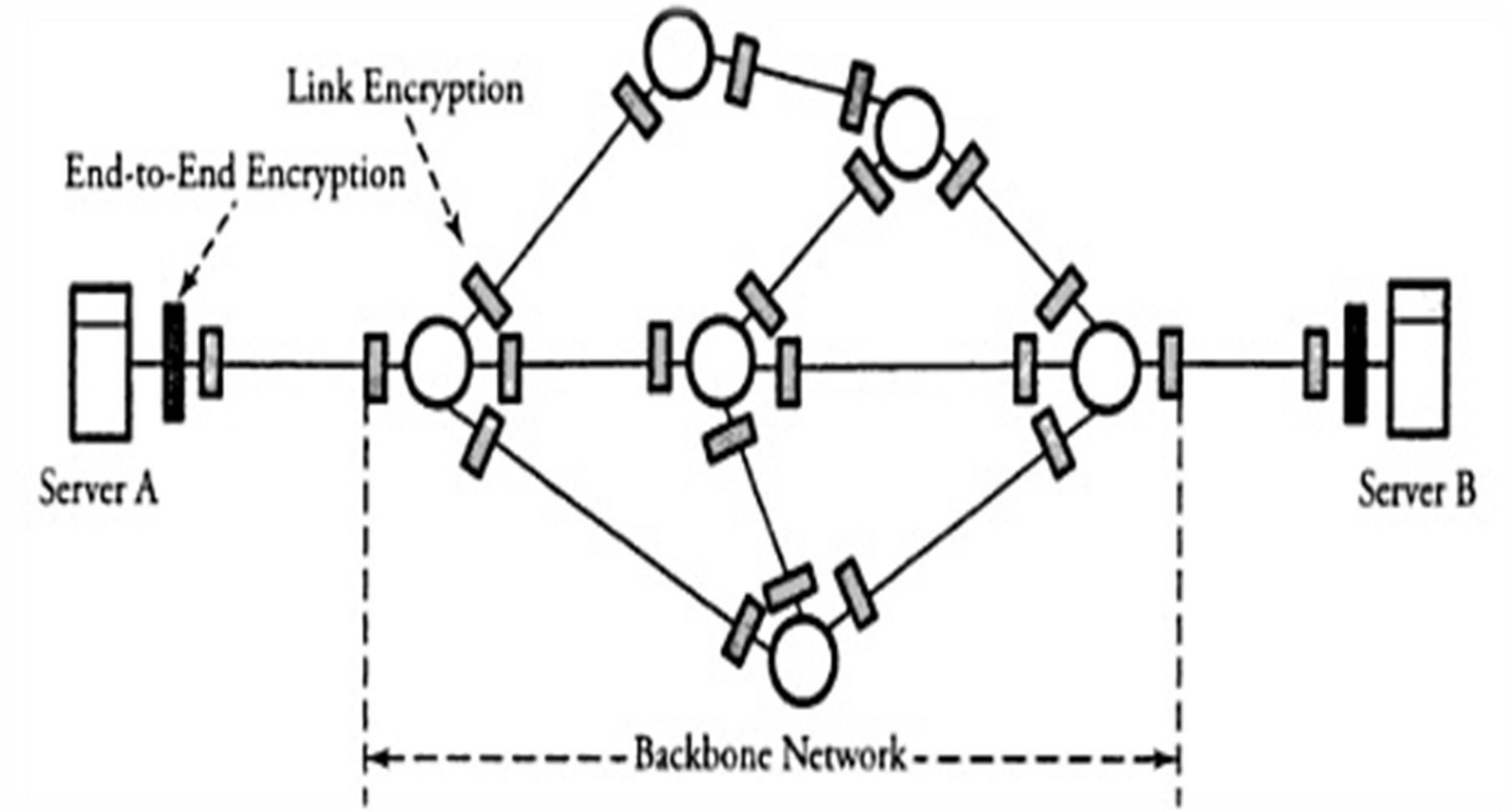
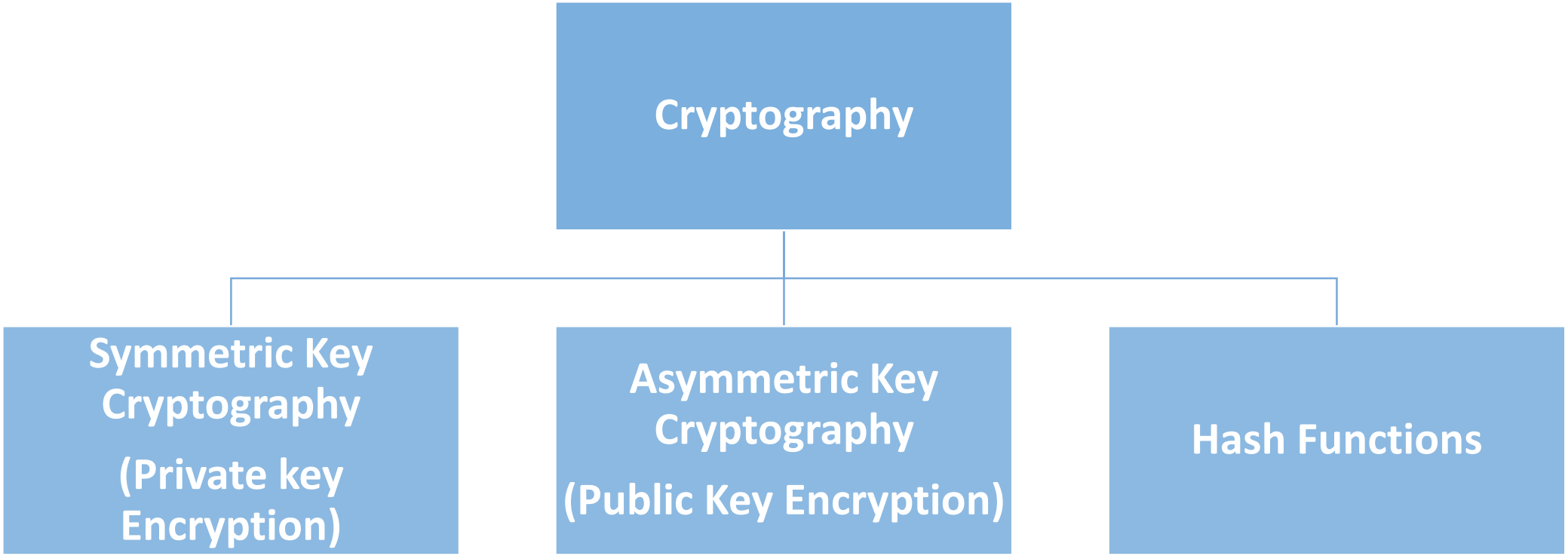


