Network Security

Module 4

Contents

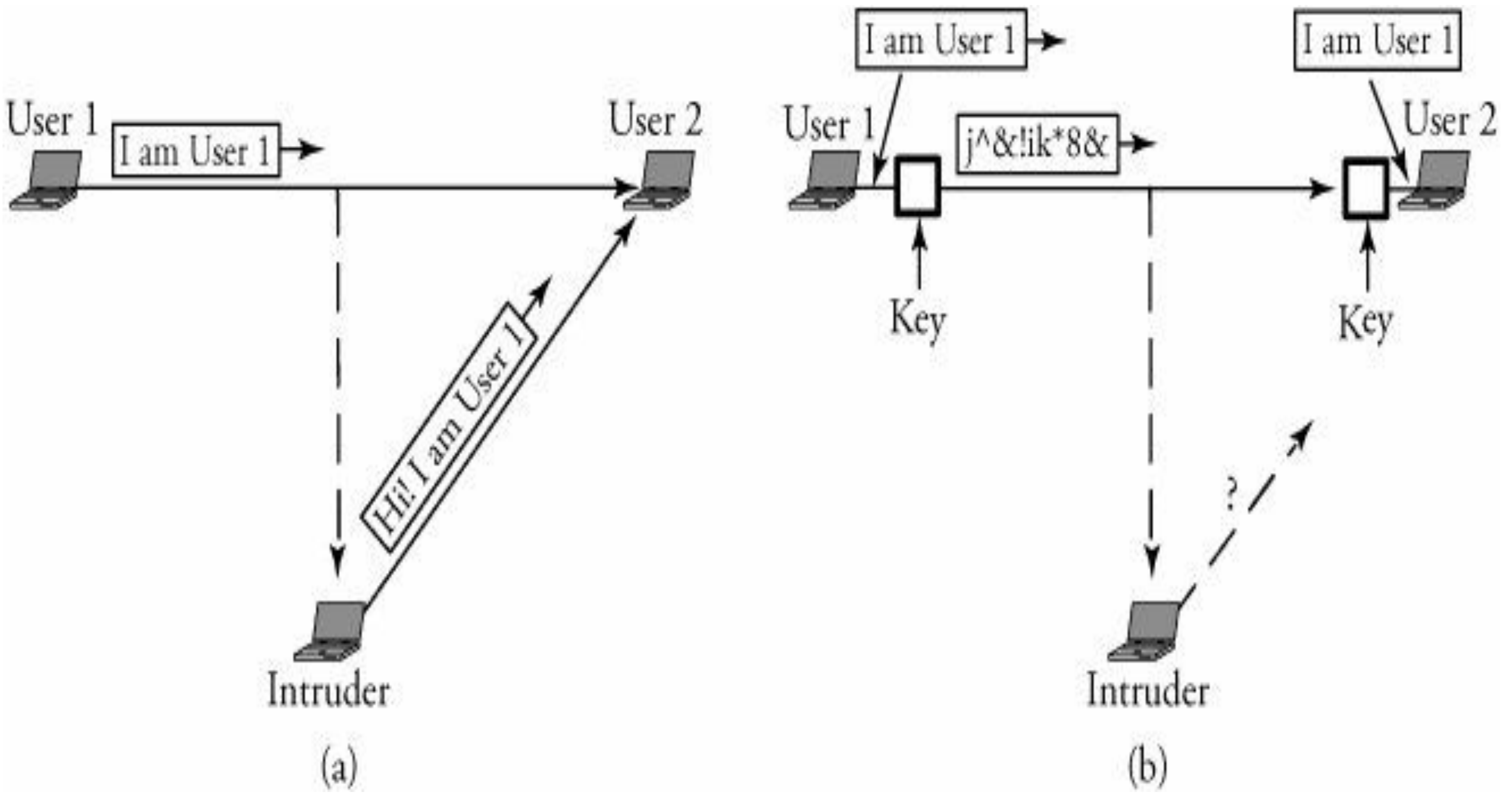
- Overview of Network Security: Elements and Threats
- Overview of Security Methods
- Secret-key Encryption Protocols
- Public-key Encryption Protocols
- Authentication: Message Digest and Digital Signatures
- Security of IP and Wireless Networks
- Firewalls

Elements of Network Security

- Network security is a top-priority issue in data networks.
- Network security is concerned mainly with the following two elements:
  - **Confidentiality**: Information should be available only to those who have rightful access to it.

  - **Authenticity and integrity:** The sender of a message and the message itself should be verified at the receiving point.

Elements of Network Security



Threats to Network Security

- Classified into four categories, as follows

- DNS hacking
- Routing Table Poisoning
- Packet mistreatment
- Denial of Service

DNS hacking

- DNS server is a distributed hierarchical and global directory that translates domain names into numerical IP address
- In the normal mode of operation, hosts send UDP queries to the DNS server.
- Servers reply with a proper answer, or direct the queries to smarter servers
- A DNS hacking attack may result in the lack of data authenticity and integrity

DNS hacking

- Appear in any of the following forms:
  - An information-level attack
  - A masquerading attack
  - An information leakage attack
  - The domain high jacking attack

Routing Table Poisoning

- undesired modification of routing tables

- An attacker can do this by maliciously modifying the routing information update packets sent by routers

- Two types of routing table poisoning attacks are the link attack and the router attack

Routing Table Poisoning

- **Link attack** occurs when a hacker gets access to a link and thereby intercepts, interrupts, or modifies routing messages on packets
- Similarly on both the link-state and the distance-vector protocols
- If an attacker succeeds in placing an attack in a link-state routing protocol, a router may send incorrect updates about its neighbors or remain silent even if the link state of its neighbor has changed

Routing Table Poisoning

- **Router attacks** may affect the link-state protocol or even the distance-vector protocol
- If link-state protocol routers are attacked, they become malicious
- In the distance-vector protocol, an attacker may cause routers to send wrong updates about any node in the network

Packet mistreatment

- Attack can occur during any data transmission
- A hacker may capture certain data packets and mistreat them
- This is also be subclassified into link attacks and router attacks.
- The link attack causes interruption, modification, or replication of data packets.
- A router attack can misroute all packets and may result in congestion or denial of service.

Packet mistreatment

- Some examples of a packet-mistreatment attack
  - ✓ Interruption
  - ✓ Modification
  - ✓ Replication
  - ✓ Ping of death
  - ✓ Malicious misrouting of packets

Denial of Service

- DoS is a type of security breach that prohibits a user from accessing normally provided services

- The denial of service does not result in information theft or any kind of information loss but can nonetheless be very dangerous

- Denial-of-service attacks affect the destination rather than a data packet or router.

Denial of Service

- Denial-of-service attacks are easy to generate but difficult to detect

- They take important servers out of action for few hours, thereby denying service to all users

- In these attacks, the hacker's main aim is to overwhelm victims and disrupt services provided to them.

Denial of Service

- Denial-of-service attacks are two types

  1. Single-source
  2. Distributed

Overview of Security Methods

- 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.

