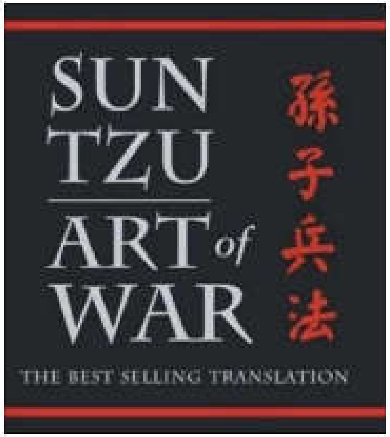
UNIT 4:Network Security

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

(*The Art of War,* Sun Tzu)



SUN TZU

ART of WAR

孫子兵法

THE BEST SELLING TRANSLATION

Introduction

- Network Security is the protection of Information and systems and hardware that use, store, and transmit 2 that information
- The protection of network, controlling access from unauthorized or untrusted network is known as network security.
- In other words, network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, thereby creating a secure platform for computers users and programs to perform their critical functions within a secure environment.

- Network security consists of policies and practices adopted to prevent and monitor unauthorized access.
- Network security is typically handled by a network administrator who implements the security policy.

Network Security and its growth are driven by various factors..!!

- Internet Connectivity is 24/7 and is Worldwide.
- Increase in Cyber Crime.
- Proliferation of Threats.
- Impact on Business and Individuals
- Sophistication of Threats.
- Legislation and Liabilities

Increase in Cyber Crime

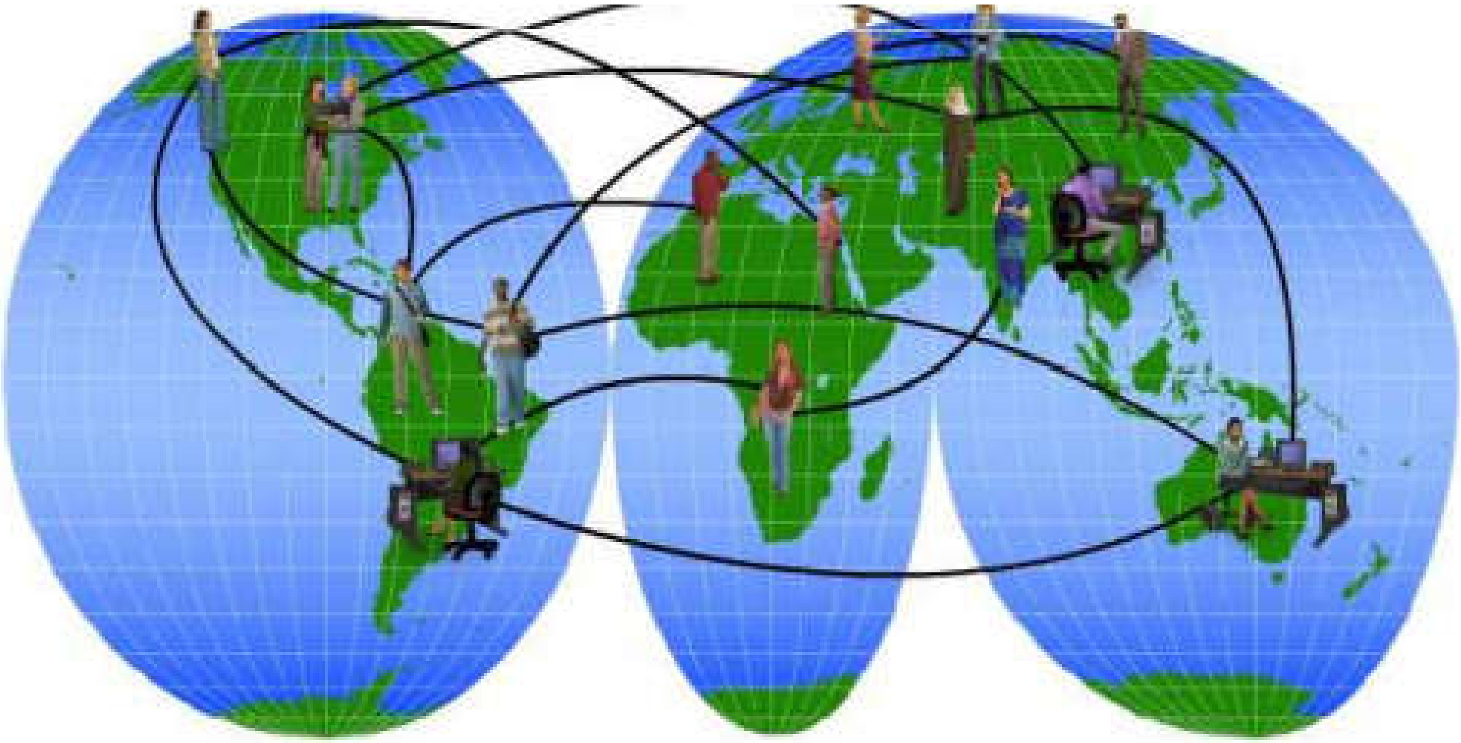
- WASHINGTON, D.C. -- An Estimated 3.6 million households, or about 3 percent of all households in the nation, learned that they had been the victim of at least one type of identity theft during a six-month period , according to the Justice Department’s Bureau of Justice Statistics

Business Impact

- Decrease in Productivity
- Loss of Sales Revenue
- Release of Unauthorized sensitive data
- Threat of Trade secrets or formulas
- Compromise of Reputation and trust
- Threat to environmental and safety systems
- Loss of time