Figure *overview of encryption points in a communication network*

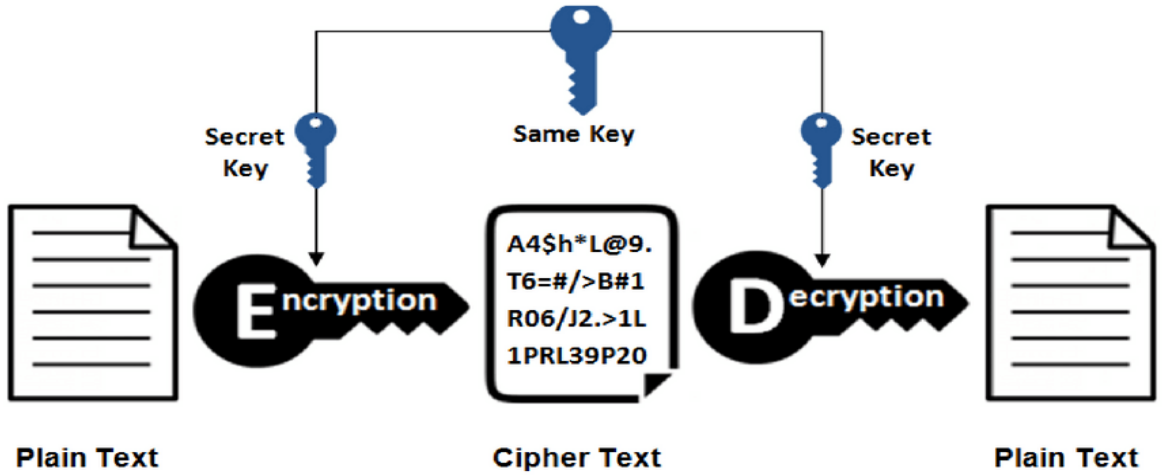


Types Of Cryptography



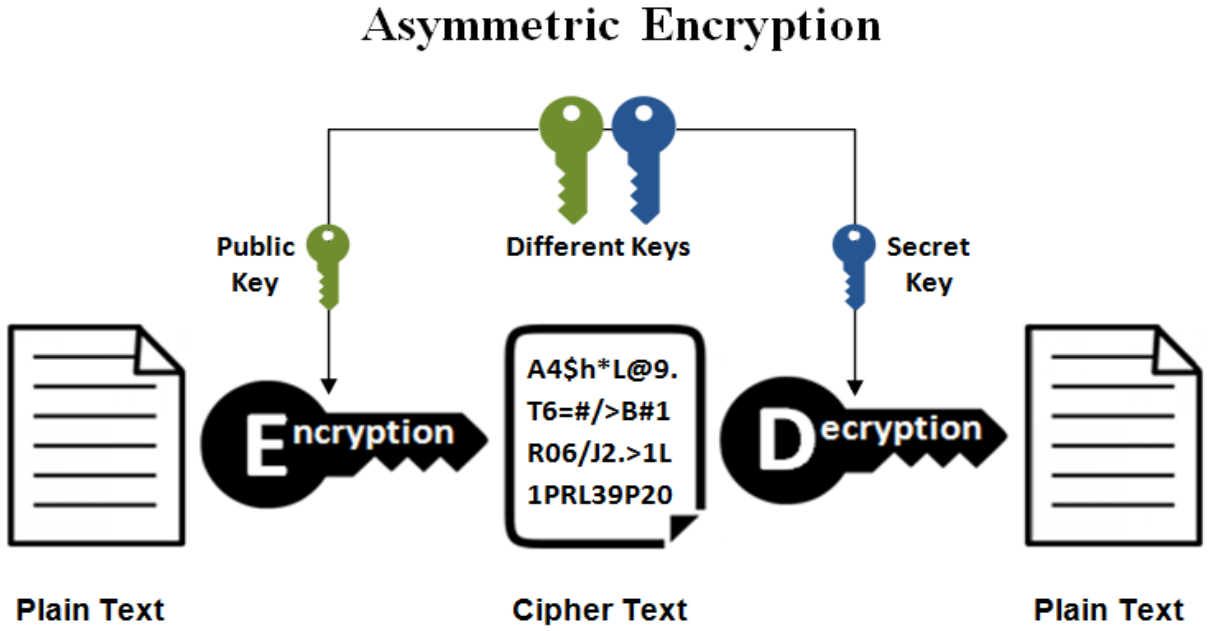
Symmetric Key Cryptography

- It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.
- Ex: DES, AES



Asymmetric Key Cryptography

- Under this system a pair of keys is used to encrypt and decrypt information.
- A public key is used for encryption and a private key is used for decryption.
- Public key and Private Key are different.
- Ex: RSA Algorithm



Cryptographic techniques

Summary:

Secret key encryption: both sender and receiver conventionally use the same key for an encryption process

Public key encryption: sender and receiver each use a different key.

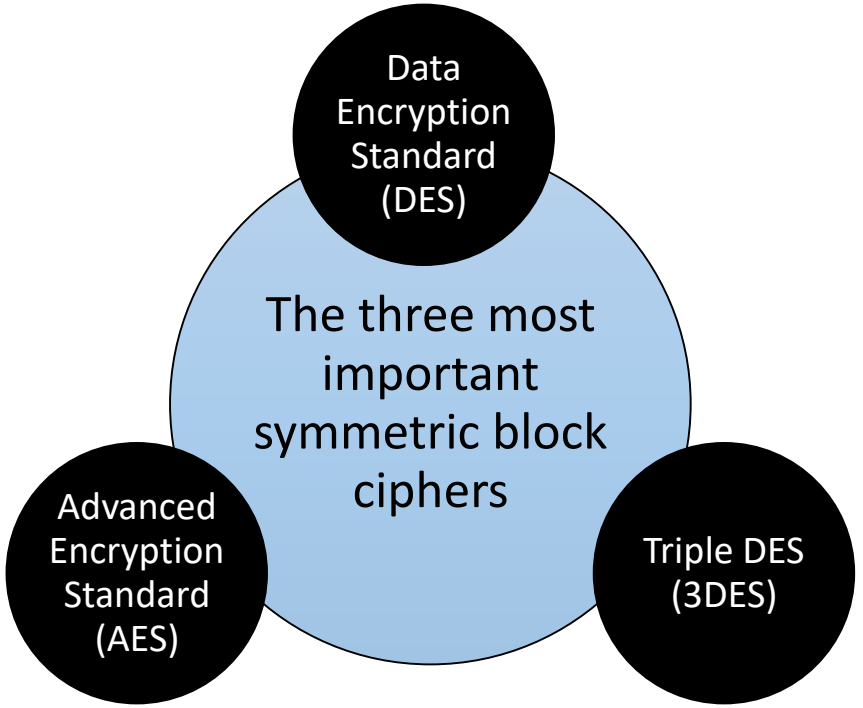
It is more powerful than the secret-key system and provides better security and message privacy
Drawback is encryption speed is less, more complex computationally and may not be practically in many cases.

Authentication techniques

- Verifying the Authenticity of the message and the sender of the message
- Two categories of authentication techniques
  - Authentication with message digest
  - Authentication with digital signature

Secret key Encryption protocols

These sometimes known as symmetric encryption, or single-key encryption protocols, or conventional encryption models.