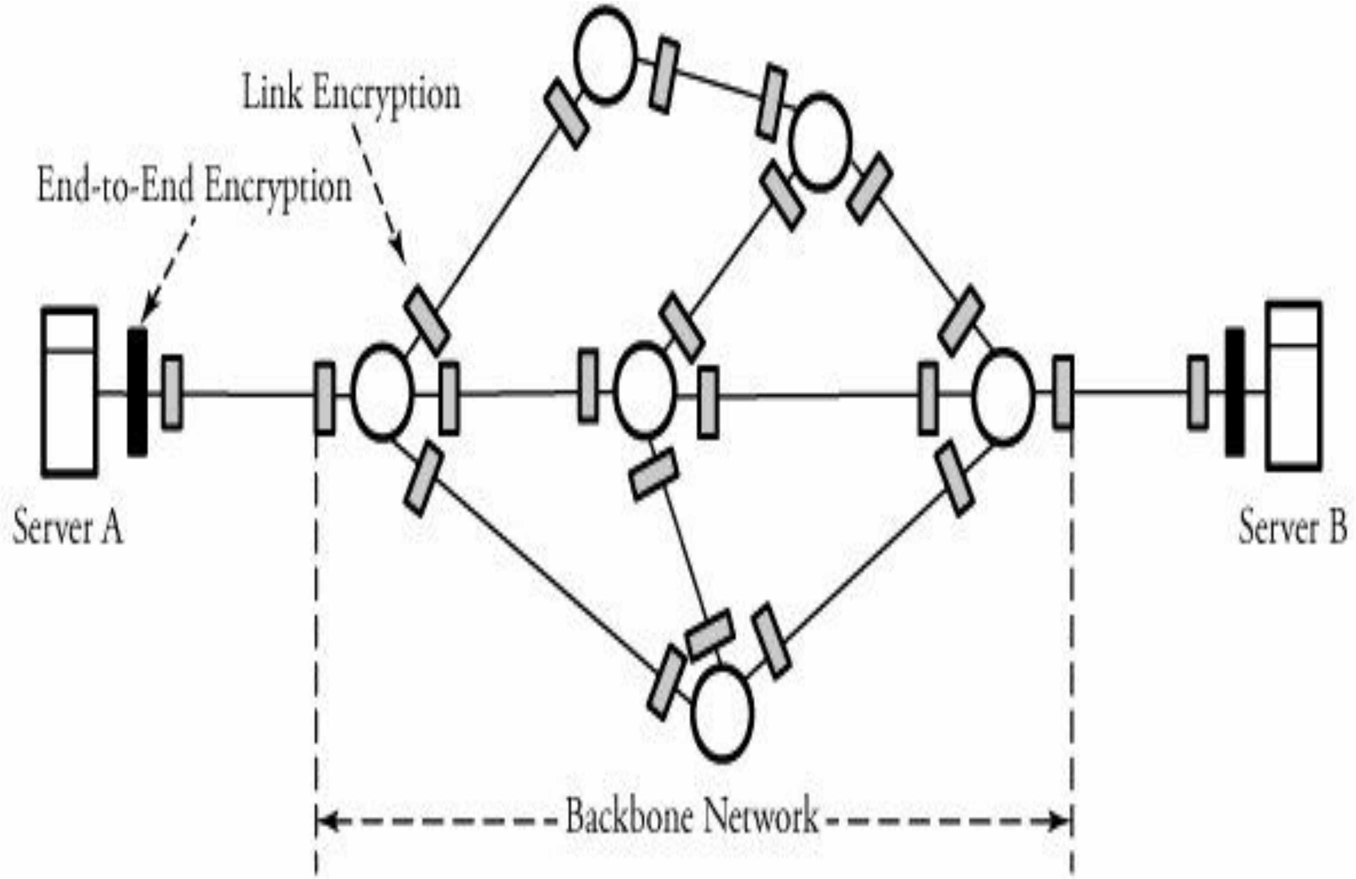
- The message is scrambled before transmission so that it is undetectable by outside watchers

- This kind of message needs to be decoded at the receiving end before any further processing

Cryptographic Techniques

- to encrypt a message M is a secret key K;
- The fundamental operation often used to encrypt a message is the Exclusive-OR.

Overview of encryption points in a communication network



Cryptographic Techniques

- Two types of encryption techniques are *secret-key encryption* and *public-key encryption*

- In a secret-key model, both sender and receiver conventionally use the same key for an encryption process.

- In a public-key model, a sender and a receiver each use a different key

- The public-key system is more powerful than the secret-key system and provides better security and message privacy.
- But the biggest drawback of public-key encryption is speed.

Authentication Techniques

- Encryption methods offer the assurance of message confidentiality
- A networking system must be able to verify the authenticity of the message and the sender of the message
- authentication techniques are categorized as authentication with message digest and authentication with digital signature
- Message authentication protects a user in a network against data falsification and ensures data integrity
- These methods do not necessarily use keys.

Secret-Key Encryption Protocols

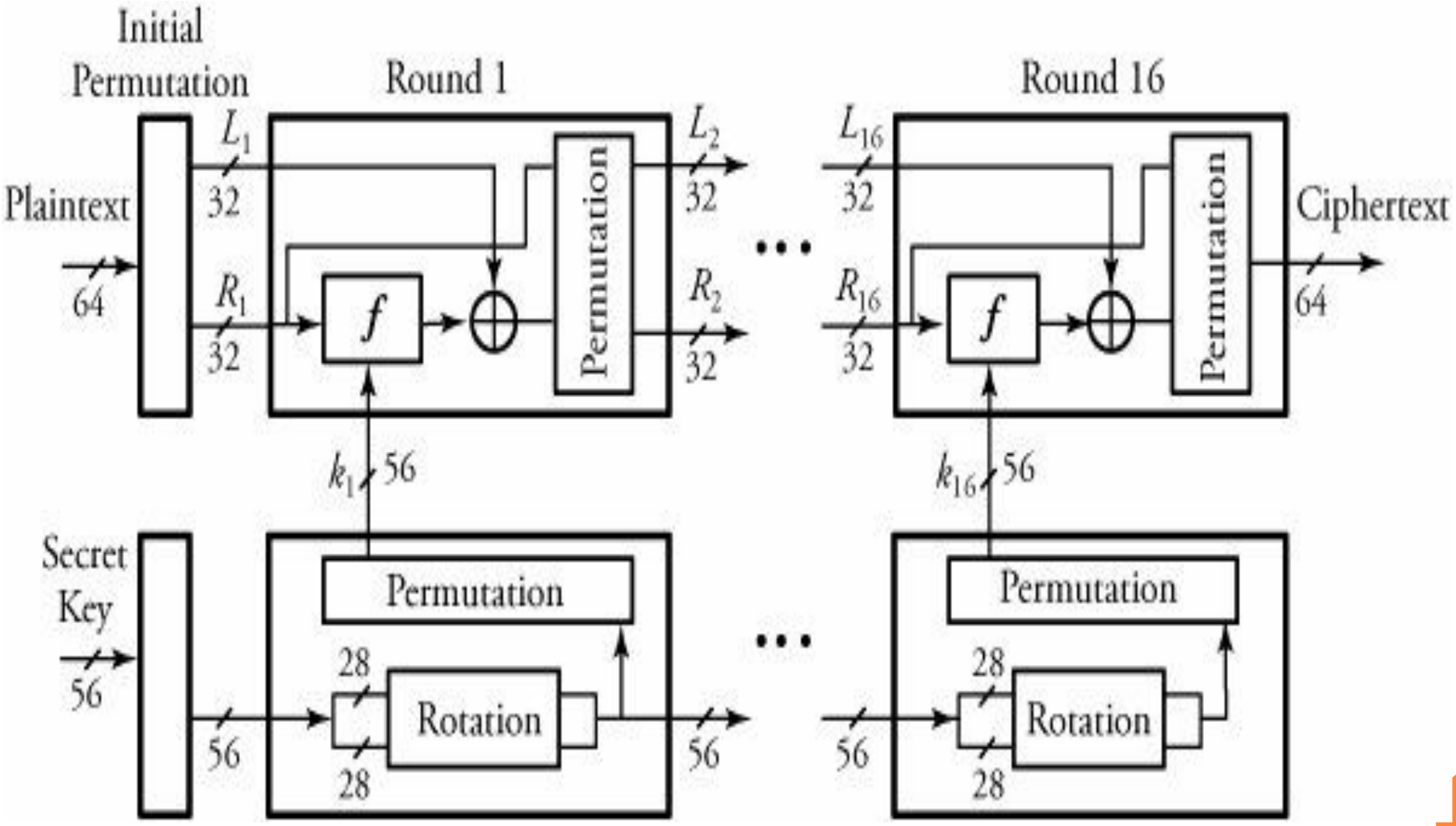
- Secret-key encryption protocols, known as symmetric encryption, or single-key encryption protocols

