JGI JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

Master of Computer Applications

23MCAC102 – Advanced Computer Networks

Unit - V

Network Security Services

Module-5 Syllabus

- Security Services
- Message Confidentiality
- Message Integrity
- Message Authentication
- Digital Signature
- Entity Authentication
- Key Management
- IP Security
- SSL
- Firewall types

Network Security

- Network security is a **shield against** the rising tide of

  → **cyber threats that seek to exploit vulnerabilities**,

  → **compromise data integrity**, and

  → **disrupt the seamless flow of information**.

- It plays a pivotal role in safeguarding

  → sensitive data,

  → preventing unauthorized access, and

  → thwarting malicious activities such as phishing, malware attacks, and unauthorized intrusions.

Network Security

- **Network security is important due to several compelling reasons:**

1. Protection of Sensitive Data:

Organizations store vast amounts of sensitive and confidential information on their networks, including

→ customer data,

→ financial records, and

→ intellectual property.

→ Network security **safeguards this information from unauthorized access**, preventing data breaches and potential financial loss.

Network Security

2. Prevention of Unauthorized Access:

- Unauthorized access to a network can lead to a multitude of problems, including

  → data theft,

  → tampering, or destruction.

- Network security measures such as

  → firewalls,

  → authentication protocols, and encryption

help ensure that only authorized users can access the network resources.

Network Security

3. Mitigation of Cyber Threats:

The internet is rife with various cyber threats, including

→ malware,

→ ransomware,

→ phishing attacks, and more.

- Effective network security measures **act as a defense mechanism**, **detecting and mitigating** these threats before they can cause harm.

Network Security

4. Business Continuity:

- A secure network is essential for maintaining business continuity.
- Downtime due to cyberattacks or security breaches can result in
  → significant financial losses,
  → damage to reputation, and
  → disruptions to operations.
- Network security services contribute to the resilience of business operations.

Network Security

5. Compliance with Regulations:

- Many industries are subject to strict data protection and privacy regulations.
- Implementing robust network security measures ensures that

→ organizations comply with these regulations,

→ avoiding legal consequences,

→ fines, and

→ damage to their reputation.

Network Security

6. Protection Against Insider Threats:

- Insider threats, whether intentional or unintentional, pose a significant risk to an organization's security.
- Network security helps

→ monitor and control internal access to sensitive information,

→ reducing the likelihood of insider-related incidents.

7. Maintaining Customer Trust:

- Customers trust businesses with their data, and a security breach can erode that trust quickly.
- A strong network security posture demonstrates a commitment to protecting customer information, fostering trust and loyalty.

Network Security

8. **Prevention of Service Disruption:**
   - Cyberattacks such as Distributed Denial of Service (DDoS) can disrupt services and lead to financial losses.
   - Network security services help prevent and mitigate the impact of such attacks, ensuring uninterrupted service delivery.
9. **Protection of Intellectual Property:**
   - Organizations invest heavily in the development of intellectual property.
   - Network security safeguards proprietary information, preventing unauthorized access and theft of valuable intellectual assets.

Network Security Services

Network Security Services

- Network Security Services means

  → **Confidentiality**

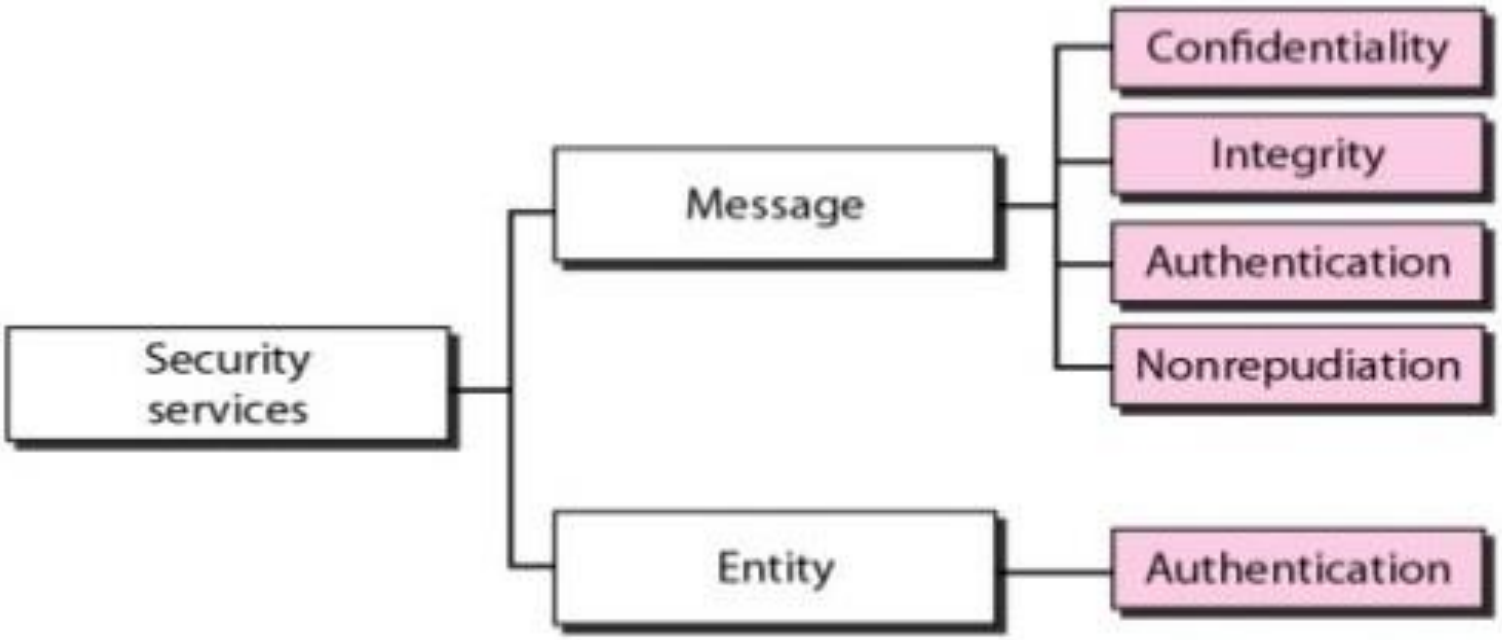
  → **Integrity**

  → **Authentication**

  → **Non-repudiation or Entity authentication**.

The first four services are related to the message exchange using a network while entity authentication service provides identification.

Network Security Services



Message Confidentiality

- The confidentiality or **privacy make sense when the transmitted message must make sense to only the intended** / expected receiver. The message must be garbage to all others.
- To achieve such privacy, the **sender must encrypt / encode the message and the only receiver should decrypt** / decode it.
- Such privacy can be provided using **two ways:**

i) Secret key Encryption / Decryption &

ii) Public key Encryption/Decryption

Encryption / Decryption

Encryption:

- Encryption means that the **sender converts the original information into another form** and