Data Encryption Standard (DES)

- The DES algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team.
- Adopted by the National Institute of Standards and Technology (NIST).
- DES is based on the **Feistel block cipher** called LUCIFER, developed in 1971 by IBM cryptography researcher Horst Feistel.
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA)

DES algorithm

- Description of the algorithm:
  - Plaintext is 64 bits in length
  - Key is 56 bits in length
  - There are 16 rounds of processing
  - Process of decryption is essentially the same as the encryption process

DES Algorithm

1. Initialize. Before round 1 begins, all 64 bits of the message and all 56 bits of the secret key are separately permuted (shuffled).
2. Each incoming 64-bit message is broken into two 32-bit halves denoted by L_i and R_i respectively.
3. The 56 bits of the key are also broken into two 28-halves, and each half is rotated one or two bit positions, depending on the round.
4. All 56 bits of the key are permuted, producing version k_i of the key on round i.
5. L_i and R_i are determined by

   $L_i = R_{i-1}$ and

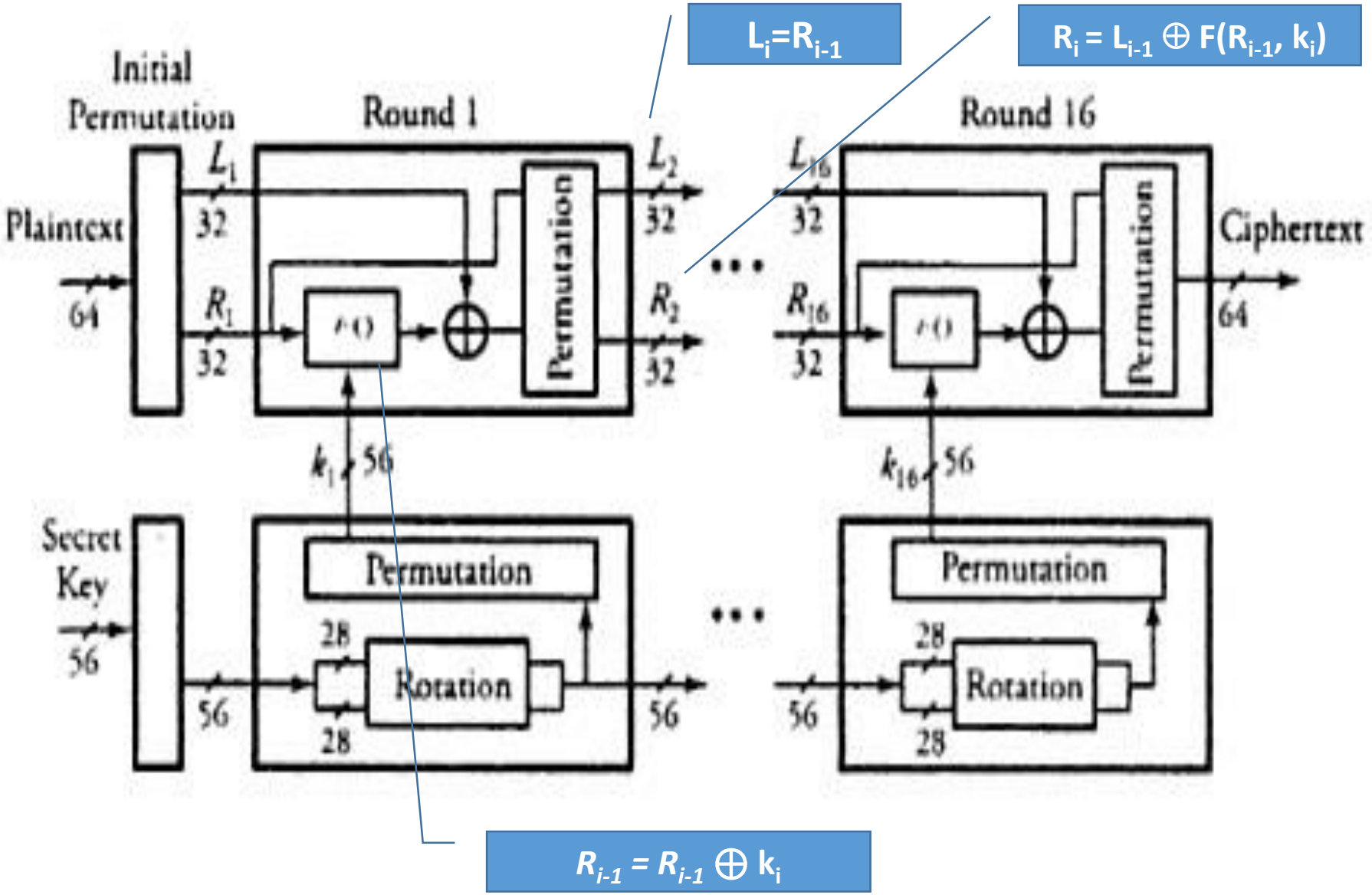
   $R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$
6. All 64 bits of a message are permuted.