- Two protocols:
  - Data Encryption Standard (DES) and
  - Advanced Encryption Standard (AES).

Data Encryption Standard (DES)

- Plaintext messages are converted into 64-bit blocks, each encrypted using a key.
- The key length is 64 bits but contains only 56 usable bits;
- The last bit of each 8 byte in the key is a parity bit for the corresponding byte.
- DES consists of 16 identical rounds of an operation

Data Encryption Standard (DES)



Data Encryption Standard (DES)

- Begin DES Algorithm

1. Initialize. Before round 1 begins, all 64 bits of an incoming 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-bit halves, and each half is rotated one or two bit positions, depending on the round.

Data Encryption Standard (DES)

4. All 56 bits of the key are permuted, producing version k_i of the key on round i.

5. In this step, combination of logic Exclusive-OR, and the a function F() appears. Then, L_i and R_i are determined by

$L_i=R_{i-1}$

$R_i=L_{i-1} \square F(R_{i-1}; k_i)$

6. All 64 bits of a message are permuted.

Advanced Encryption Standard (AES)

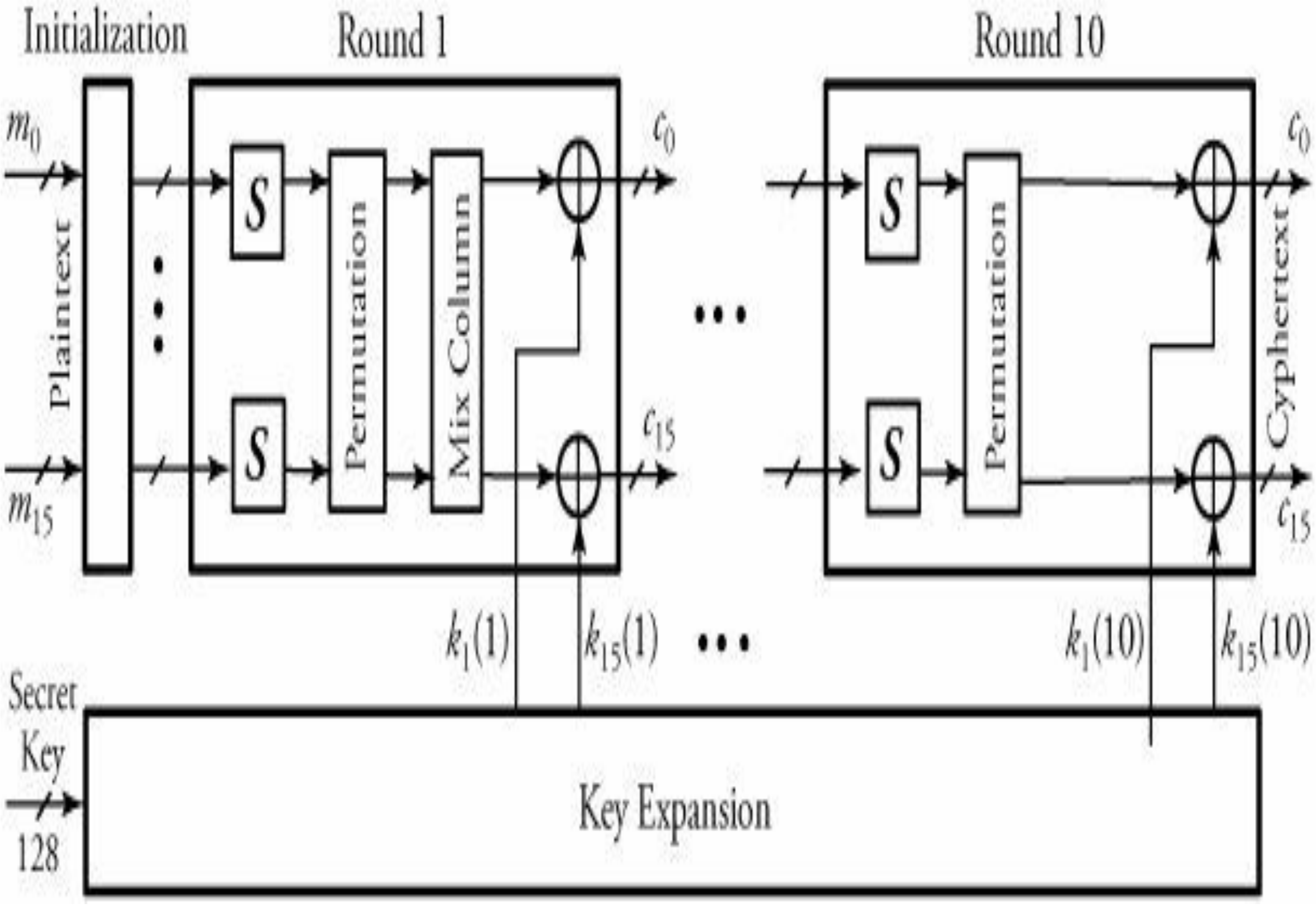
- Protocol has a better security strength than DES.

- AES supports 128-bit symmetric block messages

- It uses 128, 192, or 256 bit keys.

- The number of rounds in AES is variable from 10 to 14 rounds, depending on the key and block sizes.

Advanced Encryption Standard (AES)



Advanced Encryption Standard (AES)

- A single block of 128-bit plaintext (16 bytes) as an input arrives from the left.
- The plaintext is formed as 16 bytes m_0 through m_{15} and is fed into round 1 after an initialization stage.
- In this round, substitute units indicated by S in the figure perform a byte-by-byte substitution of blocks.
- The ciphers, in the form of rows and columns, move through a permutation stage to shift rows to mix columns.
- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key $k_0(1)$ through $k_{15}(1)$.
- The 128-bit key is expanded for ten rounds.