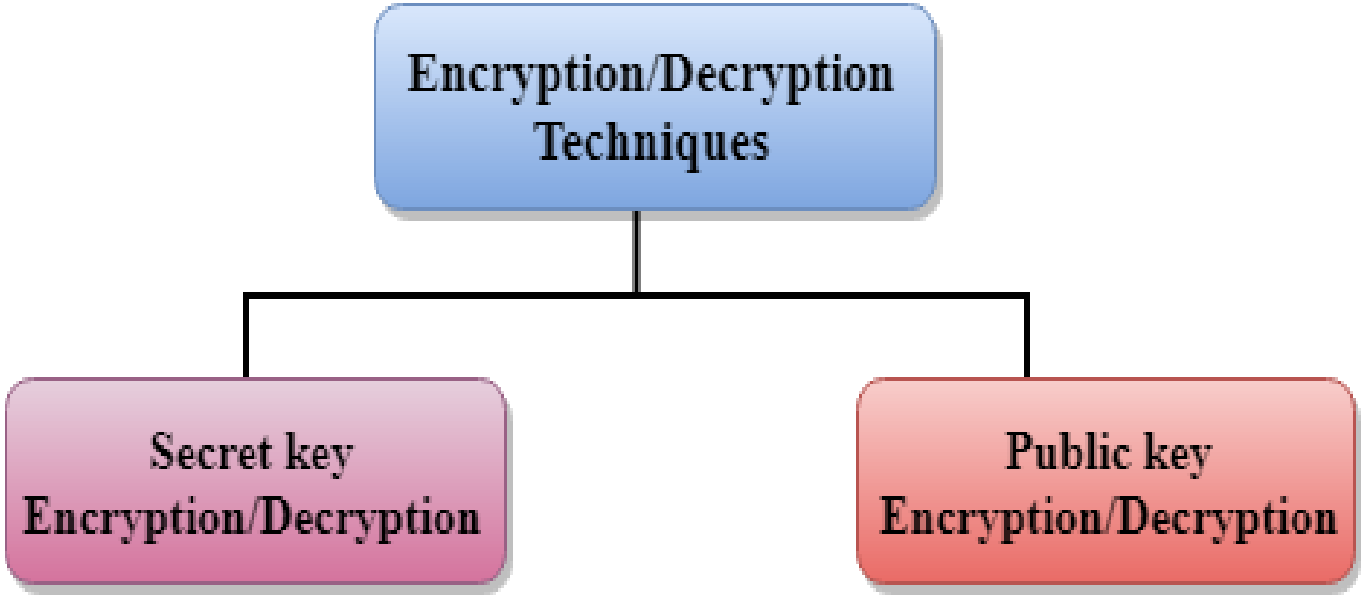
  → **sends the unintelligible message** over the network.

Decryption:

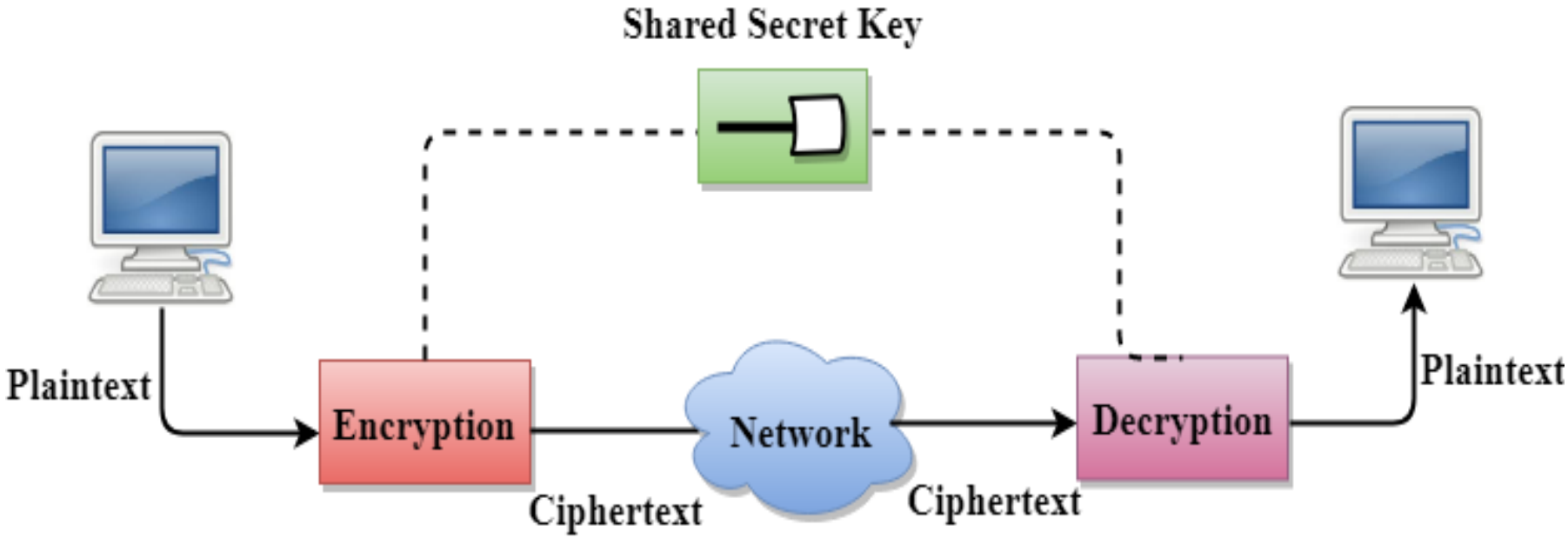
- Decryption **reverses the Encryption process in order to transform the message back to the original form**.
- The data which is to be **encrypted at the sender site is known as plaintext**, and

  → **the encrypted data** is **known as ciphertext**.
- The data is decrypted at the receiver site.

Encryption / Decryption



Secret Key Encryption / Decryption technique



Secret Key Encryption / Decryption Technique

(Contd…)

- In Secret Key Encryption/Decryption technique, the **same key is used by both the parties**, i.e., the sender and receiver.
- The sender uses the **secret key and encryption algorithm to encrypt the data;**
- the **receiver uses this key and decryption algorithm to decrypt the data.**
- In Secret Key Encryption/Decryption technique, **the algorithm used for encryption is the inverse of the algorithm used for decryption**.
- It means that **if the encryption algorithm uses a combination of addition and multiplication,** then **the decryption algorithm uses a combination of subtraction and division**.

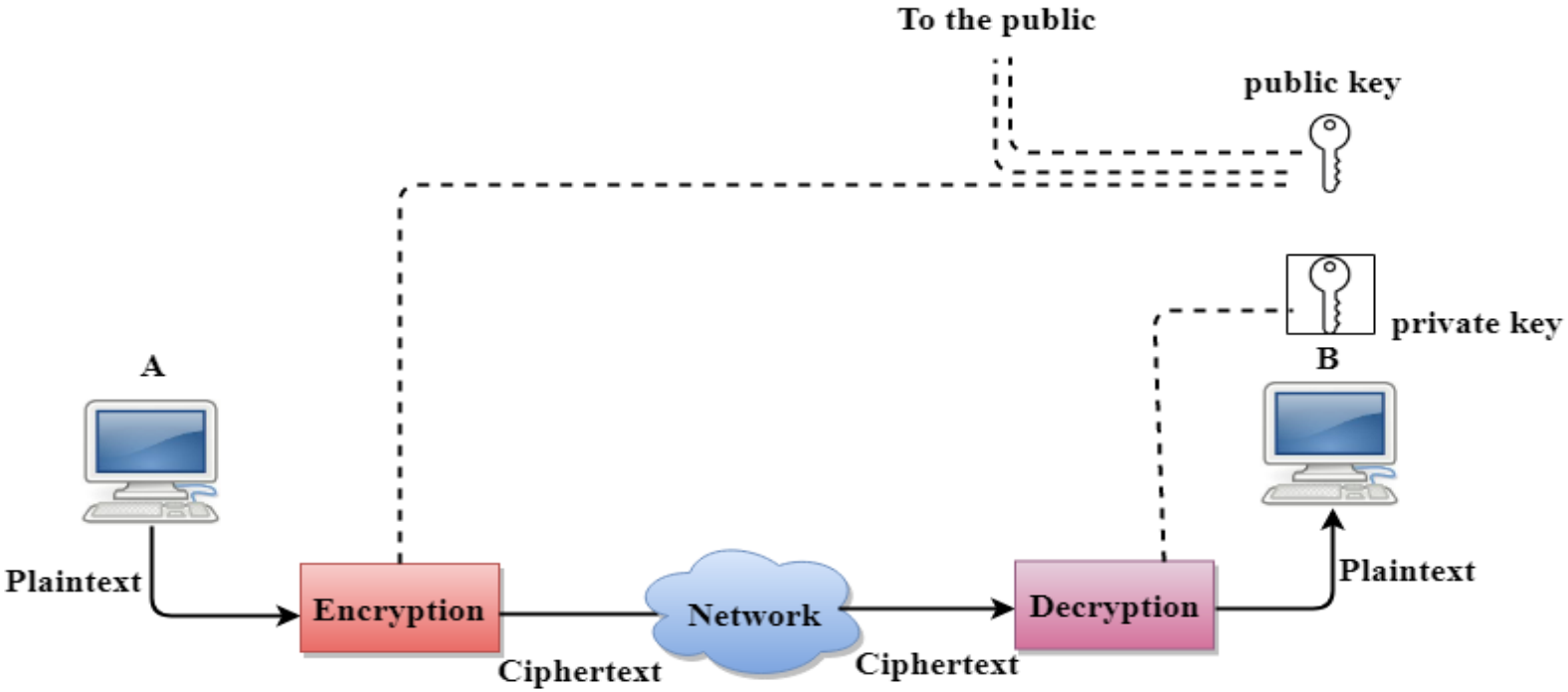
Secret Key Encryption / Decryption Technique