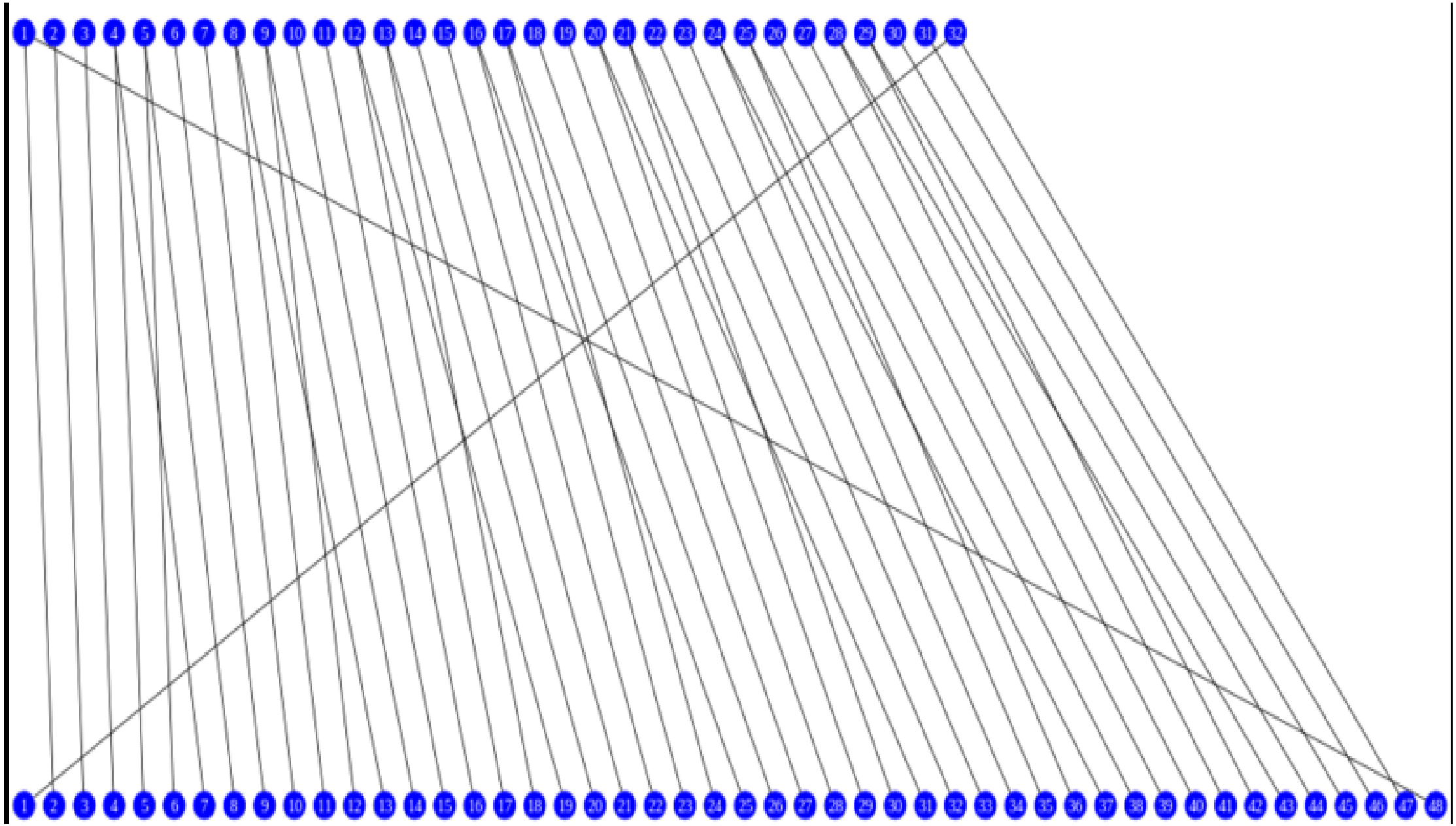
DES Algorithm

- The operation of function *F()* at any round '*i*' of DES is as follows:
  1. *Out of 56 bits of k_i , function F() chooses 48 bits.*
  2. *The 32-bit R_{i-1} is expanded to 48 bits*
  3. *The function F() also partitions 48 bits of k_i into 8 6-bit chunks*
  4. *then we have*

$$R_{i-1} = R_{i-1} \oplus k_i$$

Figure *The Data Encryption Standard*

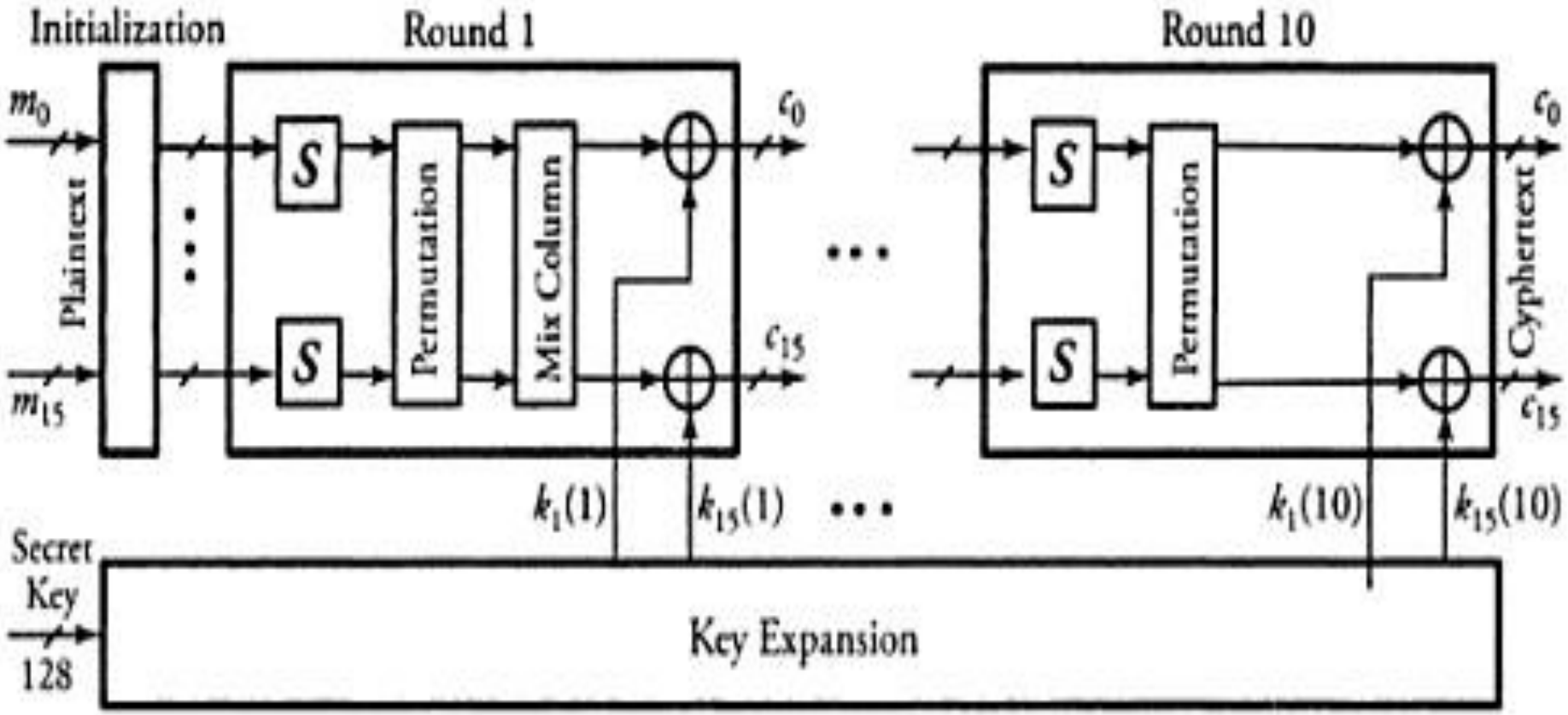


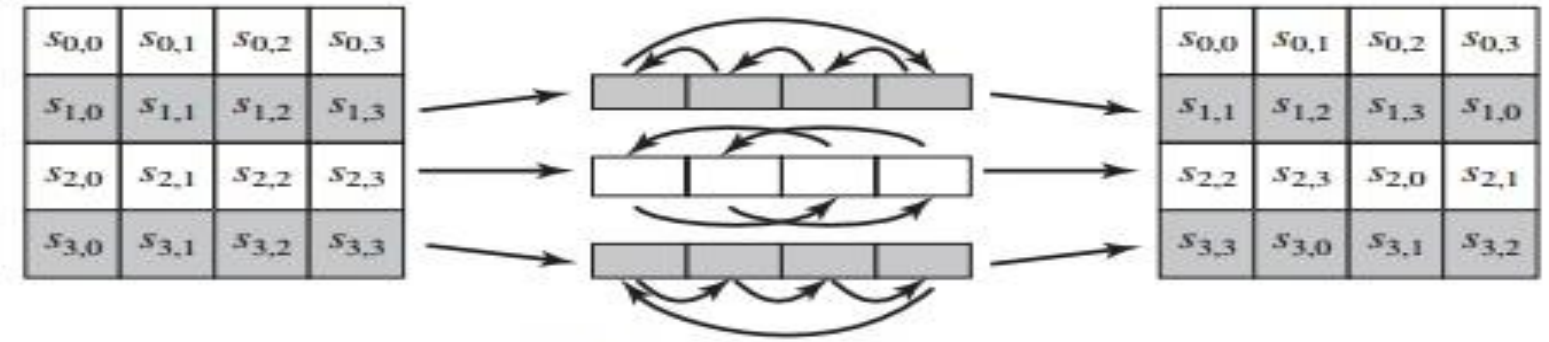


Advanced encryption standard (AES)