Advanced Encryption Standard (AES)

- AES decryption algorithm is fairly simple and is basically the reverse of the encryption algorithm at each stage of a round.

- All stages of each round are reversible.

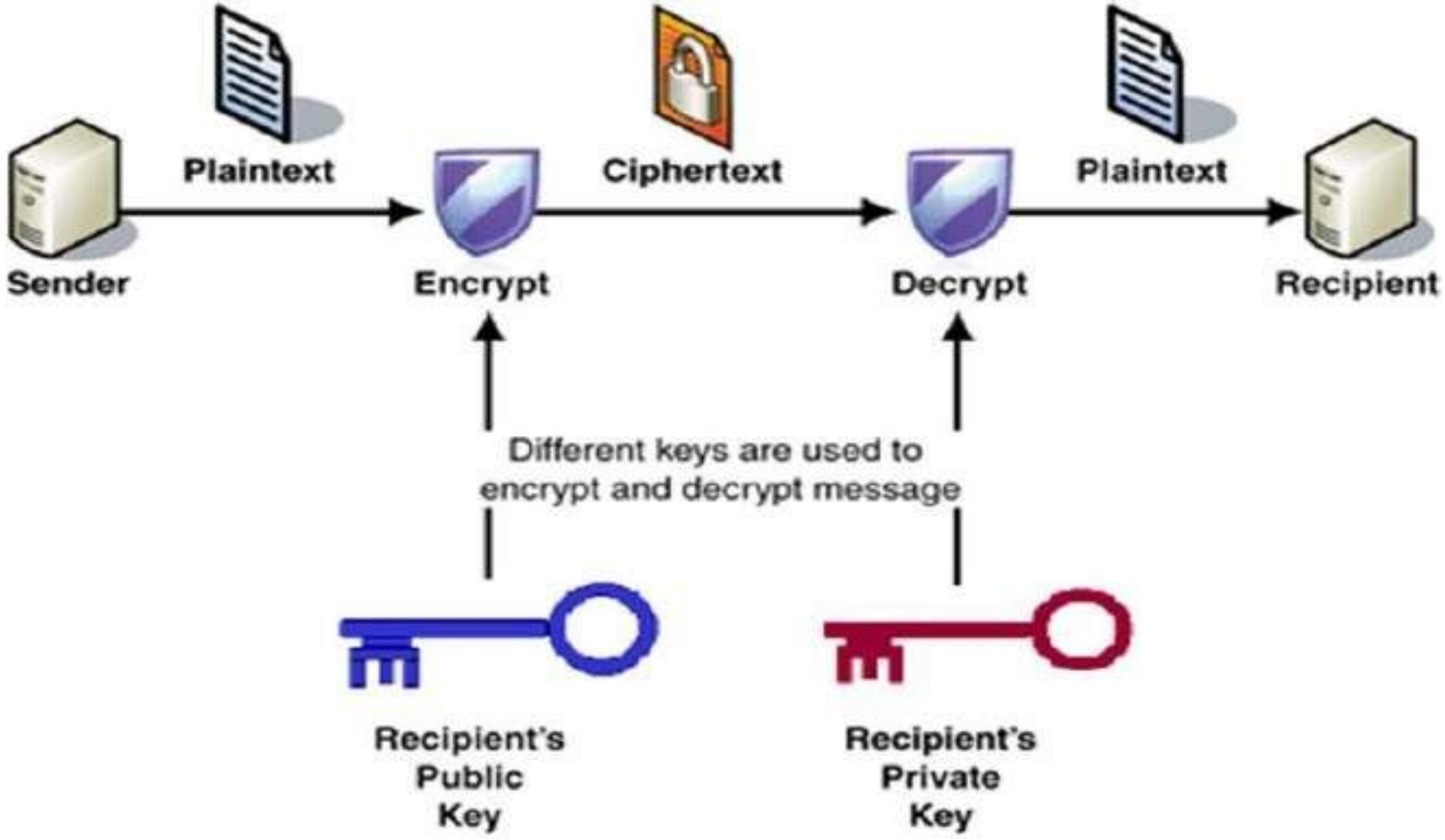
Public-Key Encryption Protocols

- Public-key cryptography provided a very clever method for key exchange.
- In the public-key encryption model, a sender/ receiver pair use different keys.
- This model is sometimes known as asymmetric, or two-key, encryption.
- Several public-key encryption protocols can be implemented.
- The following two protocols are the focus of our study:
  - Rivest, Shamir, and Aldeman (RSA) protocol
  - Diffie-Hillman key-exchange protocol.

Public-Key Encryption Protocols

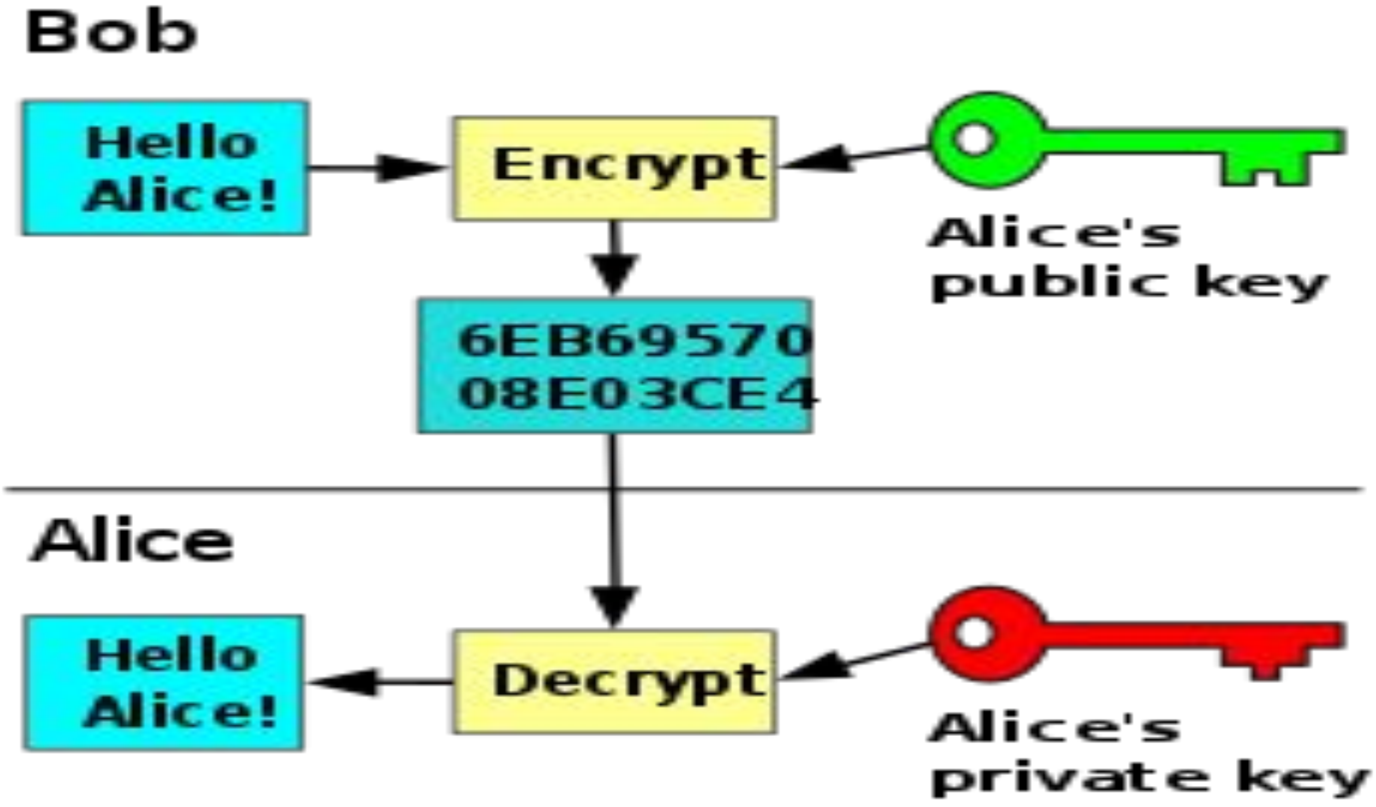
- In the public-key encryption methods, either of the two related keys can be used for encryption;
- The other one, for decryption.
- It is computationally infeasible to determine the decryption key given only the algorithm and the encryption key.
- Each system using this encryption method generates a pair of keys to be used for encryption and decryption of a message that it will receive.
- Each system publishes its encryption key by placing it in a public register or file and sorts out the key as a public one.
- The companion key is kept private.