(Contd…)

- The secret key encryption algorithm is also known as **symmetric encryption algorithm** because the same secret key is used in bidirectional communication.
- In secret key encryption/decryption algorithm, the secret code is used by the computer to encrypt the information before it is sent over the network to another computer.
- The secret key requires that we should know which computers are talking to each other so that we can install the key on each computer.

Public Key Encryption/Decryption technique

- There are **two keys** in public key encryption: **a private key and a public key.**
- The **private key is given to the receiver** while the **public key is provided to the public.**



Public Key Encryption/Decryption technique

- In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.
- In public key Encryption/Decryption, **the public key used by the sender is different from the private key used by the receiver**.
- The public key is available to the public while the private key is kept by each individual.
- The **most commonly used public key algorithm is known as RSA**.

Advantages of Public Key Encryption

- The **main restriction of private key encryption is the sharing of a secret key**. A third party cannot use this key.
- In public key encryption, **each entity creates a pair of keys, and they keep the private one and distribute the public key**.
- The **number of keys in public key encryption is reduced tremendously.**
- **For example**, for **one million users to communicate**, **only two million keys are required**, **not a half-billion keys as in the case of secret key encryption.**

Disadvantages of Public Key Encryption

- **Speed:** One of the major disadvantage of the **public-key encryption is that it is slower than secret-key encryption**.
- In secret key encryption, a single shared key is used to encrypt and decrypt the message which speeds up the process while **in public key encryption, different two keys are used, both related to each other by a complex mathematical process.**
- Therefore, we can say that encryption and decryption take **more time in public key encryption.**

Disadvantages of Public Key Encryption

- **Authentication:** A public key encryption **does not have a built-in authentication**.
  - Without authentication, the **message can be interpreted or intercepted without the user's knowledge**.
- **Inefficient:** The main **disadvantage of the public key is its complexity**.
  - If we want the method to be effective, **large numbers are needed**.
  - But in public key encryption, **converting the plaintext into ciphertext using long keys takes a lot of time**.
  - Therefore, the public key encryption algorithms are efficient for short messages not for long messages.

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Define	Secret Key Encryption is defined as the technique that uses a **single shared key to encrypt and decrypt** the message.	Public Key Encryption is defined as the technique that uses **two different keys for encryption and decryption.**

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Efficiency	It is efficient as this technique **is recommended for large amounts of text.**	It is inefficient as this technique is **used only for short messages**.

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Other name	It is also known as **Symmetric Key encryption**.	It is also known as **Asymmetric Key Encryption**.

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Speed	Its speed is **high as it uses a single key** for encryption and decryption.	Its speed is **slow as it uses two different keys,** both keys are related to each other through the complicated mathematical process.

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Algorithms	The Secret key algorithms are **DES, 3DES, AES & RCA.**	The **Public key algorithms are Diffie-Hellman, RSA.**

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Purpose	The **main purpose** of the secret key algorithm is **to transmit the bulk data**.	The main purpose of the public key algorithm is **to share the keys securely**.

Message Integrity

- Message Integrity is **more important than privacy.**
- Instead of **hiding message from other**, it is **more important to keep it safe from any tampering.**
- Message integrity **can be provided using the following methods:**
  A. **Document & Fingerprint**
  B. **Message & Message Digest**

Message Integrity

A. Document & Fingerprint: Fingerprint is a way **to preserve the integrity of a document.**

- If one needs to be sure that the contents of her document will not be illegally changed, she can put her fingerprint at the bottom of the document.
- **To preserve the integrity of a document**, **both the Fingerprint & the Document are needed.**

Message Integrity

B. Message & Message Digest: Message & Message Digest is the **electronic equivalent of Document & Fingerprint**.

- Here, the **message is passed through the Hash algorithm** for integrity preservation of the message.
- The **hash function creates a compressed image of the message** that can be used as a fingerprint.

Message Integrity

Bob receives msg from Alice, wants to ensure:

- message originally came from Alice
- message not changed since sent by Alice

Cryptographic Hash:

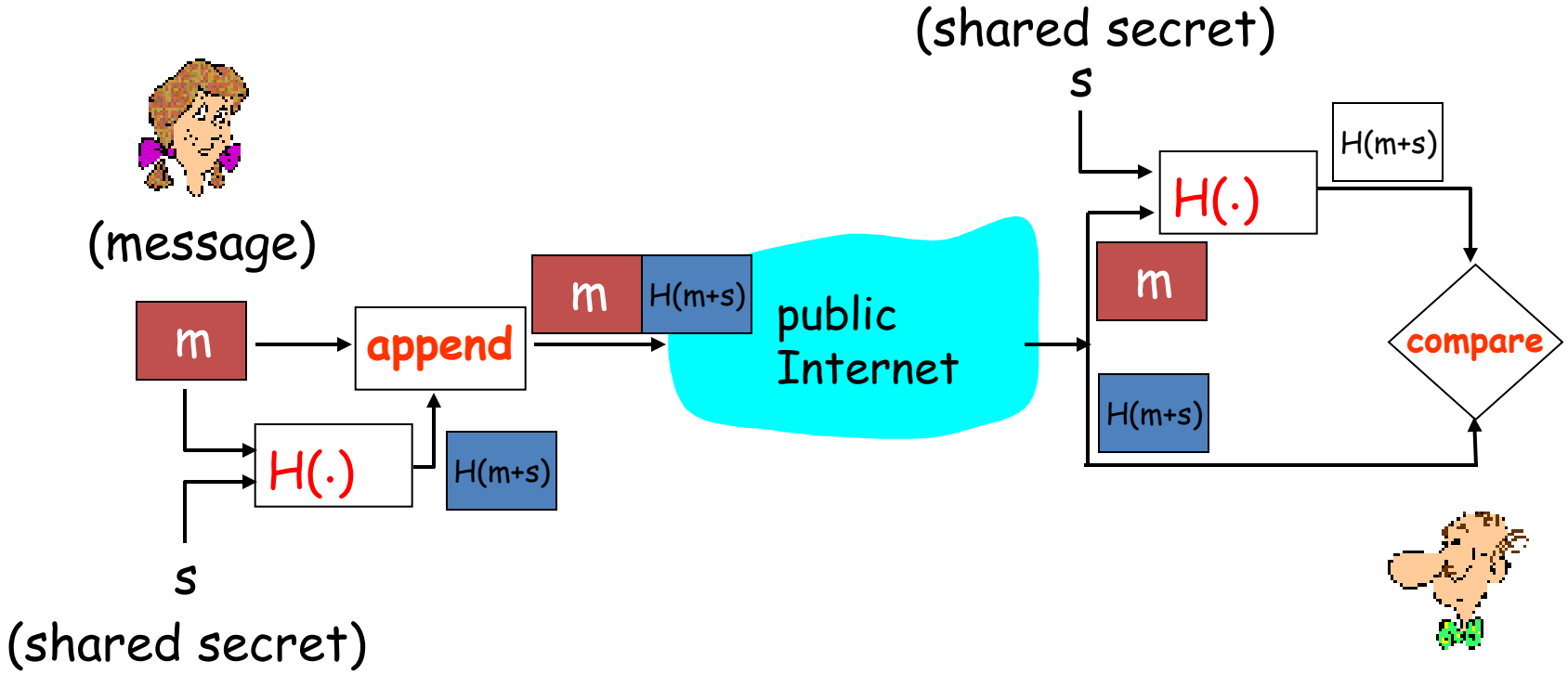
- **takes input m**, produces fixed length value, H(m)
  - **e.g., as in Internet checksum**
- **computationally infeasible** to find two different messages, x, y such that **H(x) = H(y)**
  - equivalently: given m = H(x), **(x unknown)**, **can not determine x.**
  - **note:** Internet checksum *fails* this requirement!