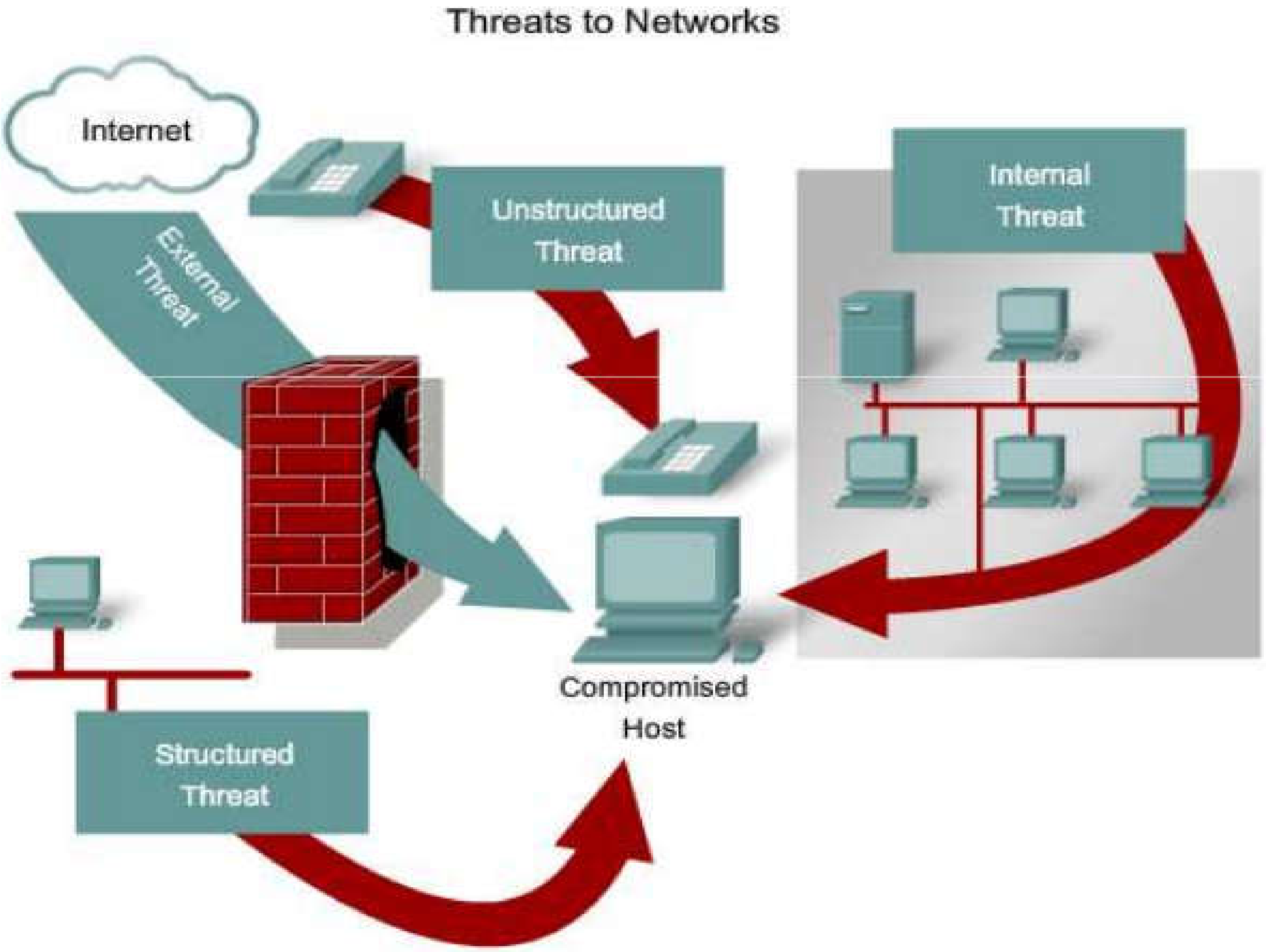
Proliferation of Threats

- Threat Landscape is very dynamic
- Necessary to adopt newer security measures

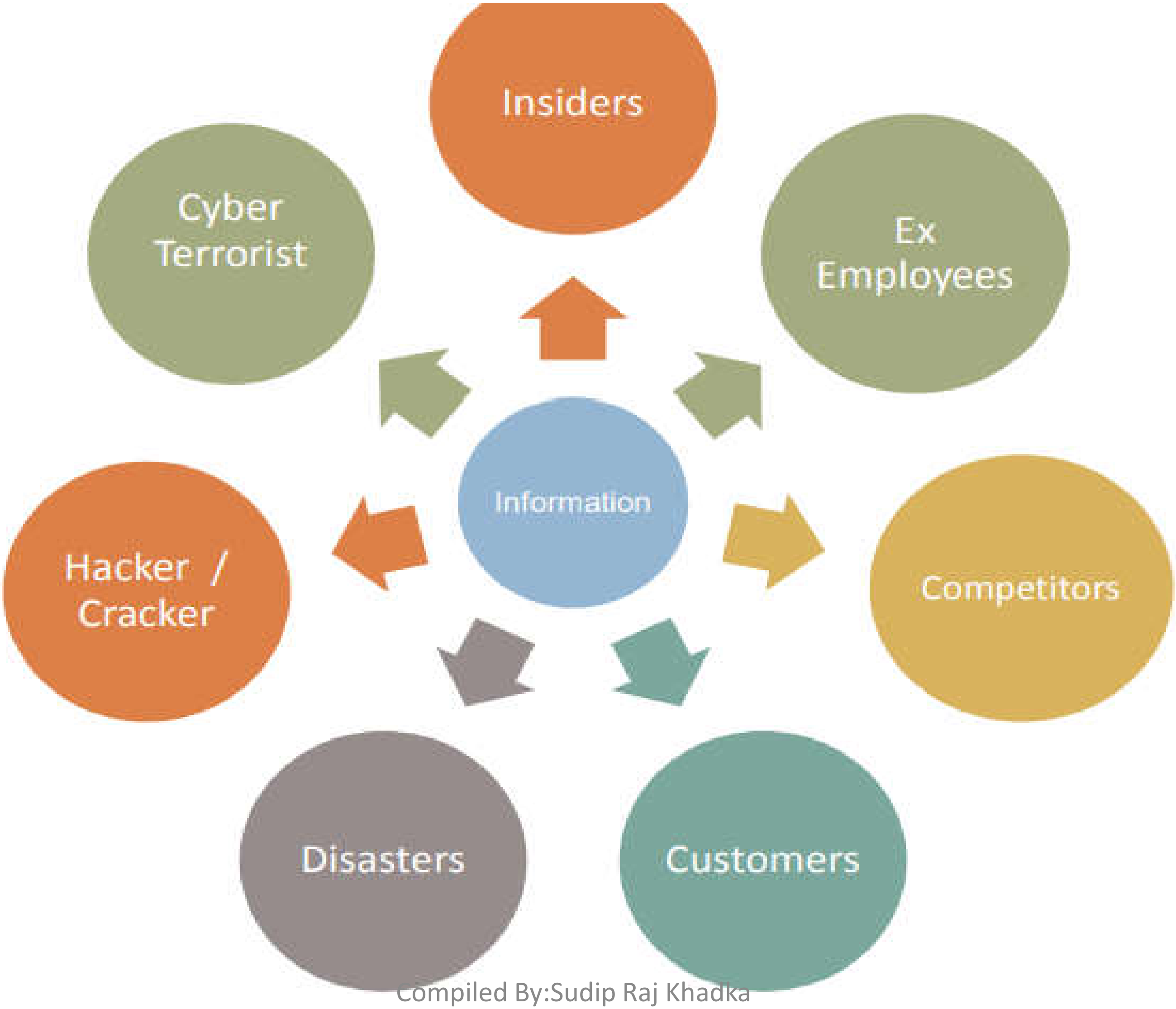


“The World is Flat”- Thomas L. Friedman

Sophistication of Threats



Who Attacks on Information ??



Information

Insiders

Ex Employees

Competitors

Customers

Disasters

Hacker / Cracker

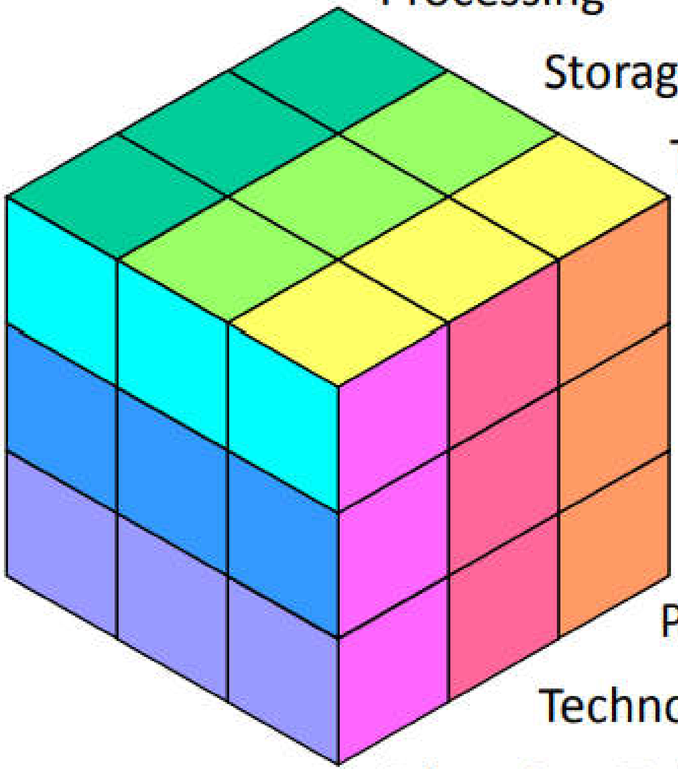
Cyber Terrorist

Information Security Goal:::

- **Confidentiality**
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes.
- **Integrity**
  - The protection of system information or processes from intentional or accidental modification.