EXAMPLES



Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to encrypt and decrypt message
Recipient's Public Key
Recipient's Private Key

Examples


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

RSA Algorithm

- Rivest, Shamir, and Aldeman developed the RSA public-key encryption and signature scheme
- This was the first practical public-key encryption algorithm.
- RSA is based on the intractability of factoring large integers.
- Assume that a plaintext M must be encrypted to a ciphertext C.
- The RSA algorithm has three phases for this: key generation, encryption, and decryption.

RSA Algorithm

- **Key Generation**
  - The key length is typically 512 bits,
  - Which requires an enormous computational power.
  - A plaintext is encrypted in blocks, with each block having a binary value less than some number n.
  - Encryption and decryption are done as follows, beginning with the generation of a public key and a private key.

RSA Algorithm

- **Begin Key Generation Algorithm**

1. Choose two roughly 256-bit prime numbers, a and b, and derive n = ab.
2. **Find x**. Select encryption key x such that x and (a - 1)(b - 1) are relatively prime.
3. **Find y**. Calculate decryption key y:

   xy mod(a-1)(b-1)=1
4. At this point, a and b can be discarded.
5. The public key = **{x, n}.**
6. The private key = **{y, n}.**

In this algorithm, x and n are known to both sender and receiver, but only the receiver must know y

RSA Algorithm

- **Encryption**
  - Both sender and receiver must know the value of n.
  - The sender knows the value of x, and only the receiver knows the value of y.
  - Thus, this is a public-key encryption, with the public key {x, n} and the private key {y, n}.
  - Given m<n, ciphertext c is constructed by

$$\mathbf{C = m^{x} \bmod n}$$

- **Decryption**
  - Given the ciphertext, c, the plaintext, m, is extracted by

$$\mathbf{m = C^{y} \bmod n}$$

RSA Algorithm

- Example

Diffie-Hillman Key-Exchange Protocol

- Diffie-Hillman key-exchange protocol, two end users can agree on a shared secret code without any information shared in advance.

- Thus, intruders would not be able to access the transmitted communication between the two users or discover the shared secret code.

- This protocol is normally used for virtual private networks (VPNs),

Diffie-Hillman Key-Exchange Protocol

- The essence of this protocol for two users, 1 and 2, is as follows.
- Suppose that user 1 selects a prime a, a random integer number x_1, and a generator g and creates $y_1 \in \{1, 2, ..., a - 1\}$ such that

  $$\mathbf{y_1 = g^{x1} mod\ a}$$

- The two end users agree on **a** and **g** ahead of time.
- User 2 performs the same function and creates y_2:

  $$\mathbf{y_2 = g^{x2} mod\ a}$$

Diffie-Hillman Key-Exchange Protocol

- User 1 then sends y_1 to user 2 and User 2 sends y_2 to user 1.
- Now, user 1 forms its key, k_1, using the information its partner sent as

  $$\mathbf{k_1 = y_2^{x1} mod\ a}$$

- User 2 forms its key, k_2, using the information its partner sent it as

  $$\mathbf{k_2 = y_1^{x2} mod\ a}$$

- It can easily be proved that the two Keys k_1 and k_2 are equal.
- Therefore, the two users can now encrypt their messages, each using its own key created by the other one's information

Authentication

- Authentication techniques are used to verify identity.

- Message authentication verifies the authenticity of both the message content and the message sender.

- Message content is authenticated through implementation of a hash function and encryption of the resulting message digest.

- The sender's authenticity can be implemented by use of a digital signature.