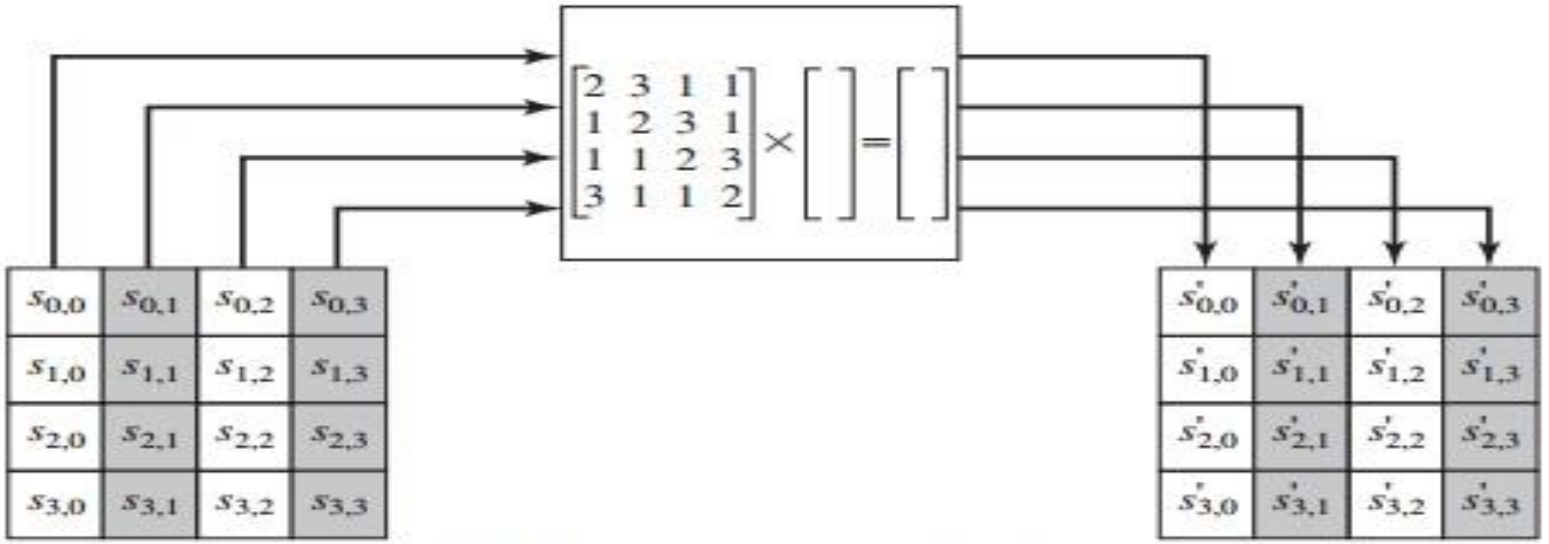
- Provides better security than DES.
- Supports 128-bit symmetric block message
- Uses 128-, 192-, 256-bit keys
- Number of rounds in AES is variable from 10, 12 and 14.
- A round includes:
  - Substitution
  - Permutation
  - Mix Column(skipped in last round)
  - Add round key

Figure *overview of Advanced Encryption Standard*





(a) Shift row transformation



(b) Mix column transformation

Figure 5.7 AES Row and Column Operations

Module Content

- Overview of Network Security
- Elements of Network Security
- Classification of Network Attacks
- Overview of Security Methods
- Symmetric-Key Cryptography
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
- Public-Key Cryptography
  - **RSA Algorithm**
  - **Diffie-Hellman Key-Exchange Protocol**
- Authentication
  - Hash Function
  - Secure Hash Algorithm (SHA)
  - Digital Signatures
- Firewalls
- Packet Filtering
- Proxy Server .

RSA Algorithm: Rivest–Shamir–Adleman

- It is an Asymmetric key cryptosystem
- It uses two Keys
  - Public Key for Encryption by Sender
  - Private Key for Decryption by Receiver
- It has three major steps
  1. Key Generation
  2. Encryption
  3. Decryption

Key Generation

1. Choose two large prime numbers →p, q
   Calculate n→n=p×q and
   ϕ(n) → ϕ(n) = (p-1) × (q-1)
2. Find e. Select encryption key ‘e’ such that e and ϕ(n) are relatively prime and
   1<e< ϕ(n)
3. Find d. Calculate decryption key ‘d’:
   $e \times d \bmod \phi(n) = 1$
4. At this point p and q can be discarded
5. The **Public Key = (e, n)**
6. The **Private Key = (d, n)**

p= 3 and q= 11

n = 3 × 11 → 33 ,

ϕ(n) = 2 × 10 → 20

e= 7

Find d

$7 \times d \bmod 20 = 1$

d=3

Public Key = (7,33)

Private Key = (3,33)

Public Key = (e, n) → (7,33)
Private Key = (d, n)→ (3,33)

Encryption

$$Ciphertext(C) = M^e \bmod n$$

Message 'M' = 9

$Ciphertext(C) = 9^7 \bmod 33$

$= 15$

Decryption

$$Message\ (M) = C^d \bmod n$$

$Message\ (M) = 15^3 \bmod 33$

$= 9$

Assignment Problems

1. Perform encryption and decryption using the RSA algorithm for the following: find y and perform encryption and decryption

a. $a = 3; b = 11, x = 7; M\ 5$

b. $a = 5; b = 11, x = 3; M\ 9$

c. $a = 7; b = 11, x = 17; M\ 8$

d. $a = 11; b = 13, x = 11; M\ 7$

e. $a = 17; b = 31, x = 7; M\ 2$

Diffie-Hellman Key Exchange Algorithm

- Diffie-Hellman key exchange is a simple public key algorithm.
- The protocol enables 2 users to establish a secret key using a public key scheme based on discrete algorithms.
- The protocol is secure only if the authenticity of the 2 participants can be established.
- Normally used for Virtual Private Network(VPN).

Algorithm

g is primitive root of *a*
If $g^1 \bmod a, g^2 \bmod a \ldots\ldots g^{a-1} \bmod a \Rightarrow \{1,2,\ldots.a-1\}$

STEPS	ALICE	BOB
1	Alice and Bob agree on a prime number *a* and *g*(primitive root of *a and g<a*) ahead of time.	
2	Private Key Selected = x_1	Private Key Selected = x_2
3	Calculate Public Key $y_1 = g^{x1} \bmod a$	Calculate Public Key $y_2 = g^{x2} \bmod a$
4	Exchange the value of y_1 and y_2	
5	Calculate $k_1 = y_2^{x1} \bmod a$	Calculate $k_2 = y_1^{x2} \bmod a$

The value of k_1 and k_2 are equal. That key will be used as Symmetric Key for cryptography process.