- **Availability**
  - The assurance that systems and data are accessible by authorized users when needed

Information Security Model



Processing

Storage

Transmission

Information State

Confidentiality

Integrity

Availability

Informaion Security Properties

Policy and Procedures

Technology

Education, Training, and Awareness

Security Measure

Security threat

- Security threat is a possible danger that might exploit vulnerabilities in a computer system to breach security and thus cause possible harm
- Vulnerability is weakness in a computer system that can be exploited by a threat.
- A threat is something that may or may not happen, but has the potential to cause serious damage.

Compiled By:Sudip Raj Khadka

- A threat can be either intentional or accidental
- Intentional threats are normally due to intelligent persons like hacker or crackers
- On the other hand accidental threats are due to malfunctioning of computers or due to natural disaster or due to mistakes done by computer users

There are four types of security threats to consider

a. Interception:

- Refers to the situation that an unauthorized party has gained access to a service or data. A typical example of interception is where communication between two parties has been overheard by someone else
- This is an attack on confidentiality. Example : Wiretapping to capture data in a network.

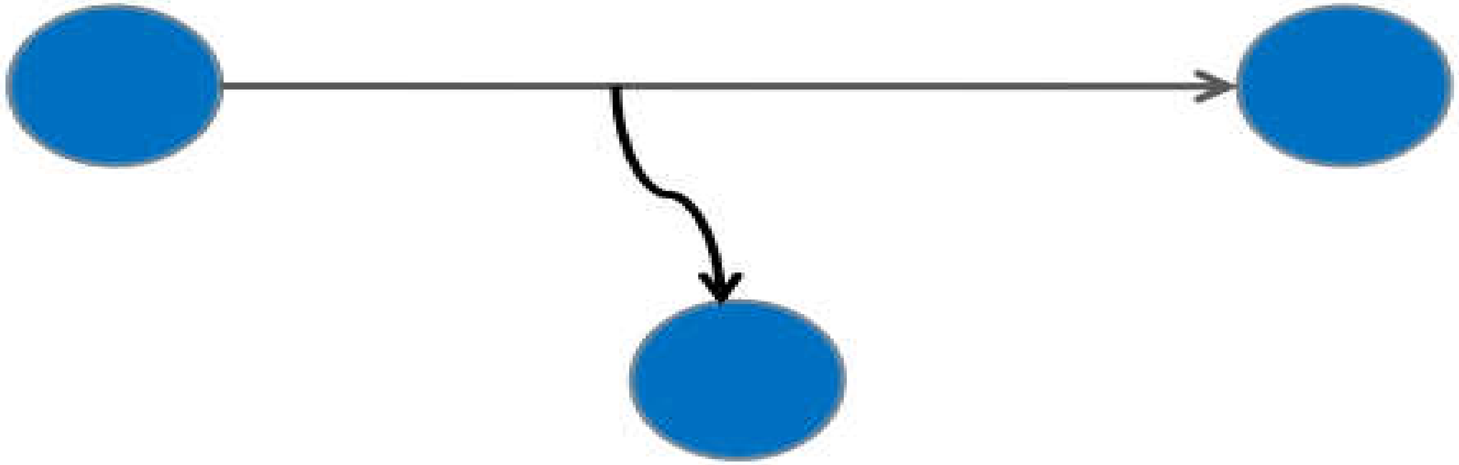
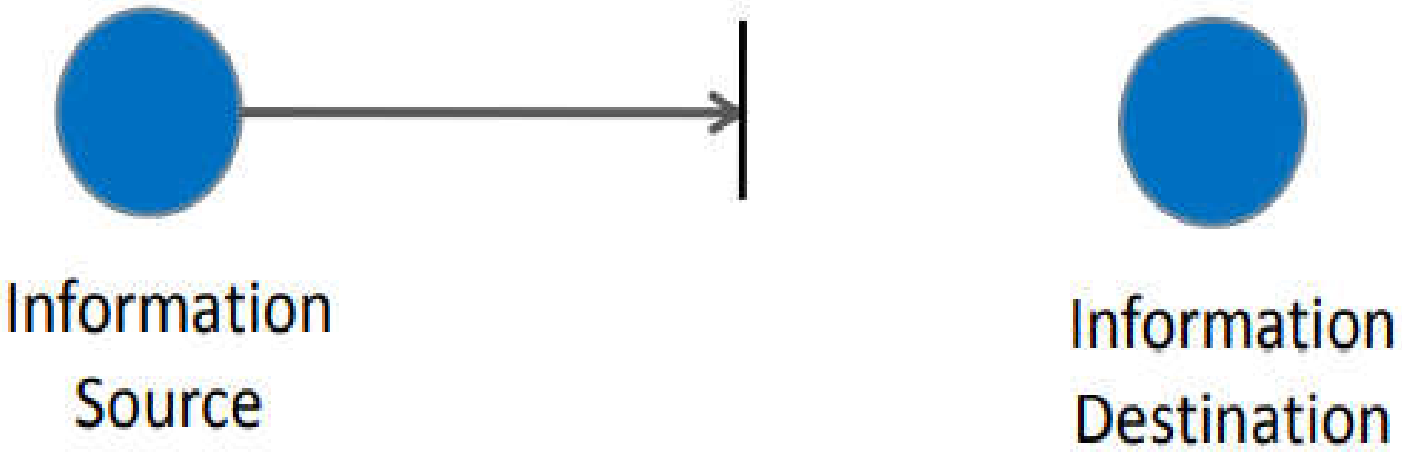


Fig : Interception

- Interruption:
  - Refers to the situation, in which services or data become unavailable, unusable or destroyed
  - This is an attack on availability. Example : Cutting of a communication line.



Information Source

Information Destination

Fig : Interruption

Modification:

- Modification involve unauthorized changing of data
- This is an attack of Integrity Example : Changing values in a data file

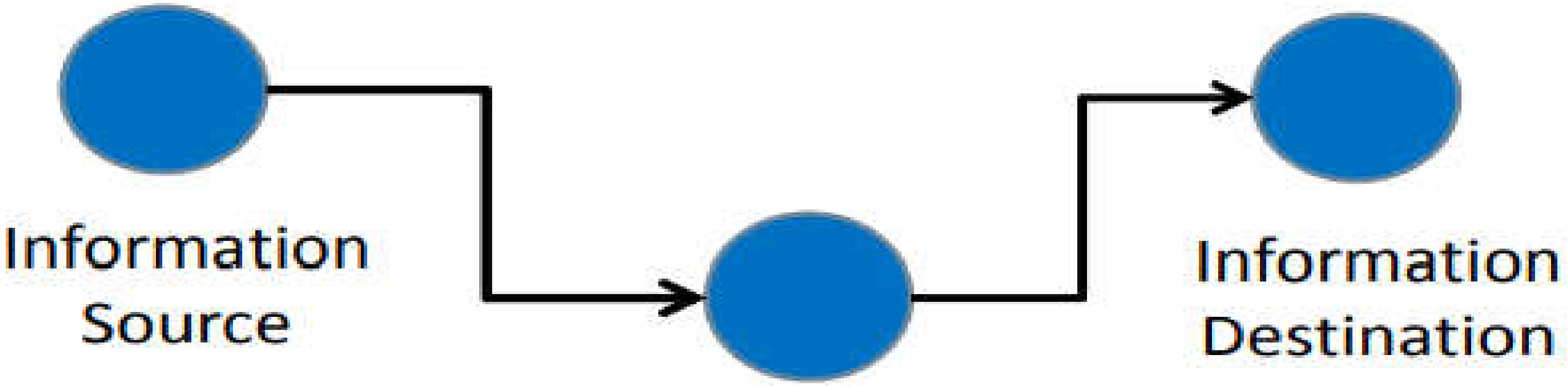


Fig : Modification

- Fabrication:
  - Refers to the situation in which additional data or activities are generated that would normally not exist.
  - This is an attack on authenticity
  - Example : Insertion of fake messages in a network.