Message Authentication

- Message authentication **ensures the receiver about the sender's identity.**
- A **Hash function can guarantee the integrity of the message** but it **does not authenticate the sender of the message**.
- **To provide message authentication,** the **sender needs to provide proof that he is sending the message** and **he is not an imposter**.

Message Authentication Code

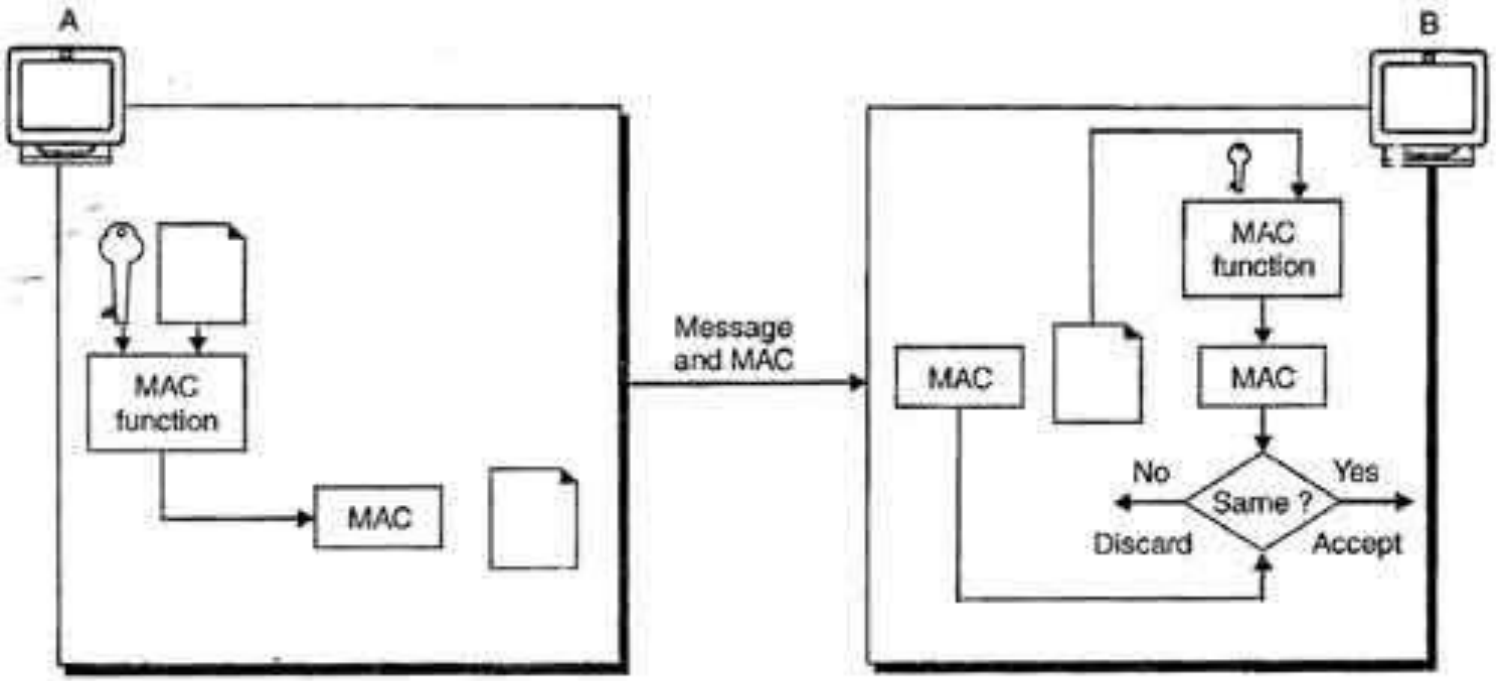
We can **add authenticity of the message in the network** by the following ways:



Message Authentication

- **Message Authentication Code (MAC):** we need to change MDC (Modification Detection Code) provide by Hash function to MAC (Message Authentication Code) to provide message authentication. MDC uses keyless hash function while MAC has keyed hash function. Keyed hash function includes the symmetric key at the time of digest creation between sender and receiver.

Message Authentication



MAC created by A and checked by B.

Message Authentication

- Figure shows how a sender A uses a keyed hash function to authenticate his message and how the receiver B can verify the authenticity of the message.
- This system makes use of a symmetric key shared by A and B.
- A, using this symmetric key and a keyed hash function, generates a MAC.
- A then sends this MAC along with the original message to B.
- B receives the message and the MAC and separates the message from the MAC.

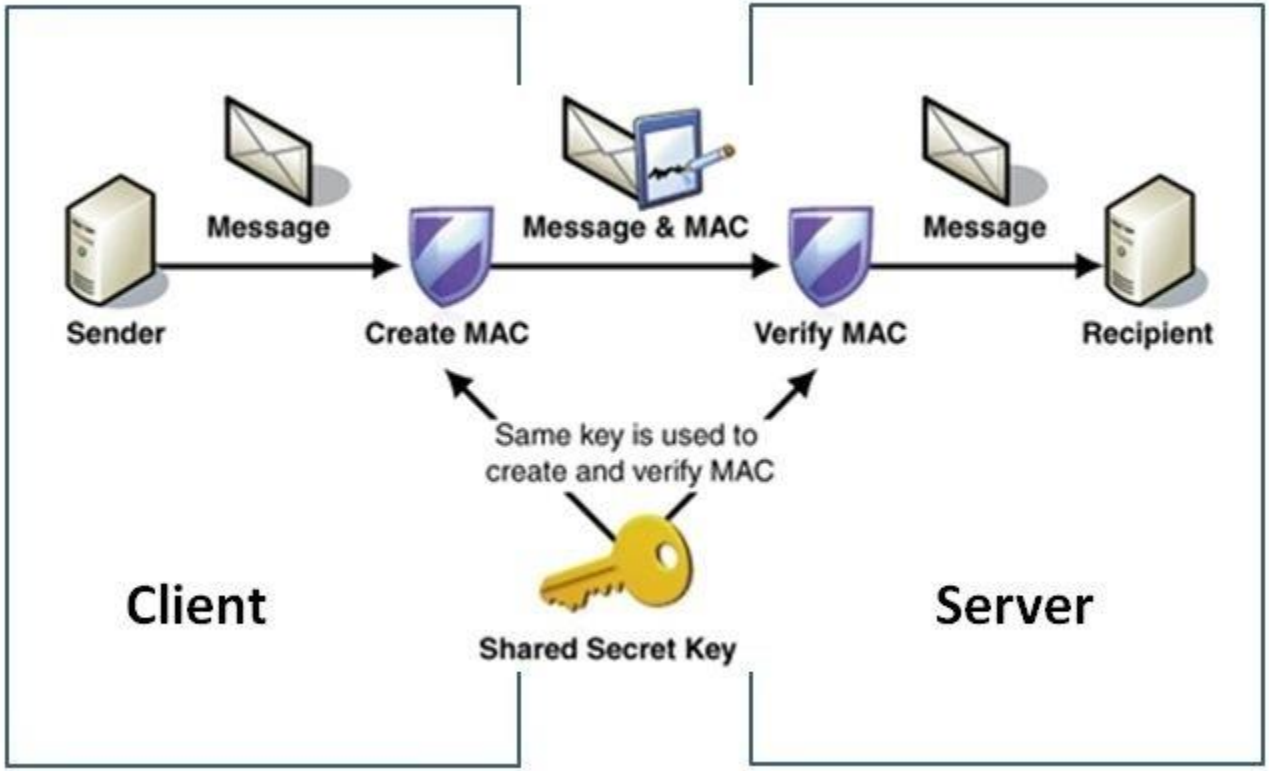
Message Authentication

- B then applies the same keyed hash function to the message using the same symmetric key to get a fresh MAC.
- B then compares the MAC sent by A with the newly generated MAC.
- If the two MACs are identical, it shows that the message has not been modified and the sender of the message is definitely A.