Authentication

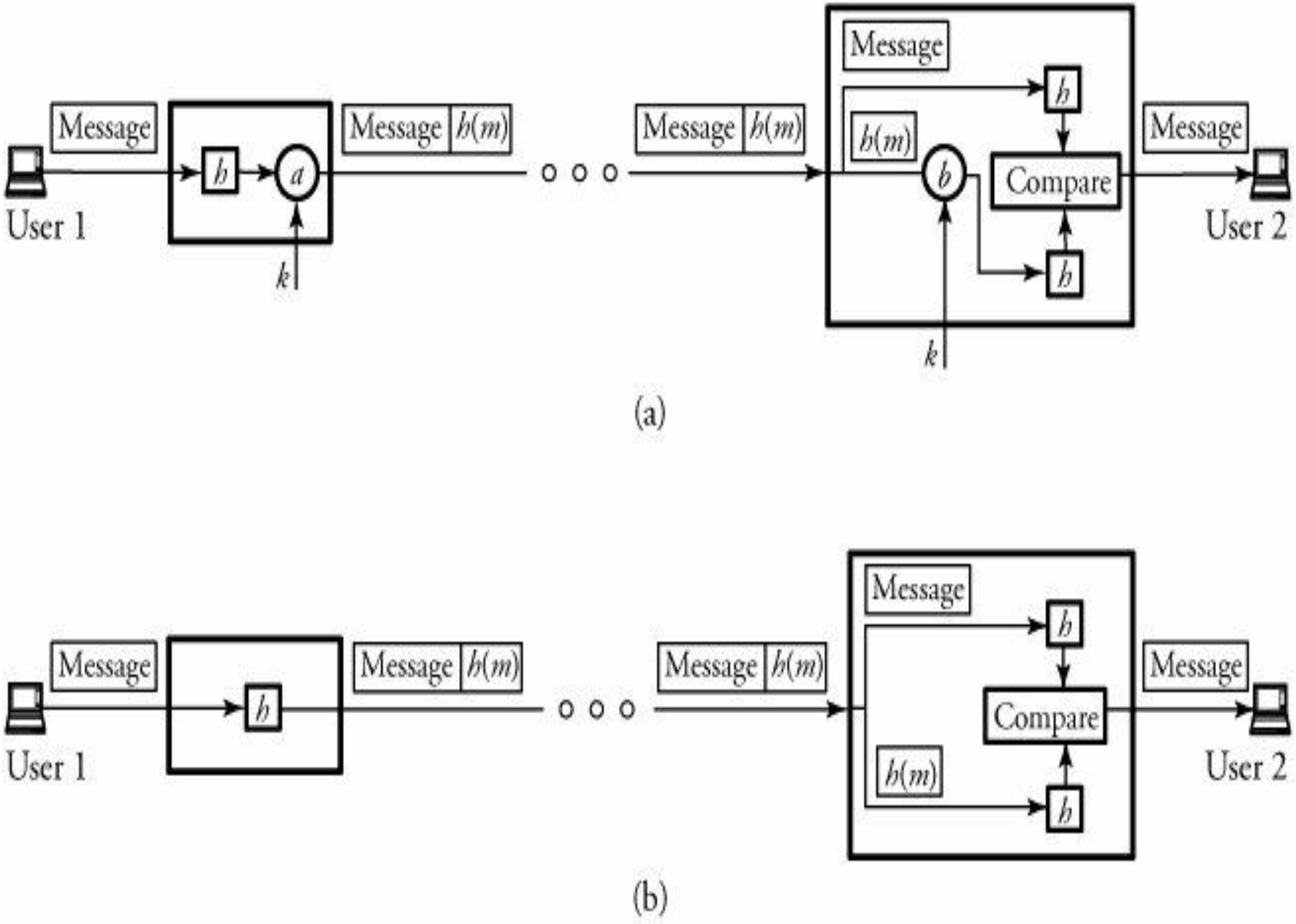
- A common technique for authenticating a message is to implement a hash function
- Which is used to produce a "fingerprint" of a message.
- The hash value is added at the end of message before transmission.
- The receiver re-computes the hash value from the received message and compares it to the received hash value.
- If the two hash values are the same, the message was not altered during transmission.

Authentication

- Once a hash function is applied on a message, **m**, the result is known as a message digest, or **h(m).**

- The hash function has the following properties.
  - Unlike the encryption algorithm, the authentication algorithm is not required to be reversible.
  - Given a message digest **h(m)**, it is computationally infeasible to find **m**.
  - It is computationally infeasible to find two different messages $\mathbf{m_1}$ and $\mathbf{m_2}$ such that $\mathbf{h(m_1) = h(m_2)}$**.**

Authentication



(a)

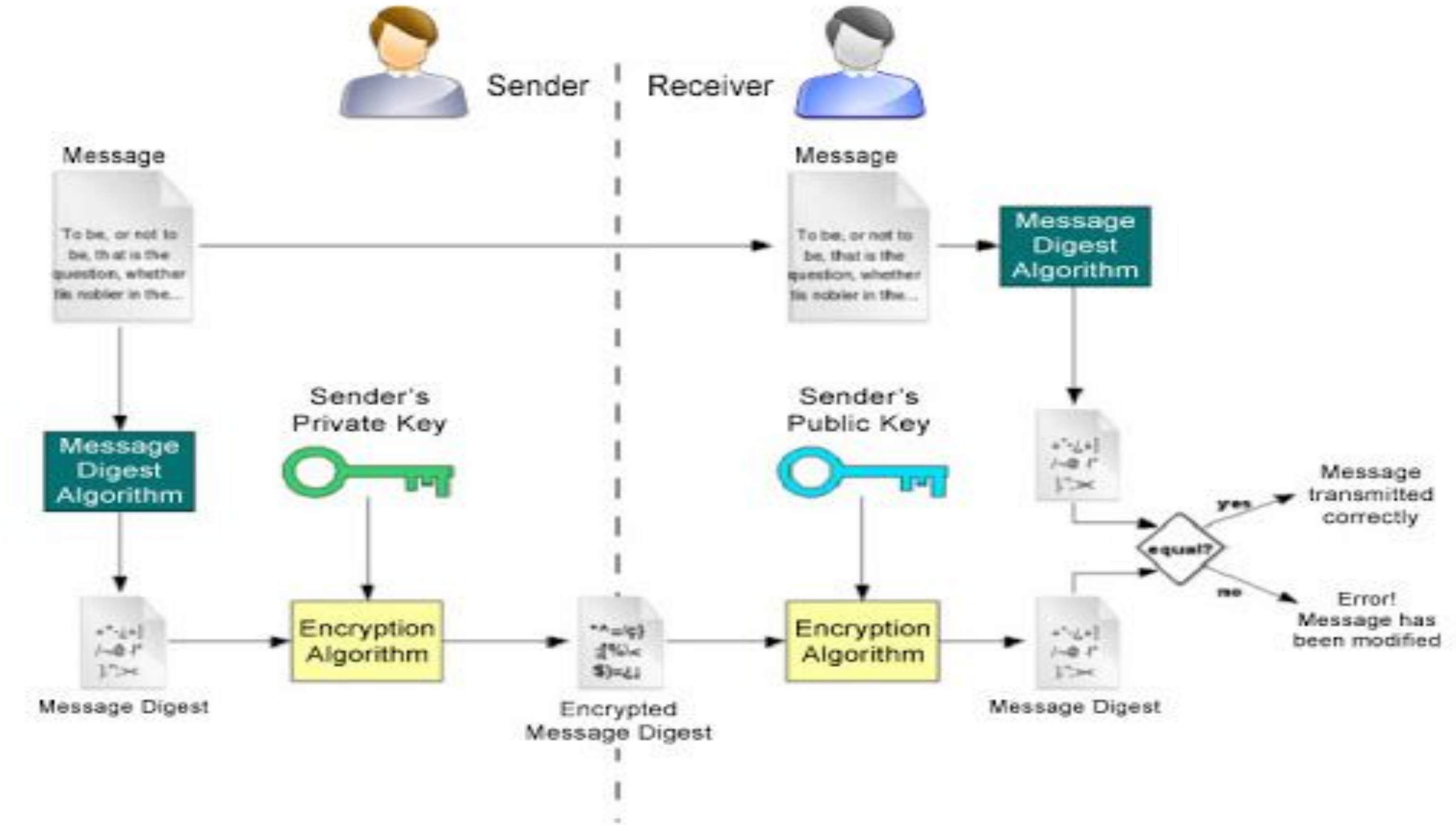
(b)

Authentication

- Message authentication can be implemented by two methods
- In the first method, a hash function is applied on a message, and then a process of encryption is implemented. Thus, a message digest can also be encrypted in this method.

- In the second method, no encryption is involved in the process of message authentication.
- This technique is more popular in the security infrastructure of the Internet Protocol.

Authentication



Secure Hash Algorithm (SHA)

- SHA was proposed as part of the digital signature standard.

- SHA-1, the first version of this standard, takes messages with a maximum length of 2^{24} and produces a 160-bit digest.

- With this algorithm, SHA-1 uses five registers, R_1 through R_5, to maintain a "state" of 20 bytes.