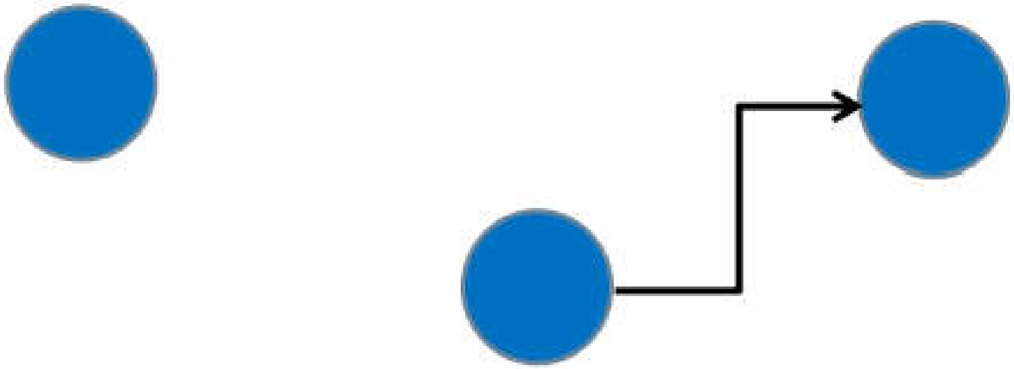


Fig : Fabrication

Security Attack

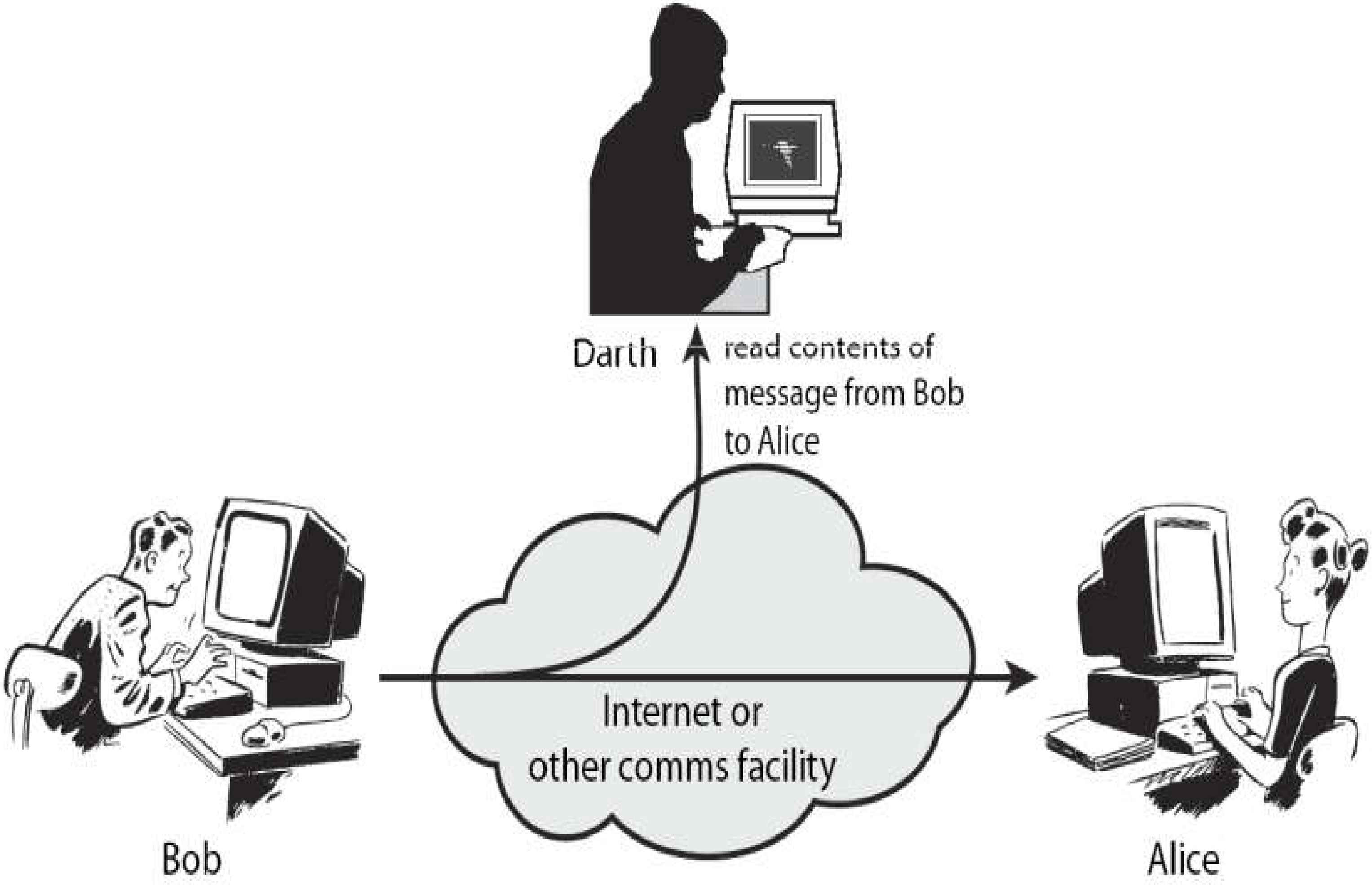
Security Attacks => Exploitation of Vulnerability

- An attack is any attempt to destroy, alter, disable steal or gain unauthorized access or make unauthorized use of an asset
- Intruders first of all analyze our environment and collect information in order to exploit vulnerabilities and then perform desired type of attack in our computer system.
- E.g. intruders can install harmful malicious software in our computer without our knowledge