Message Authentication

- **Hashed Message Authentication Code (HMAC):** Hashed MAC or HMAC uses any keyless hash function such as SHA-1. HMAC creates a nested MAC by applying a keyless hash function to the concentration of the message and a symmetric key.

Message Authentication



Digital Signature

Digital Signature

- The Digital Signature is a technique which is used to validate the authenticity and integrity of the message.

Three aspects can be achieved by using a digital signature:

i) Integrity

ii) Authentication

iii) Non-repudiation

- The basic idea behind the Digital Signature is **to sign a document**.

We can sign a document in two ways:

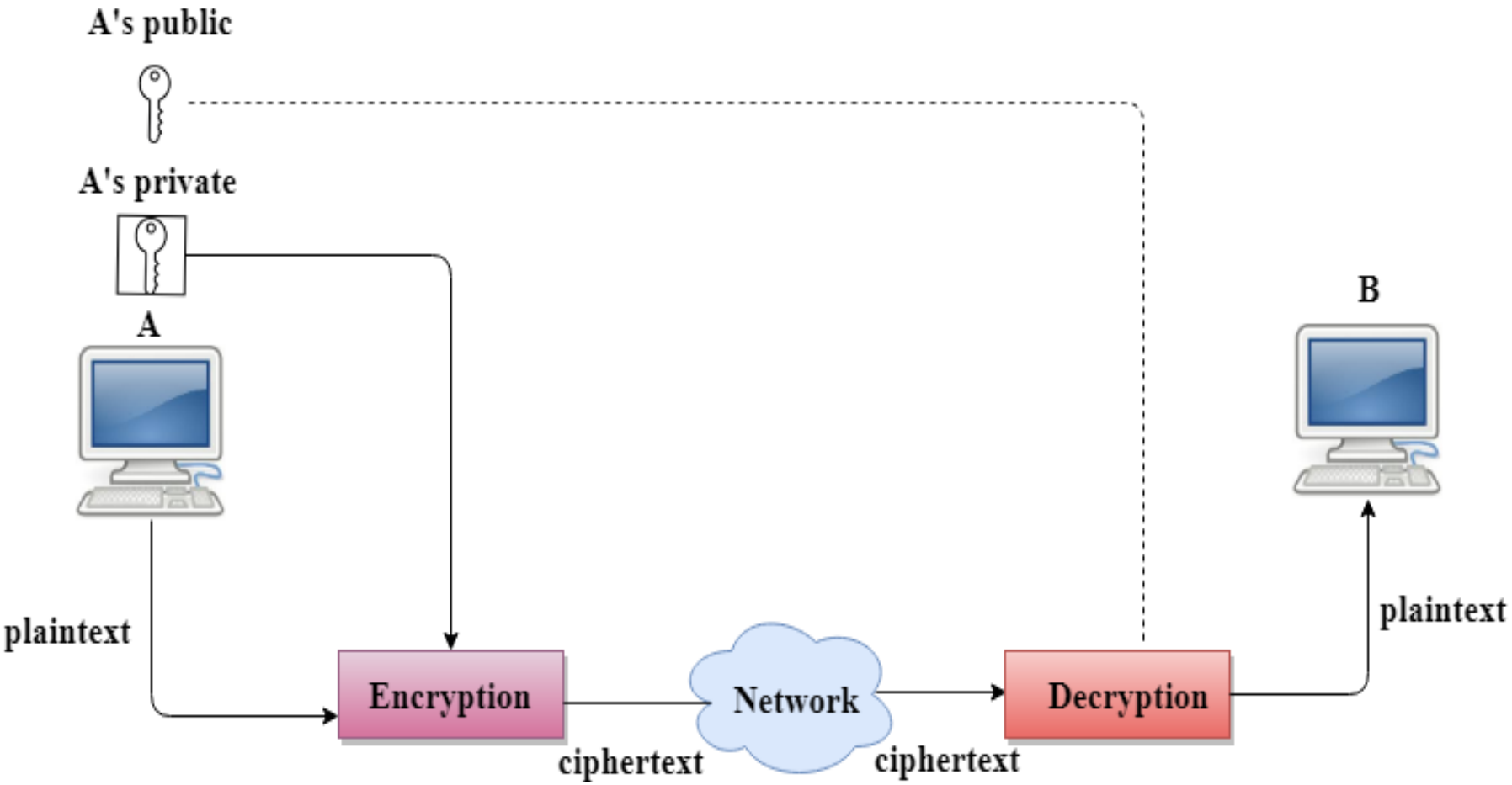
i) to sign a whole document and

ii) to sign a digest.

i) Signing the Whole Document

- In Digital Signature, a **public key encryption technique is used to sign a document**.
- However, the **roles of a public key and private key are different here**.
- The **sender uses a private key to encrypt the message** while the **receiver uses the public key of the sender to decrypt the message**.
- In Digital Signature, the **private key is used for encryption** while the **public key is used for decryption.**
- **Digital Signature cannot be achieved by using secret key encryption.**

i) Signing the Whole Document



Digital Signature is used to achieve the following three aspects:

i) Integrity:

- The Digital Signature **preserves the integrity of a message** because, if any **malicious attack intercepts a message** and **partially or totally changes it,** then the decrypted message would be impossible.

ii) Authentication:

- If an **intruder (user X) sends a message pretending that it is coming from someone else (user A)**,

➔ **user X uses her own private key to encrypt the message.**

➔ **The message is decrypted by using the public key of user A.**

Therefore this makes the message unreadable.

Digital Signature is used to achieve the following three aspects:

iii) Non-Repudiation:

- Digital Signature also provides non-repudiation.
- If the **sender denies sending the message**,

➔ **then her private key corresponding to her public key is tested on the plaintext.**

- If the **decrypted message is the same as the original message**, then **we know that the sender has sent the message.**

ii) Signing the Digest

- **Public key encryption is efficient if the message is short.**
- **If the message is long, a public key encryption is inefficient to use.**
- The **solution to this problem is** to **let the sender sign a digest of the document instead of the whole document.**
- The **sender creates a miniature version (digest) of the document** and **then signs it**, the **receiver checks the signature of the miniature version.**

ii) Signing the Digest

- **The hash function is used to create a digest of the message**.
- The **hash function creates a fixed-size digest from the variable-length message.**
- **The two most common hash functions** used:

i) MD5 (Message Digest 5) and

ii) SHA-1 (Secure Hash Algorithm 1).