Example

2^1 mod 11	2^2 mod 11	2^3 mod 11	2^4 mod 11	2^5 mod 11	2^6 mod 11	2^7 mod 11	2^8 mod 11	2^9 mod 11	2^{10} mod 11
2	4	8	5	10	9	7	3	6	1

ALICE	BOB
Alice and Bob agree on a prime number $a=11$ and $g=2$ (primitive root of a) ahead of time.	
Private Key Selected $x_1 = 8$	Private Key Selected $x_2 = 4$
Calculate Public Key $y_1 = g^{x1} \bmod a$ $\Rightarrow 2^8 \bmod 11 = 3$	Calculate Public Key $y_2 = g^{x2} \bmod a$ $\Rightarrow 2^4 \bmod 11 = 5$
Exchange the value of y_1 and y_2	
Calculate $k_1 = y_2^{x1} \bmod a$ $\Rightarrow 5^8 \bmod 11 = 4$	Calculate $k_2 = y_1^{x2} \bmod a$ $\Rightarrow 3^4 \bmod 11 = 4$

Module Content

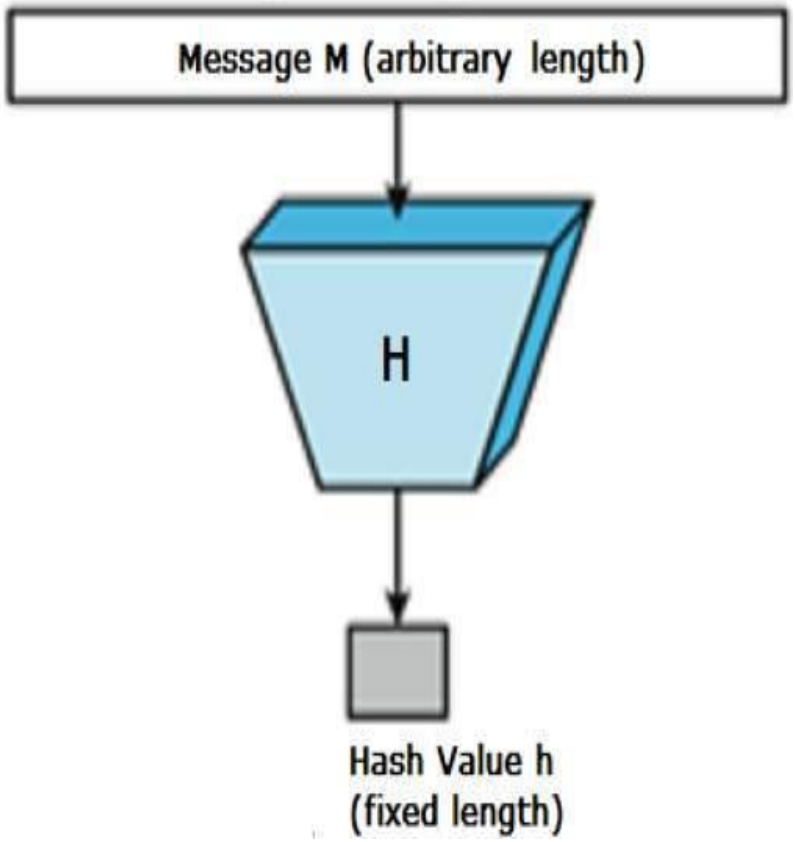
- Overview of Network Security
- Elements of Network Security
- Classification of Network Attacks
- Overview of Security Methods
- Symmetric-Key Cryptography
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
- Public-Key Cryptography
  - **RSA Algorithm**
  - **Diffie-Hellman Key-Exchange Protocol**
- Authentication
  - Hash Function
  - Secure Hash Algorithm (SHA)
  - Digital Signatures
- Firewalls
- Packet Filtering
- Proxy Server

Authentication

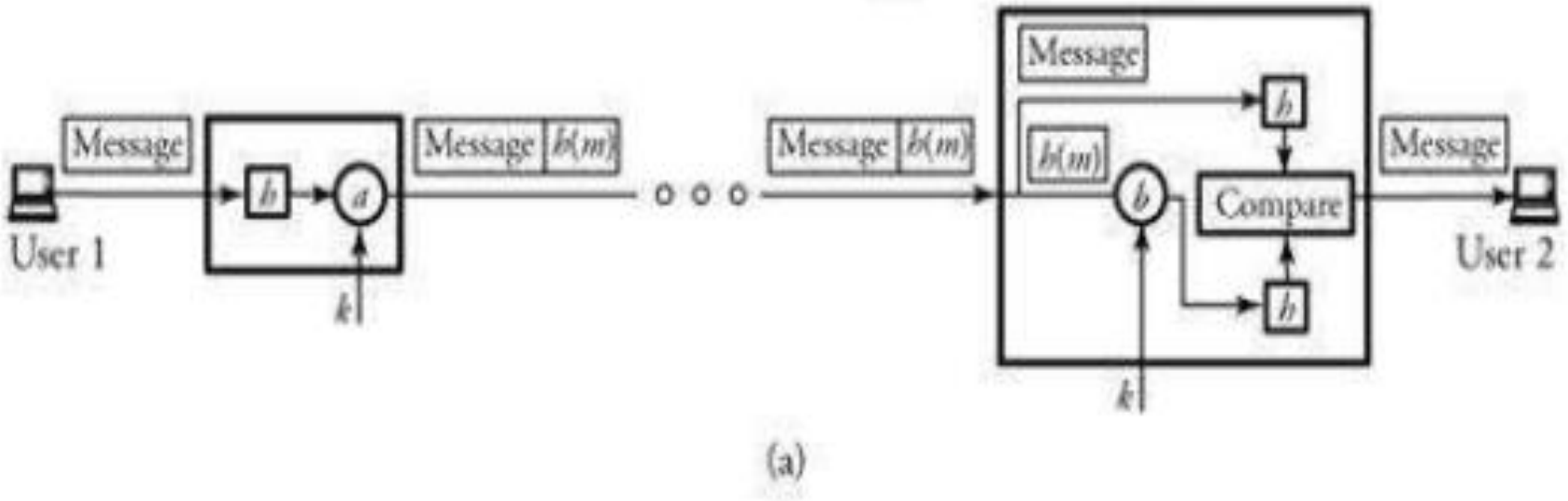
- Used to verify the identity
- Authenticates both message content and message sender
- Use of hash function and encryption of resulting message digest authenticate message contents
- Digital signature authenticates the sender