Types of Attack

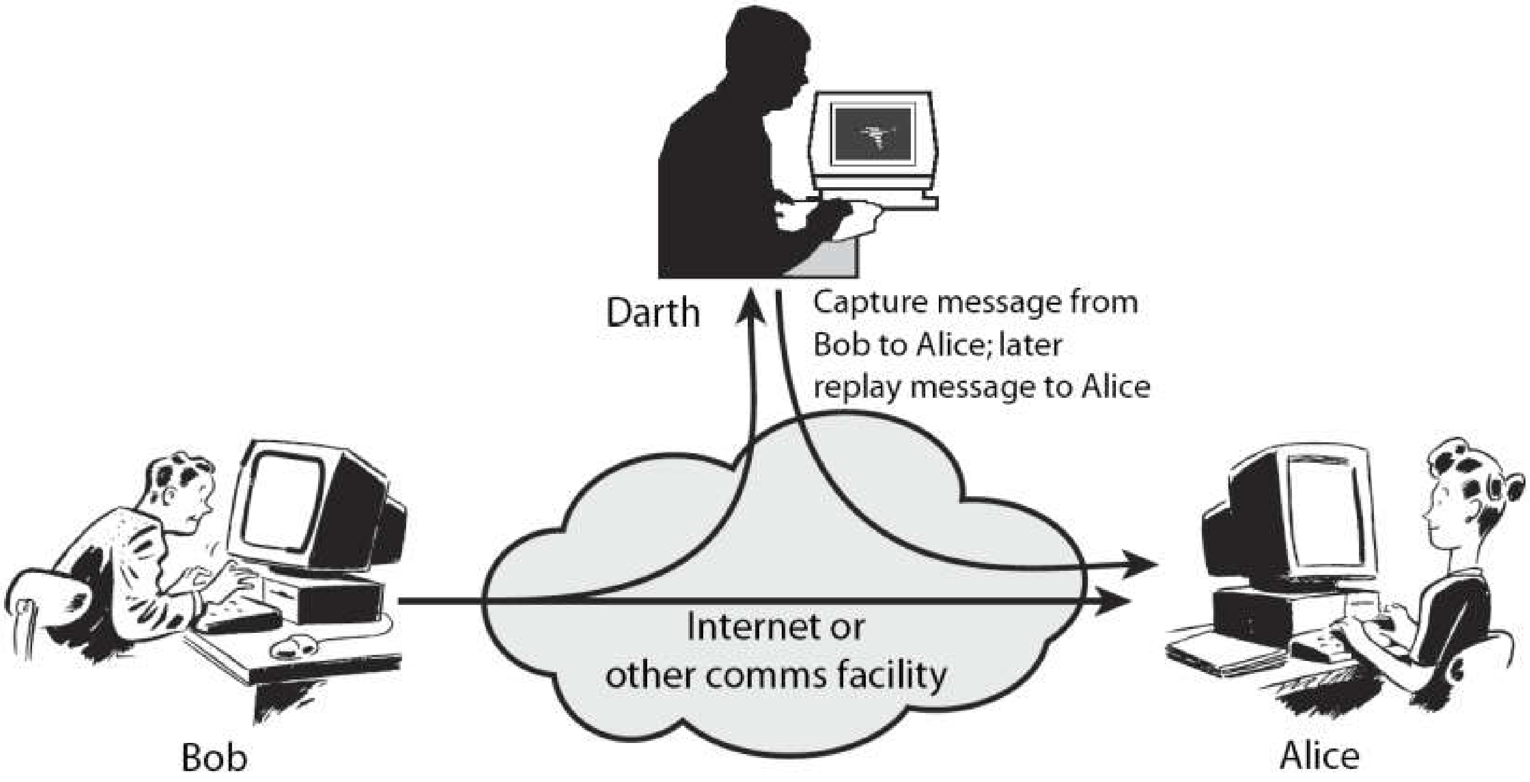
Passive attack: An attack that attempt to learn or make use of information from the system but does not affect system resources is called passive attack. Passive attacks result in the disclosure of information or data files to an attacker without the knowledge of user.

Passive Attack


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- Active attack: An attack that attempt to alter system resources or affect their operation is called active attack

Active attack



Security Policy and Mechanism

- Security policy is a statement about what is allowed and not allowed to do in a system
- Security mechanism is a procedure how to implement the security policy
- A mechanism is more about how a particular policy is done where as a policy is more about what needs to be done

- In practice, policies are rarely so precise, they normally describe in English what users and staff are allowed to do.
- Mechanisms are designed to detect, prevent or recover from security attacks.

Security Services

- Security service is a service provided by a layer of communicating system, which ensures adequate security of the system or data transfer.
- **Network Security Services** (**NSS**) is a set of libraries designed to support cross-platform development of security-enabled client and server applications

- Some of the categories of security services are:

Authentication:

- ➢ It is the act of verifying user’s identity. A user need to be authenticated before providing access to the system.
- ➢ Assurance that the communicating entity is the one claimed

Authorization:

- It is the act of defining privilileges of authenticated user.
- Authorization controls access to objects.
- Prevention of the unauthorized use of a resource

Data confidentiality:

- It is a property that ensures that information is not made available or disclosed to unauthorized individuals
- Protection of data from unauthorized disclosure

- **Data integrity:**

➢ It is a property that ensures that data cannot be modified in unauthorized way.

➢ Service to ensure Integrity (originality) of transmitted message

Non-Repudiation

➢ Ensuring the denial of receipt and transmission

E-commerce security concern

- Security concerns in e-commerce can be divided into two categories:

➢ Client-server security

➢ Data and transaction security

Client-server security

a. Client-server security: In the client-server network, the security problems are as follows:

- Physical security holes: it results when individuals gain unauthorized physical access to a computer
- Software security holes: it results when badly written programs or software are compromised into doing thing they should not do.
- Inconsistent usage holes: it results when a system administrator assembles a combination of hardware and software such that the system is seriously weak from a security point of view.

- The several types of security methods or network protection methods to client-server network are as follows:

i. Trust Based System (TBS): TBS means to trust everyone and do nothing extra for protection. There is no restriction to access information in private network as long as the users are trustworthy and all privileges are granted to them.

ii. Password scheme: A password is information associated with an entity that confirms the entity’s identity.

iii. Smart card based authentication: a smart card is a small plastic card, containing an embedded microchip that can be programmed to store specific user authentication information. The chip on a smart card can store multiple identification factors of a specific user (i.e. password, fingerprint)

iv. Biometric system: biometric authentication is a type of system that relies on the unique physiological or behavioral characteristic of individuals to verify identity for secure access to electronic system.

Some of the widely used physiological or behavioral characteristics are: face, fingerprint, voice, retinal information etc.

Biometric authentication system compare the current biometric data capture to stored authentic data in a database. In both samples of the biometric data match, authentication is confirmed and access is granted.

Among all authentication system, a biometric is the most secure and convenient authentic tool. It cannot be borrowed or stolen

v. Security Through Obscurity (STO): STO is the belief that a system of any sort can be secure as long as nobody outside of its implementation group is allowed to find out anything about its internal mechanism

Hiding account passwords in binary files or script with the assumption that “nobody will ever find them) is a case of STO.

So, STO provides security by hiding information

Emerging client server Security Threat:

- **Threat to client**
  - Software agents and malicious code threat
    - Software agent resembles a more traditional virus.
    - It is an executable program that has the ability to move from machine to machine and invoke itself without external influence.
    - Malicious code
      - Virus
      - Trojan horse
      - Worm

Threat to server

- Server security is as important as network security because servers often hold a great deal of an organization's vital information. If a server is compromised, all of its contents may become available for the cracker to steal or manipulate
- Threats to sever consists of unauthorized modification of server data, unauthorized eavesdropping or modification of incoming data packets and compromise of a server system by exploiting bugs in the server software.

Contd…

- eavesdropping (monitoring packet sent over the network) , DOS (denial of service), packet replay (recording and retransmission of message packet in the network) and modification

b. Transaction security (data and message security)

- A growing threat to message on private and public network is the theft of password, accounts and other information that passes over the network.
- Transaction security can be divided into data and message security

I. Data security: a major threat to data security is unauthorized network monitoring, also called packet sniffing. It involves capturing, decoding, inspecting and interpreting the information inside a network. The purpose is to steal information, usually user ID, password, network detail, credit card number etc.