The **first one produces 120-bit digest** while the **second one produces a 160-bit digest.**

ii) Signing the Digest

A **hash function must have two properties** to ensure the success:

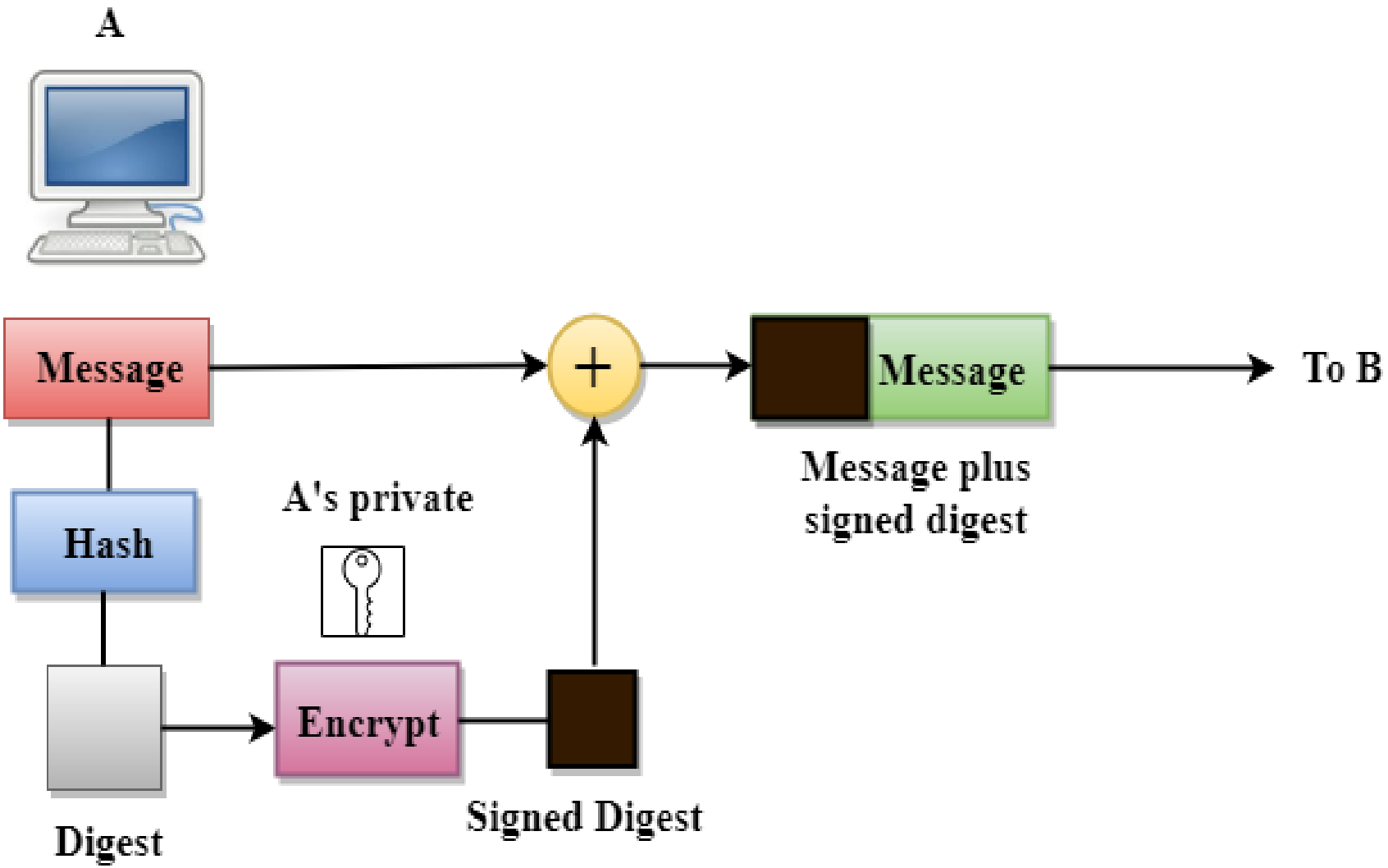
a) First, the **digest must be one way**, i.e., the **digest can only be created from the message but not vice versa**.

b) Second, **hashing is a one-to-one function**, i.e., **two messages should not create the same digest.**

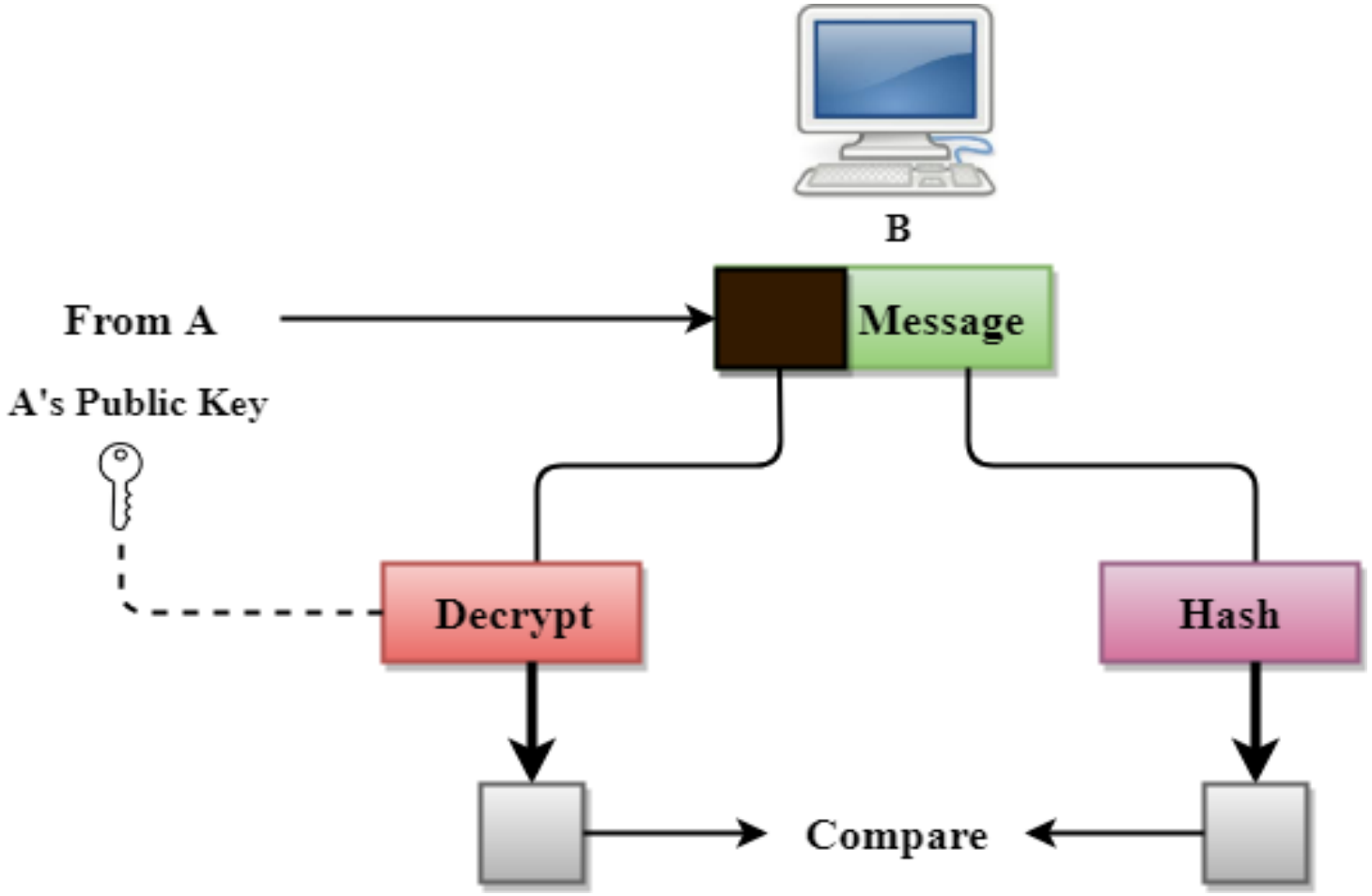
Following are the steps taken to ensure security:

- The **miniature version (digest) of the message is created** by using a hash function.
- The **digest is encrypted by using the sender's private key.**
- After the digest is encrypted, then **the encrypted digest is attached to the original message and sent to the receiver.**
- The **receiver receives the original message and encrypted digest** and separates the two.
- The **receiver implements the hash function on the original message to create the second digest,** and
- **it also decrypts the received digest by using the public key** of the sender.
- **If both the digests are same, then all the aspects of security are preserved.**

At the Sender site



At the Receiver site



Message Non-repudiation

- Message **Non-repudiation means that a sender must not be able to deny sending a message** that he/she did send in fact.
- Let us take an **example of a bank transaction**. When a customer sends a message to withdraw money from his account, the bank must have proof that the customer actually requested this transaction.
- MAC can provide message authenticity & integrity but there is a problem of sharing a symmetric key between sender and receiver.
- This can be resolved by Digital signature. **Nonrepudiation can be provided using a trusted party.**

Message Non-repudiation

- **Digital Signature:** Digital Signature is an electronic signature **that can prove the authenticity of the sender to receiver**.
- Digital Signature is a proof to the recipient that the message is coming from the authenticated person.
- It can use a pair of asymmetric keys: **a private and a public** key. The **digital signature can be achieved in two ways:**

Message Non-repudiation

a) **Signing the document**: It is easier but less efficient way. Encrypting a document with the private key of the sender and decrypt with the public key of the sender.

b) **Signing the digest of the document**: the digest of the message is signed instead of signing the original message. The sender can sign the message digest and receiver can verify the message digest. The effect is the same.

Entity Authentication

Entity Authentication

- In this service of network security, the **entity or user is verified before accessing the system resources**.
- An **entity can be a person, process, client or server**.
- The **entity whose identity needs to be verified is called CLAIMANT**.
- The **party that tries to prove the identity of the claimant is called the VERIFIER**.
- In entity authentication, the **claimant must identify herself/himself to the verifier with one of the three kinds of witnesses:**

Entity Authentication

a) **Something known:** This is a secret known only by the claimant **that can be checked by the verifier.**

➔For example, pin, password, secret key, and private key.

a) **Something possessed:** This is something that can prove claimant's identity.

➔For example, passport, driving license, credit card, smart card, identity card.

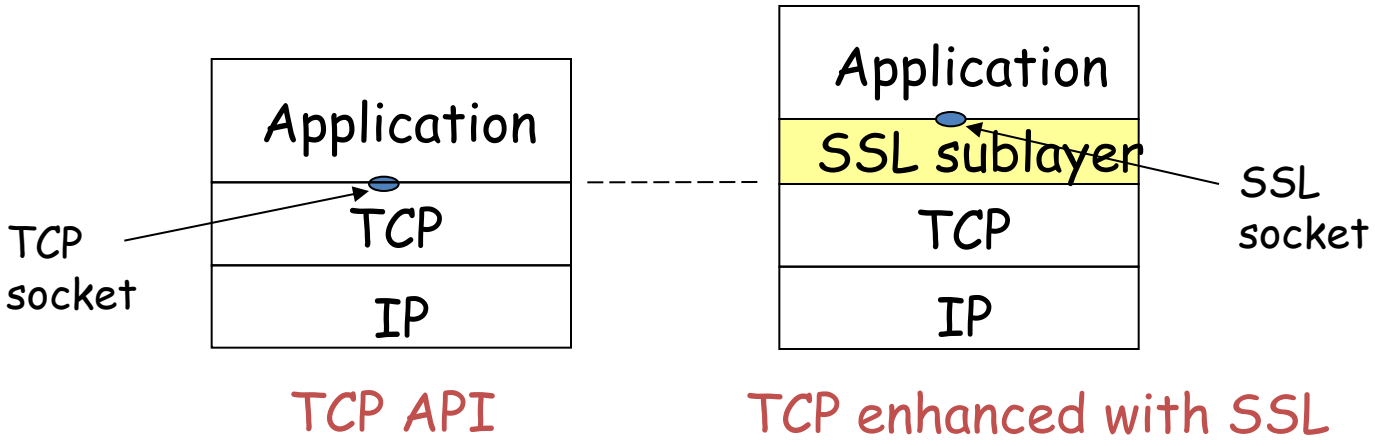
a) **Something inherent:** This is an inherent characteristic of the claimant.

➔ For example, fingerprint, voice, conventional signature, retina pattern, facial characteristics, handwriting.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL)

- Encrypt the web traffic between two sites, so no one can listen in and get credit card numbers
- Uses something called “Secure Sockets Layer” (SSL)



Secure Sockets Layer (SSL)

The Implementation

- The secure web site includes a digital certificate signed by some certificate authority.
- The certificate includes the server name, its public key, IP number, and an expiration date.
- It is typically signed with a 1024 bit key by the CA

Go to chrome://settings.

1.On the left, click Privacy and security.
2.Click Security.
3.Scroll to Advanced.
4.Click Manage certificates.
5.In the list, find the newly-added CAs.

Secure Sockets Layer (SSL)

How It Works

- The browser reads the site certificate; if it is signed by one of the trusted certificate authorities, browser accepts the certificate as valid
- If the certificate is signed by some unknown certificate authority, Netscape will ask you if you want to trust the guy who signed it
- The browser negotiates a secure session using something like the following protocol:

  1. A->B: hello
  2: B->A: Hi, I'm Bob, bobs-certificate
  3: A->B: prove it
  4: B->A: Alice, This Is bob
  { digest[Alice, This Is Bob] } bobs-private-key
  5: A->B: ok bob, here is a secret {secret} bobs-public-key
  6: B->A: {some message}secret-key

Secure Sockets Layer (SSL)

How It Works

Step 1: your browser introduces itself to the secure server

Step 2: the server responds by sending back a message with the certificate included

Step 3: Your browser tells the secure site to prove its identity, that it really is who it says it is.

Step 4: The secure server proves who it is by creating a message for the browser, generating a “fingerprint” of that message, and encrypting the “fingerprint” with the private key that is matched to the public key in the certificate. The browser generates the “fingerprint” for the message itself, then decrypts the “fingerprint” generated by the server using the public key provided in the certificate.

Secure Sockets Layer (SSL)

How It Works

At this point the browser is sure that the server is how it says it is. It can send it secret messages encrypted with the public key provided in the certificate. The server (and only the server) can decrypt these messages, because only it has the private key.

You'll use a completely different key for encrypting traffic to the web site every time you connect. This makes cracking communication more difficult; you need to discover the keys for every session rather than just one key.

IPSec

IPSec

- **IP Sec** (Internet Protocol Security) is an Internet Engineering Task Force (IETF) **standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality**.
- It also defines the encrypted, decrypted, and authenticated packets.
- The **protocols needed for secure key exchange and key management** are defined in it.

IPSec

Uses of IP Security

- **To encrypt application layer data.**
- To provide **security for routers sending routing data** across the public internet.
- To provide **authentication without encryption,** like to authenticate that the data originates from a known sender.
- To **protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted**, as with a Virtual Private Network(VPN) connection.

IPSec

Features of IPSec

1.Authentication: IPSec provides authentication of IP packets **using digital signatures or shared secrets**. This helps ensure that the packets are not tampered with or forged.

2.Confidentiality: IPSec provides confidentiality by **encrypting IP packets**, preventing eavesdropping on the network traffic.

3.Integrity: IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.

4.Key management: IPSec provides key management services, including **key exchange and key revocation**, to ensure that cryptographic keys are securely managed.

Features of IPSec

5. Tunneling: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).

6. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.