Cryptographic hash function

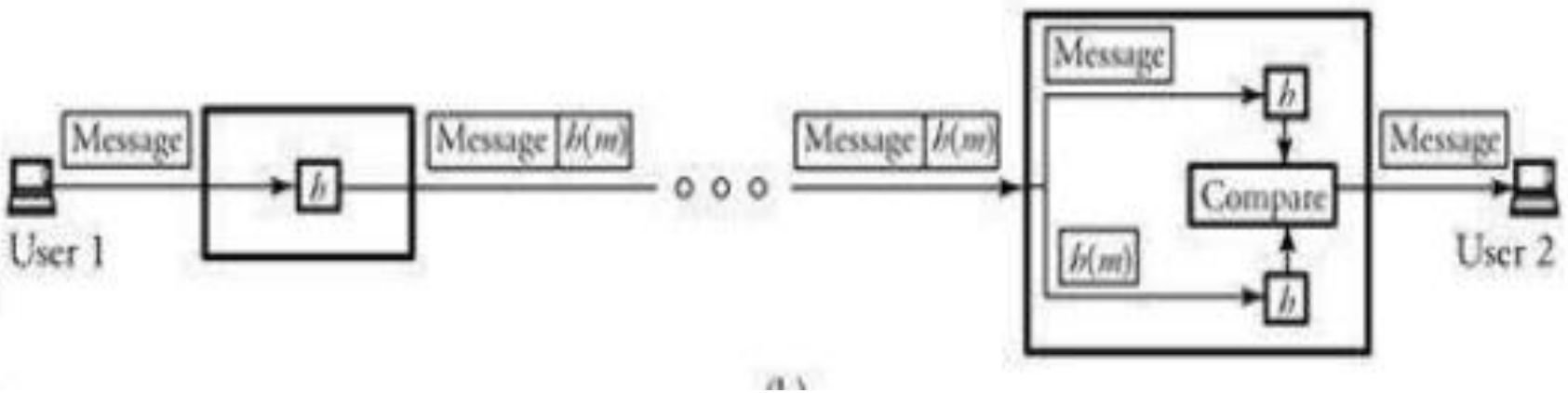
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitrary length but output is always of fixed length.
- Values returned by a hash function are called **message digest** or simply **hash values**.



- **Hash Function** to authenticate a message
- It produces “Fingerprint” of a message
- *m* → Hash function ‘*h*’ → *h(m)* (message digest)
- Hash fun. Has following properties:
  - Authentication algorithm is not required to be reversible
  - Computationally infeasible to find ‘m’ from h(m)
  - Computationally infeasible to find two different message m1 and m2 such that h(m1) = h(m2)
- Message authentication can be done in 2 methods


Message
h
a
Message
h(m)
User 1
k
Message
h(m)
Message
h
h(m)
b
Compare
h
Message
User 2
k

(a)


Message
h
Message
h(m)
User 1
Message
h(m)
Message
h
Compare
h(m)
h
Message
User 2

- Most popular message authentication protocols
  - MD5 (Message Digest 5)
  - Secure Hash Algorithm (SHA)
- Secure Hash Algorithm (SHA):
  - It is a digital signature standard
  - SHA-1 : 1st version
  - Takes message with maximum length of 2^{24} and produces 160-bit digest
  - It uses five registers R1-R5 to store state of 20 bytes

Steps in SHA-1

- Step 1: Pad a message *m* to make the length of the message $\ell_m = 448 \bmod 512$
  - *Padding includes a 1 bit and as many as 0 bits*
  - *64 bit of length are appended to the padded message*
  - *A 512 Block includes (Message+pad+64)*

350	98	64

- Step 2: Expand each block of 512 bit (16 of 32bit) word ($m_0, m_1, m_2, \ldots\ldots m_{15}$) to word of 80 of 32 bits

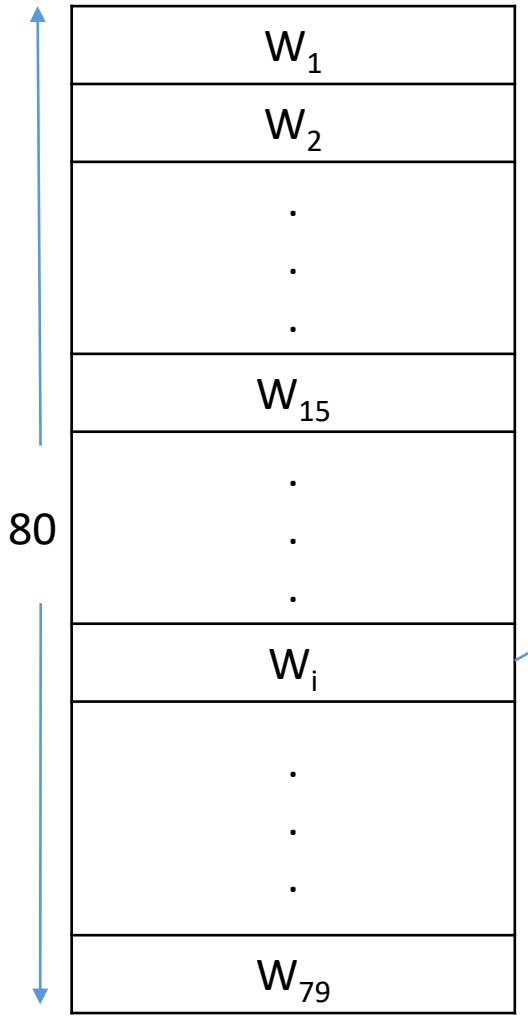
$$w_i = m_i \quad \text{for } 0 \le i \le 15$$

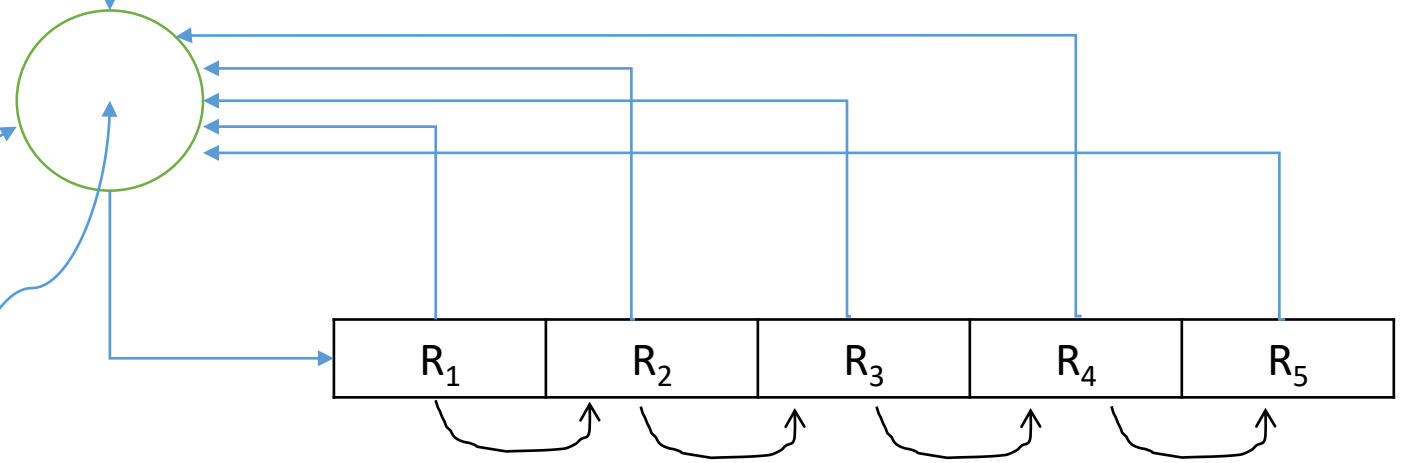
and

$$w_i = w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16} \quad \text{for } 16 \le i \le 79$$

$$w_{16} = w_{13} \oplus w_8 \oplus w_2 \oplus w_0$$

$$F_i(a,b,c) = \begin{cases} (a \cap b) \cup (\bar{a} \cap c) & 0 \le i \le 19 \\ a \oplus b \oplus c & 20 \le i \le 19 \\ (a \cap b) \cup (a \cap c) \cup (b \cap c) & 40 \le i \le 59 \\ a \oplus b \oplus c & 60 \le i \le 79 \end{cases}$$