II. Message security: secure transmission is concerned with the technique and practices that will guarantee protection from intentional message modification. The different methods to provide security of message for transmission are:

- Message confidentiality
- Message integrity
- Message authentication

- Message confidentiality: it means maintaining the privacy of sensitive data such as credit card no., employee records, government files which are being transferred through the network. Cryptography can be the better choice for maintaining the privacy of information. confidentiality is sometimes called secrecy or privacy

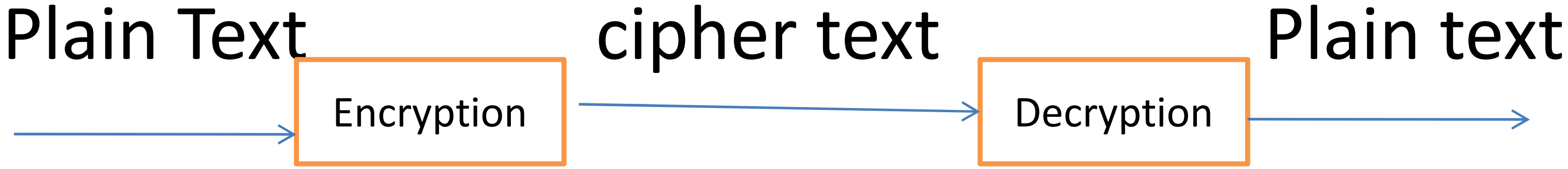
- Message integrity: integrity ensure the correctness as well as trustworthiness of data or resources. This method ensure that the content remains unmodified during transportation over the network. Integrity mechanisms fall into two classes: **preventative and detection.** Preventative mechanisms are responsible to maintain the integrity of data by blocking any unauthorized attempt to change the data. Detection mechanism simply analyze trustworthy of data’s integrity.

- Message authentication: authentication is a mechanism whereby the receiver of a message can be confident of the identity of the sender or integrity of the message. Authentication in e-commerce basically requires the user to provide his/her identity for each request service

Cryptography

- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
- The prefix **"crypt-"** means "hidden" or "vault" -- and the suffix **"-graphy"** stands for "writing."
- Cryptography is also defined as the science of providing security for information and is the art and science of information hiding.

- In ancient days, cryptography was mostly referred to as encryption and decryption.
- Encryption is the mechanism to convert the readable plaintext to unreadable text by using some algorithm and key. This unreadable text is called cipher text.
- Decryption is the mechanism to convert cipher text back to the plaintext by using some algorithm and key.



Plain Text

Encryption

cipher text

Decryption

Plain text

fig: encryption-decryption

- Modern cryptography concerns with the following four objectives

- Confidentiality
- Integrity
- Authorization
- non-repudiation: Non-repudiation is the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Types of cryptography

a. Secret-key cryptography

b. Public-key cryptography

c. Hash function

Secret key cryptography

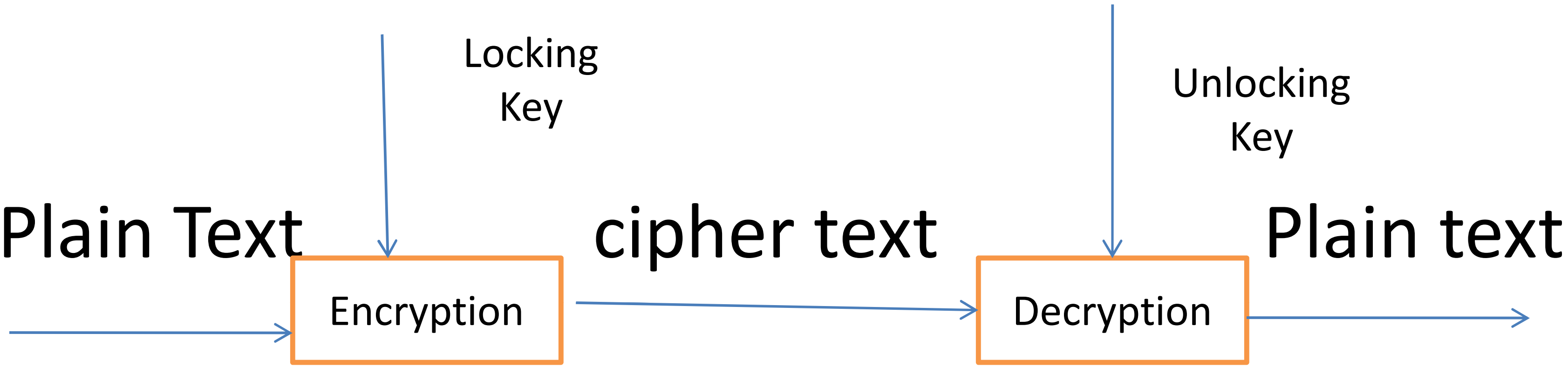
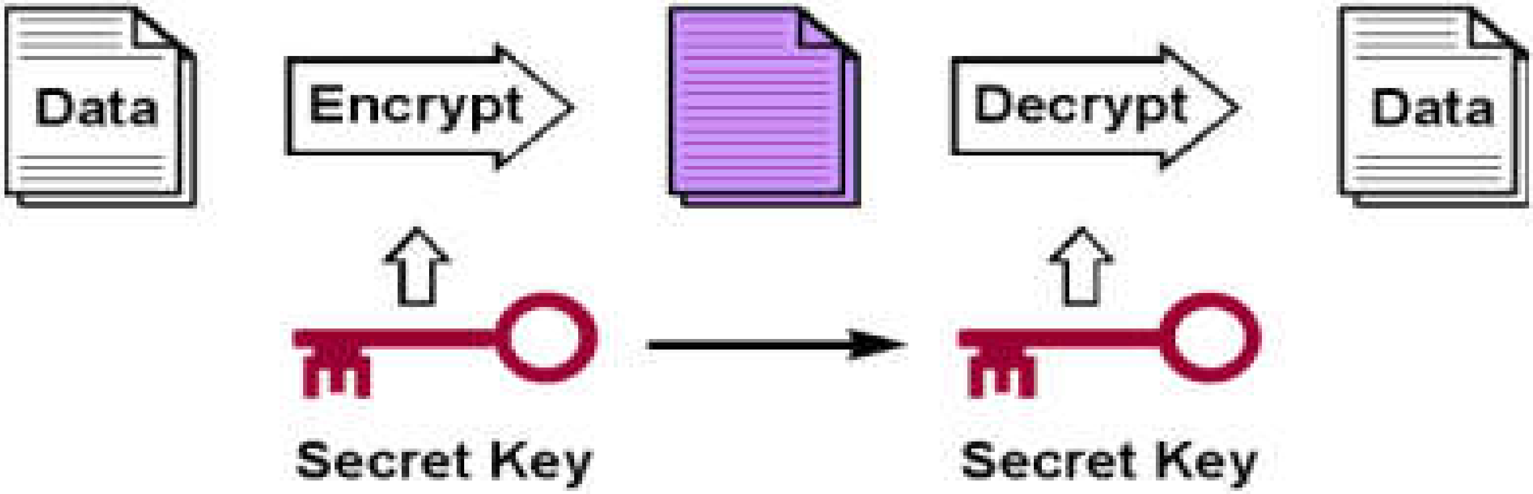


fig: Secret key cryptography


Data
Encrypt
Decrypt
Data
Secret Key
Secret Key

Secret key cryptography contd…

- In a secret key cryptography, the same key is used for both encryption and decryption.
- It is also called symmetric key cryptography or private key cryptography
- Since the keys are same, two users wishing to communicate in confidential way, and must agree and maintain a common secret key.