Secure Hash Algorithm (SHA)

- The first step is to pad a message m with length l_m.
- The message length is forced to $l_m = 448 \bmod 512$.
- In other words, the length of the padded message becomes 64 bits less than the multiple of 512 bits.
- The number of padding bits can be as low as 1 bit and as high as 512 bits.
- The padding includes a 1 bit and as many 0 bits as required.
- Therefore, the least-significant 64 bits of the message length are appended to convert the padded message to a word with a multiple of 512 bits..

Secure Hash Algorithm (SHA)

- After padding, the second step is to expand each block of 512-bit (16, 32 bits) words $\{m_0, m_1, ..., m_{15}\}$ to words of 80, 32 bits using

  $$\mathbf{w_i = m_i\ ,\ for\ 0 \le \mathit{i} \le 15}$$

and

- $w_i = w_{i-3}$ □ w_{i-8} □ w_{i-14} □ w_{i-16} □1 for $16 \le i \le 79$

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

$$F_i(a, b, c) = \begin{cases} (a \cap b) \cup (\bar{a} \cap c) & 0 \le i \le 19 \\ a \oplus b \oplus c & 20 \le i \le 39 \\ (a \cap b) \cup (a \cap c) \cup (b \cap c) & 40 \le i \le 59 \\ a \oplus b \oplus c & 60 \le i \le 79 \end{cases}.$$

$R_5 = R_4$
$R_4 = R_3$
$R_3 = R_2$ □ 30
$R_2 = R_1$
$R_1 =$ □

The message digest is produced by concatenation of the values in R_1 through R_5

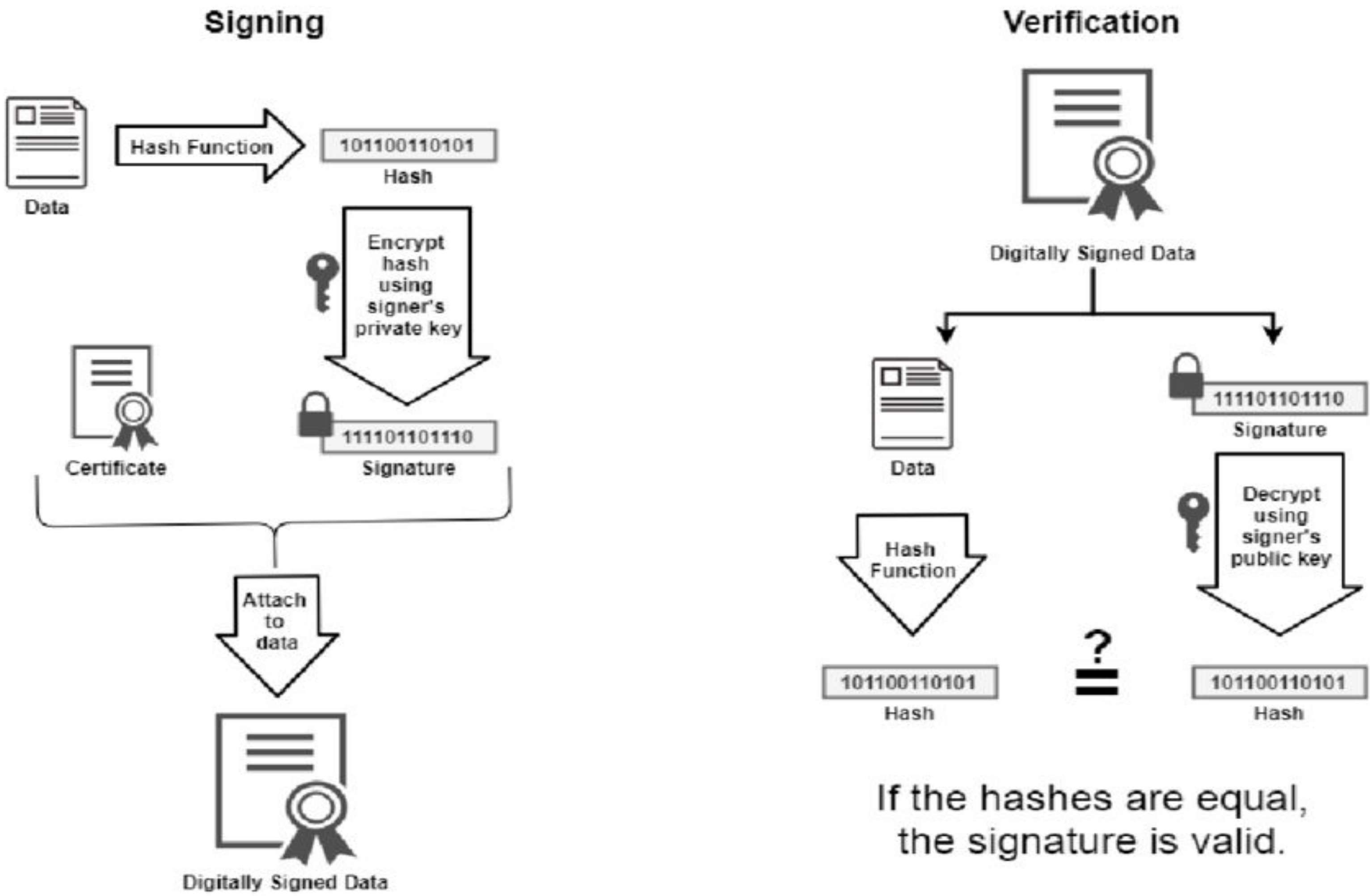
Authentication and Digital Signature

- A digital signature is one of the most important required security measures.
- Much like a person's signature on a document, a digital signature on a message is required for the authentication and identification of the right sender.
- The digital signature is supposed to be unique to an individual and serves as a means of identifying the sender.
- An electronic signature is not as easy as it was with the paper-based system.

Authentication and Digital Signature

- The technical method of providing a sender's authentication is performed through cryptography.
- The RSA algorithm implements both encryption and digital signature.
- When RSA is applied, the message is encrypted with the sender's private key.
- Thus, the entire encrypted message serves as a digital signature.
- This means that at the receiving end, the receiver can decrypt it, using the public key.
- This authenticates that the packet comes from the right user.