For 80 steps(i=0,1,2,…79)

$\delta = (R_1 << 5) + F_i(R_2,R_3,R_4) + R_5 + W_i + C_i$

R5 = R4
R4 = R3
R3 = R2 <<30
R2 = R1
R1 = δ

Versions of SHA Algorithm

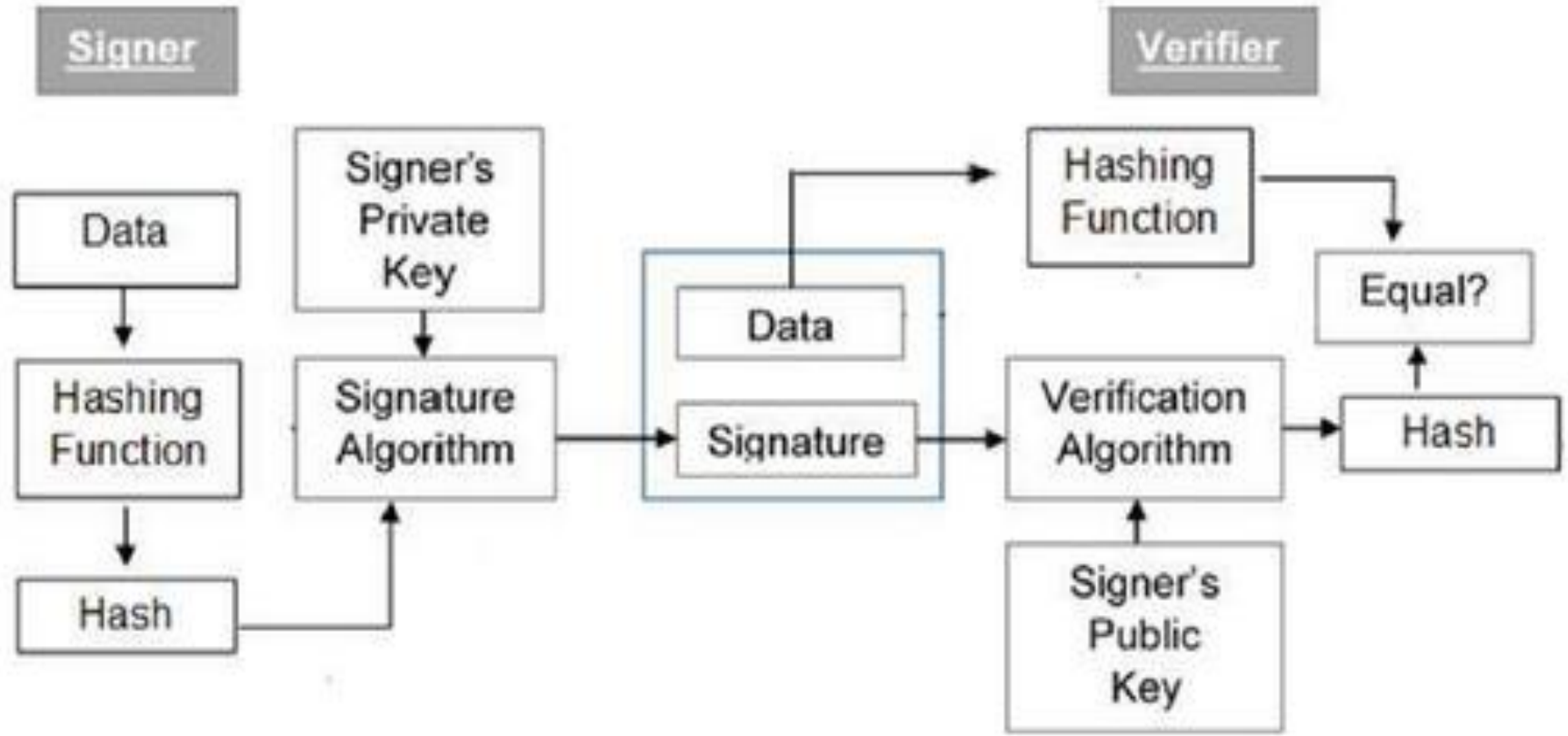
Table 1. Differences Each SHA Algorithm Variation

Algorithm	Message Length (*bit*)	Block Size (in *bits*)	Word Size (in *bits*)	The Size of the Message Digest (*bit*)
SHA 1	$<2^{64}$	512	32	160
SHA 256	$<2^{64}$	512	32	256
SHA 384	$<2^{128}$	1024	64	384
SHA 512	$<2^{128}$	1024	64	512

Digital signature

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
- As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security.
- It is intended to solve the problem of tampering and impersonation in digital communications.

Authentication and Digital Signature



FIREWALL

- Protects data from outside world
- It can be a Software or Hardware device
- It's a simple router implemented with a special program
- H/W firewall is more secure than S/W firewall
- Its also used to control data traffic
  - Packet filtering
  - Packet filtering based on source IP Address
  - Prevents DoS attacks

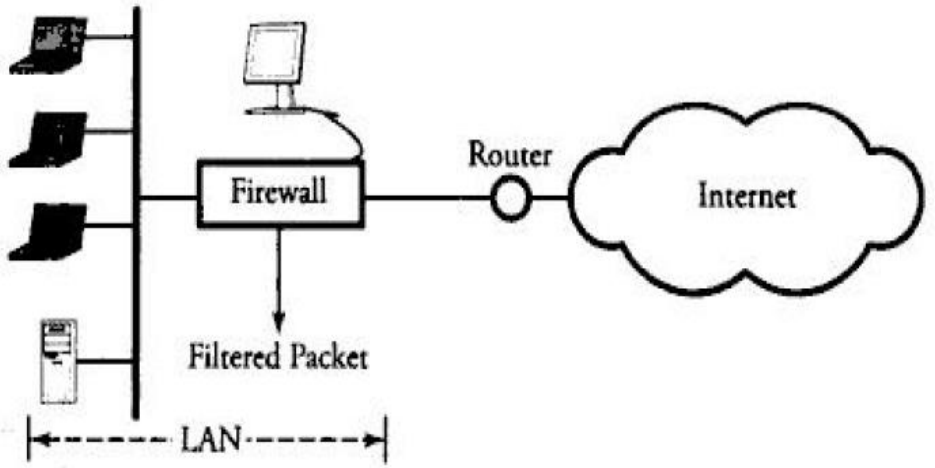


Figure 10.8 A simple configuration of a secured network using a firewall

Packet Filtering

- Packet filtering is a network security mechanism that works by controlling what data can flow to and from a network.

Proxy Server

- A **proxy server** is a computer system or router that functions as a relay between client and **server**.
- It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.
- The word **proxy** means "to act on behalf of another," and a **proxy server** acts on behalf of the user.