Secret key cryptography contd…

- In this type of system each entity must trust the other not to disclose the key.
- In this method , after creating a message, the sender encrypt it with their key and passes it to the receiver who then decrypt it by using a copy of the same key used to decrypt it
- A widely used method of secret-key encryption is the data encryption standard (DES)

Public key cryptography

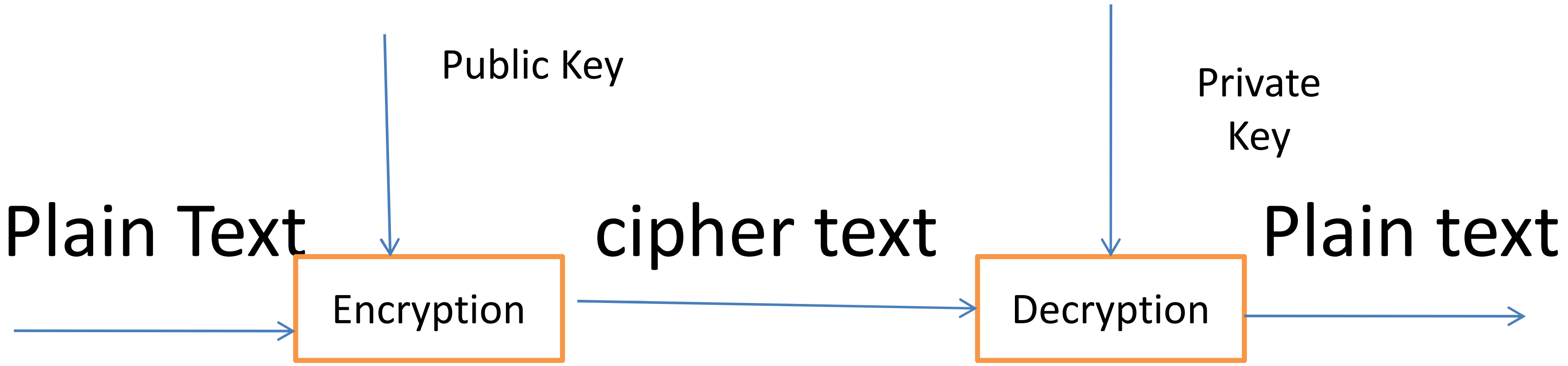


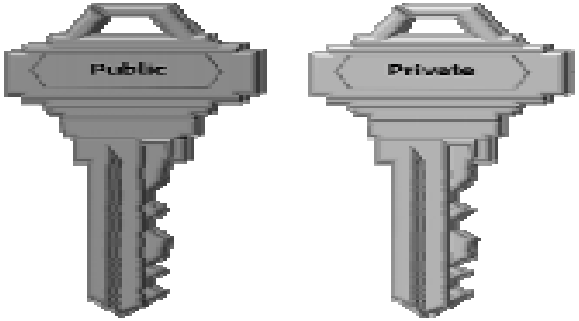
fig: publickey cryptography

Public key cryptography contd…

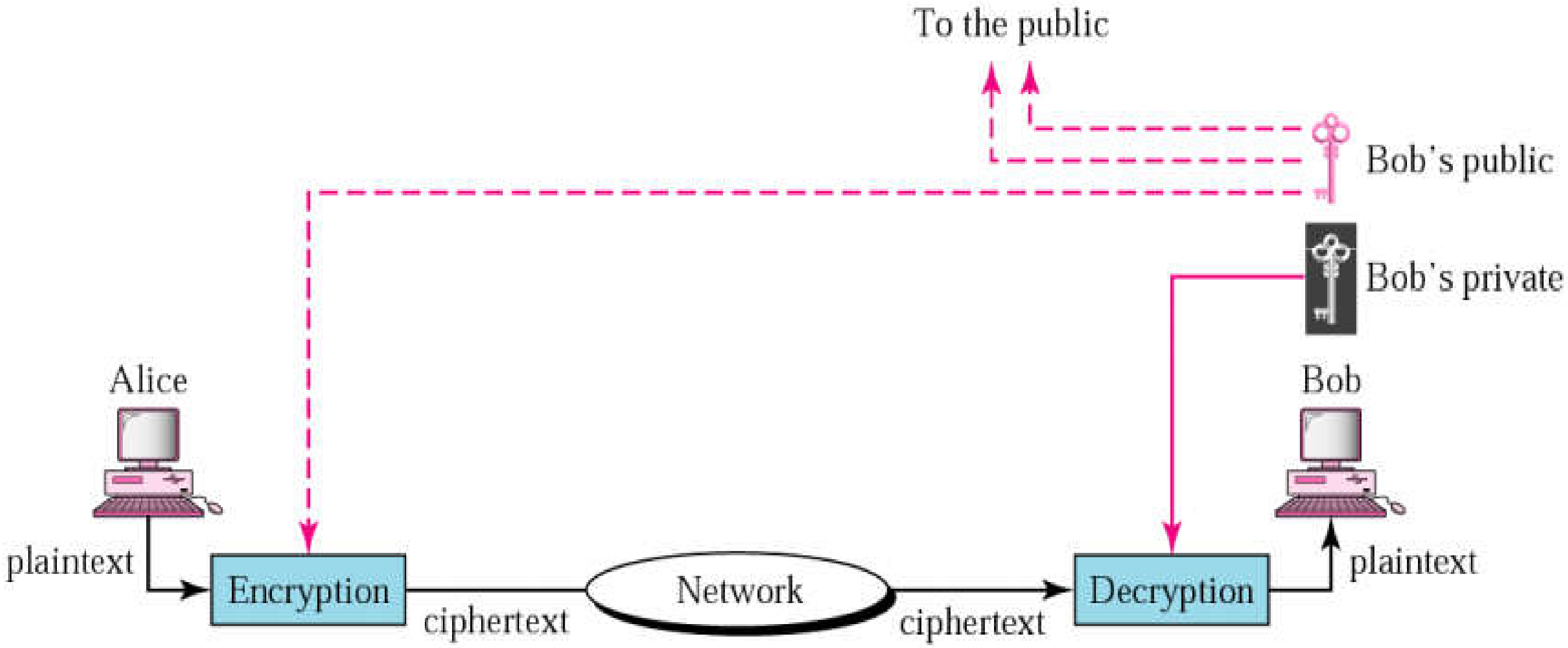
- Public key cryptography or asymmetric key cryptography involves the use of two keys, one that is used to encrypt messages (Public key) and another that is used to decrypt them (Private key)
- Knowledge of the public key allows encryption of plain text but does not allow decryption of the cipher text

Contd..

- Probably most significant advance in the 3000 year history of cryptography.
- Use Two keys => A Public & Private Key
- Asymmetric Keys => Keys used by two parties are not same.
- Uses Clever Mathematical Function.



Public Key Encryption



Hash function

- A cryptographic hash function is a one way transformation which takes an input (or 'message') and returns a fixed-size alphanumeric string.
- The string is called the 'hash value', 'message digest', 'digital fingerprint', 'digest' or 'checksum'.

- Some of the areas where hash functions are applied are:
- ➢Message integrity verification
- ➢Password verification
- ➢Digital signature