Authentication and Digital Signature

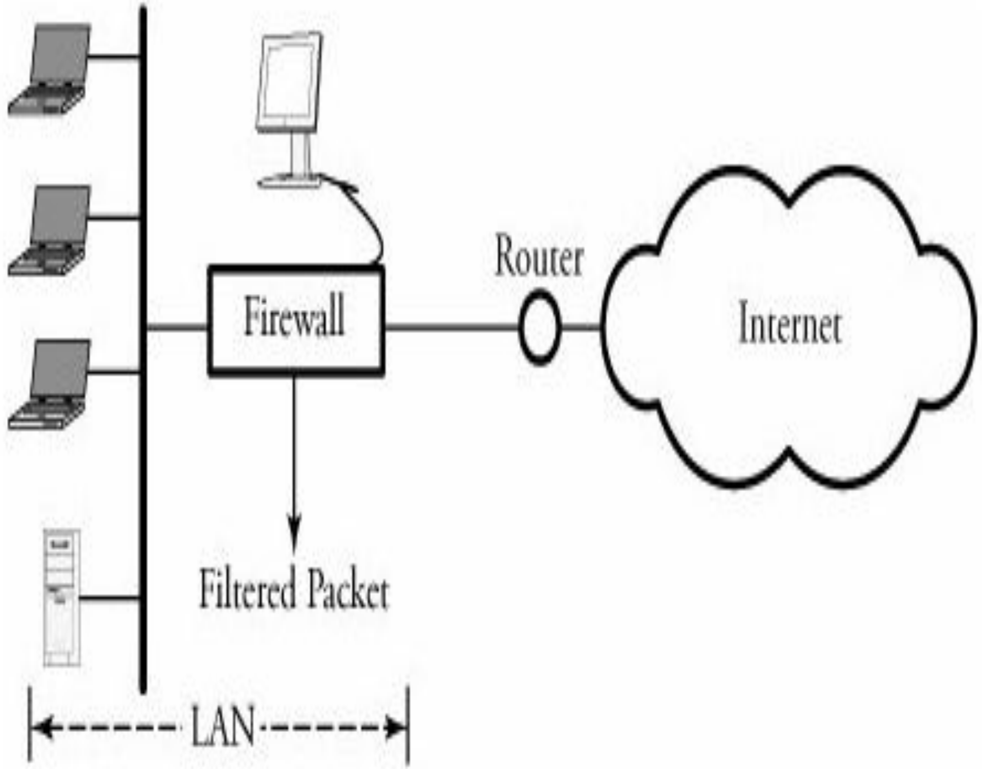


If the hashes are equal,
the signature is valid.

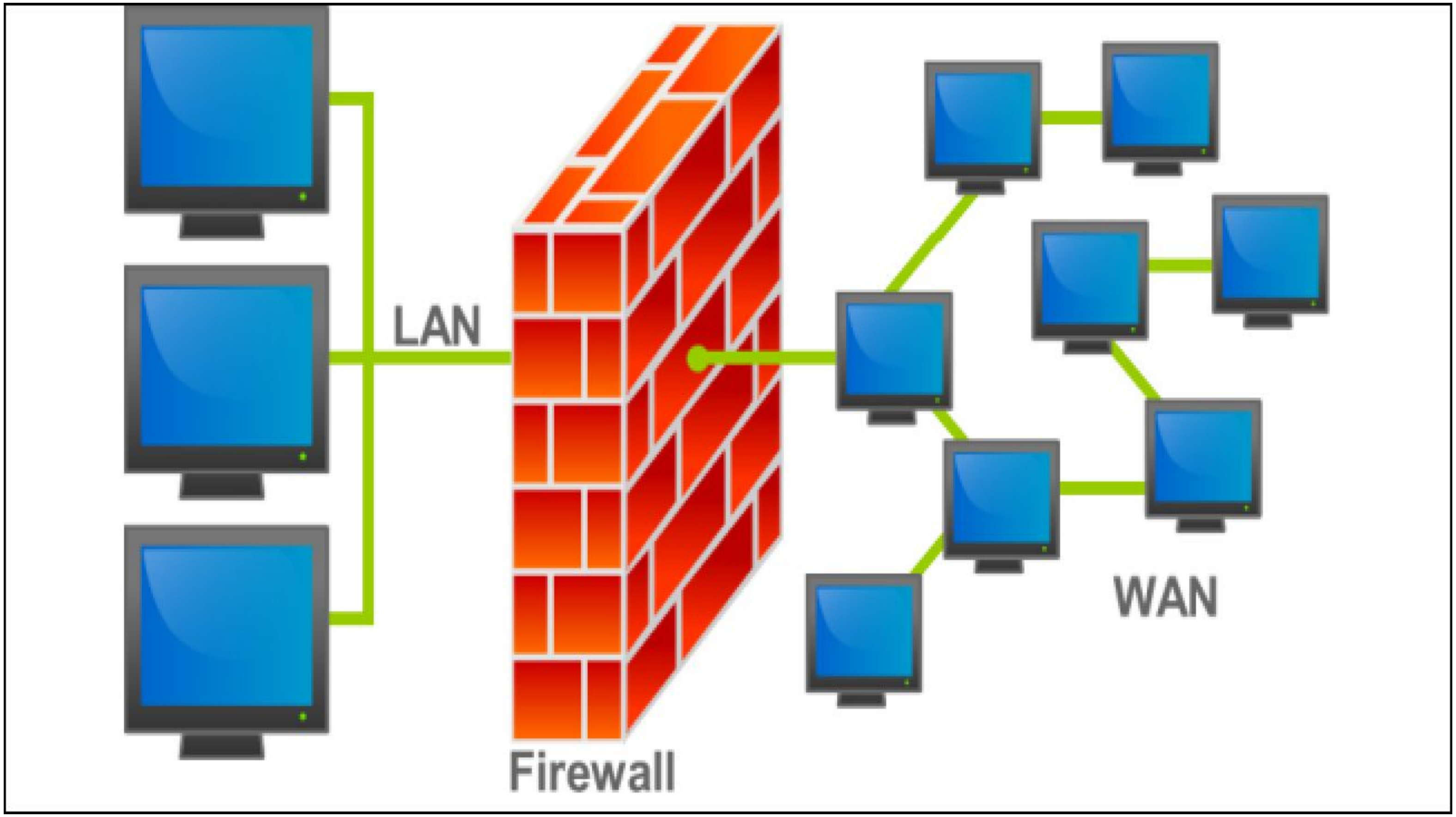
Firewalls

- Firewall protects data from the outside world.
- A firewall can be a software program or a hardware device.
- A firewall a popular security mechanism for networks.
- A firewall is a simple router implemented with a special program.
- This unit is placed between hosts of a certain network and the outside world, and the rest of the network.

Firewalls



Firewalls



Firewalls

- A firewall is placed on the link between a network router and the Internet or between a user and a router.
- The objective of such a configuration is to monitor and filter packets coming from unknown sources.
- Hackers do not have access to penetrate through a system if a firewall protects the system.
- For a large company with many small networks, the firewall is placed on every connection attached to the Internet.

Firewalls

- Companies can set rules about how their networks or particular systems need to work in order to maintain security.
- Companies can also set rules on how a system can connect to Web sites.
- These precautionary rules are followed in order to attain the advantage of having a firewall.
- Hence, the firewall can control how a network works with an Internet connection.
- A firewall can also be used to control data traffic.

Firewalls

- Software firewall programs can be installed in home computers by using an Internet connection with these so called gateways.
- The computer with such a software can access Web servers only through this software firewall.
- Hardware firewalls are more secure than software firewalls.
- Hardware firewalls are not expensive and some firewalls also offer virus protection.
- The biggest security advantage of installing a firewall in a business network is to protect from any outsider logging on to the network under protection.
- Firewalls are preferred for use in almost all network security infrastructures, as they allow the implementation of a security policy in one centralized place rather than end to end.

Firewalls

- A firewall controls the flow of traffic by one of the following three methods.
  - The first method is packet filtering
  - The second method is that a firewall filters packets based on the source IP address
  - The third method, denial of service, this method controls the number of packets entering a network.