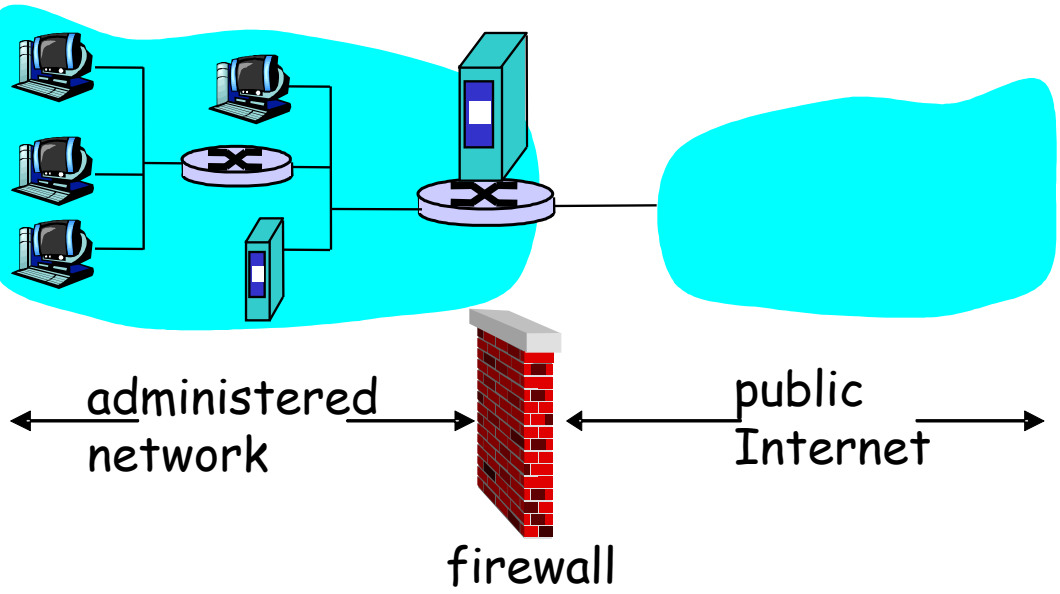
7. **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Firewalls

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Firewalls: Why

- prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections
- prevent illegal modification / access of internal data.
  - e.g., attacker replaces homepage with something else
- allow only authorized access to inside network (set of authenticated users/hosts)

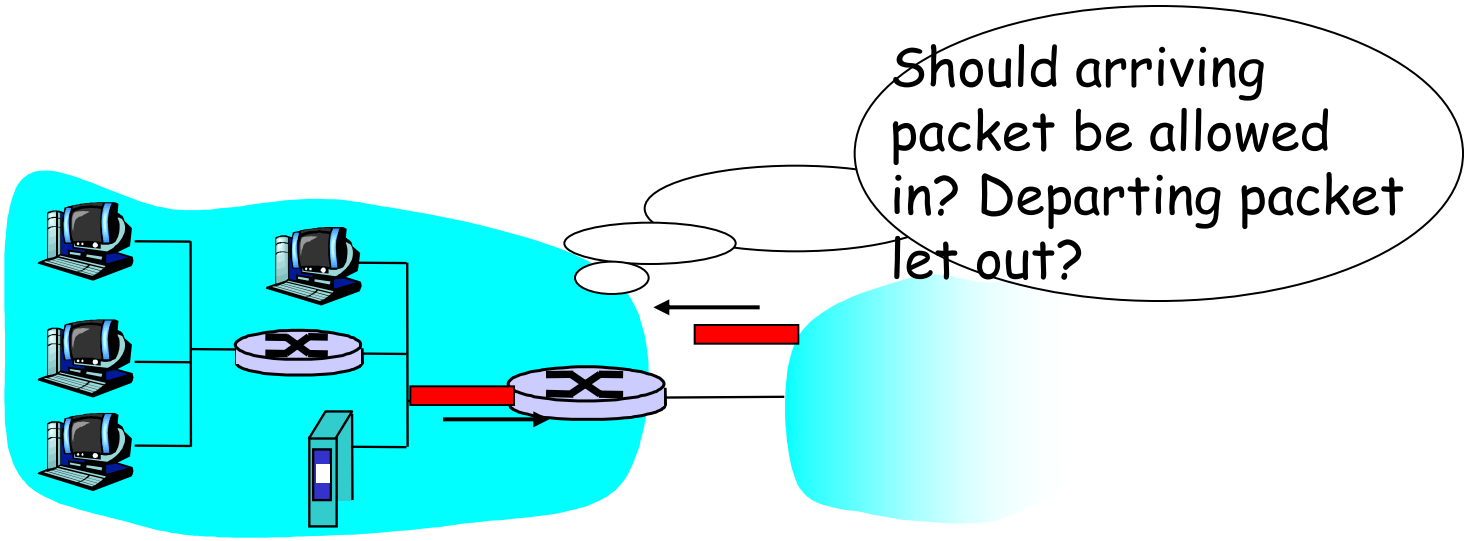
Three types of firewalls:

i) stateless packet filters

ii) stateful packet filters

iii) application gateways

i) Stateless packet filtering



- internal network connected to Internet via **router firewall**
- router **filters packet-by-packet, decision to forward/drop packet based on:**
  - **source IP address, destination IP address**
  - **TCP/UDP source and destination port numbers**
  - **ICMP message type**
  - **TCP SYN and ACK bits**

i) Stateless packet filtering: example

- **example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23 (Telnet)**
  - **all incoming, outgoing UDP flows and telnet connections** are blocked.

- **example 2: Block inbound TCP segments with ACK=0.**
  - **prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.**

i) Stateless packet filtering: more examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

ii) Stateful packet filtering

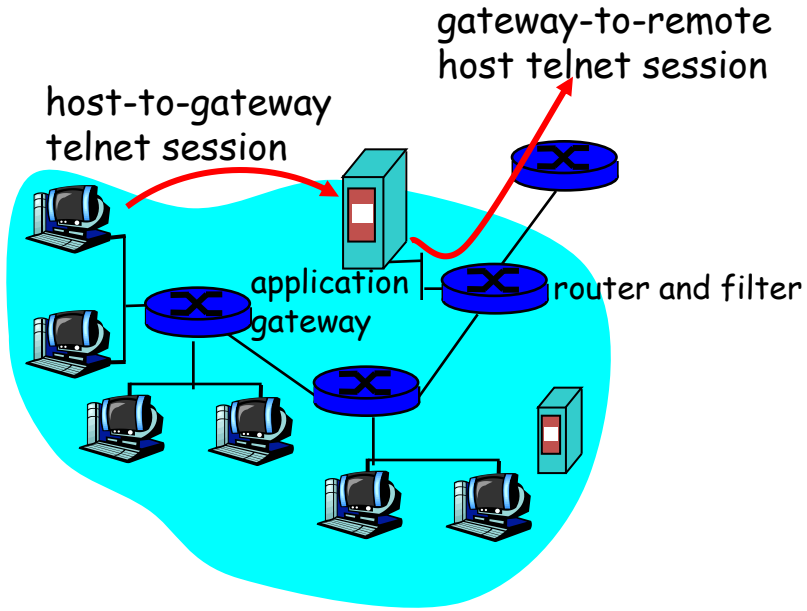
- **stateless packet filter: heavy handed tool**
  - **admits packets that "make no sense,"** e.g., **dest port = 80, ACK bit set, even though no TCP connection established**:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- ***stateful packet filter:*** **track status of every TCP connection**
  - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets "makes sense"
  - **timeout inactive connections at firewall: no longer admit packets**

iii) Application gateways

- **filters packets on application data as well as on IP/TCP/UDP fields.**
- **example: allow select internal users to telnet outside.**



1. require **all telnet users to telnet through gateway**.
2. **for authorized users, gateway sets up telnet connection** to dest host. Gateway relays data between 2 connections
3. router **filter blocks all telnet connections not originating from gateway**.

Limitations of firewalls and gateways

- **IP spoofing:** router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- **tradeoff:** degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.