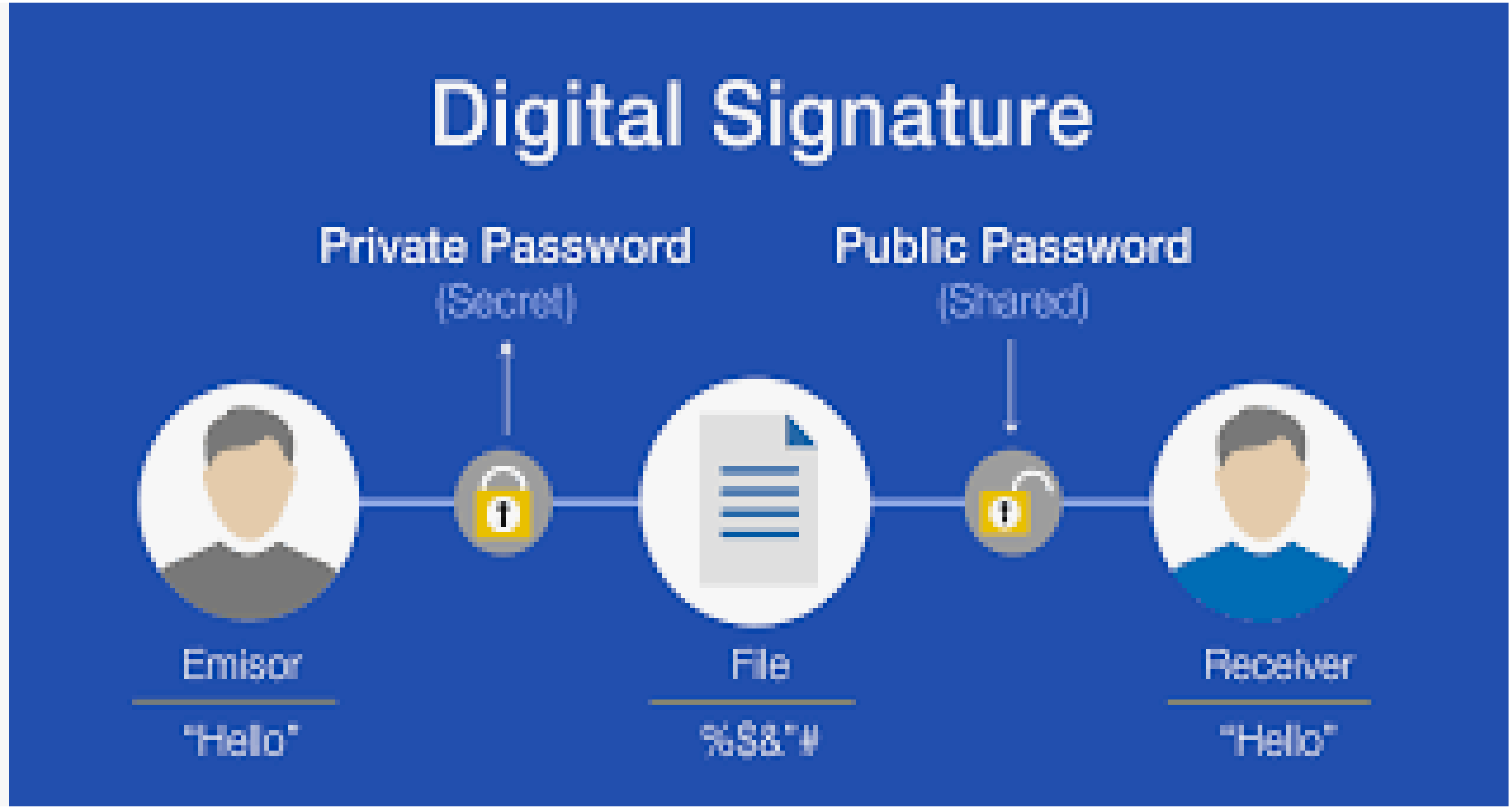
Differences between private and public key cryptography

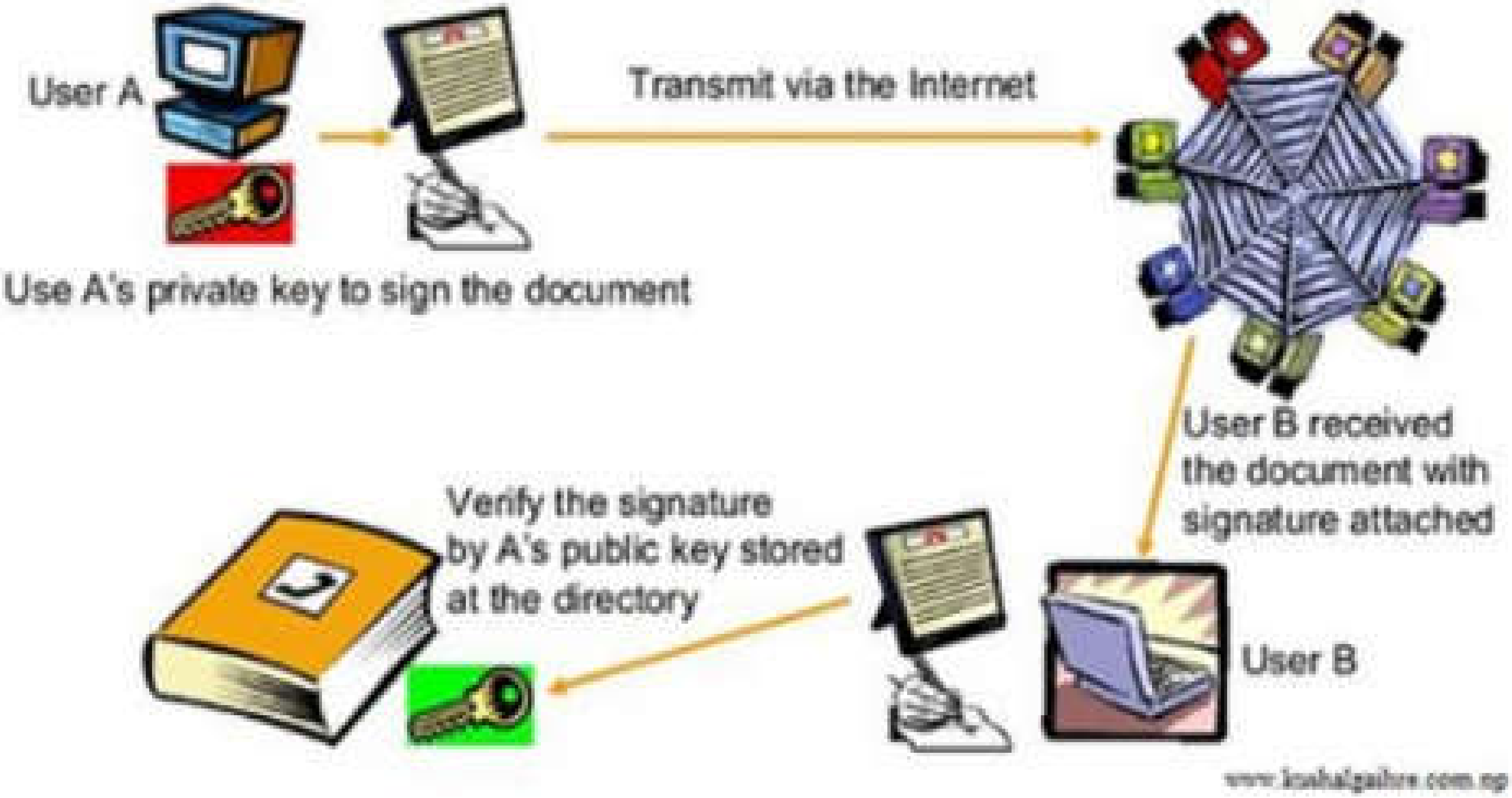
s.n.	Private key	Public key
1	The same length algorithm with the same key is used for encryption and decryption.	One algorithm is used for encryption and decryption with a pair of keys, one key for encryption and one for decryption.
2	Faster than public key	Slower than private key
3	If the key is lost or stolen then the entire system will fail	Private key do not need to be shared therefore it is relatively more secure than private key cryptography
4	It is useful in the system where it is possible to share the secret key by meetings	It is useful in when communication parties are at distant location and is difficult to share secret key
5	It is feasible when the number of users are limited	It is also feasible when the number of users in communication are large
6	Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Certificate Authority (CA)

- CA is an organization that is used to identify an individual, company or some other entity that is associated with a public key and is trusted to sign digital certificate.
- CA is a trusted third party organization or company that issues digital certificates used to create digital signature and public/private key
- The role of CA is to identify the identity of a certificate owner where that certificate becomes the key instrument on any e-commerce transactions

Digital signature




User A
Transmit via the Internet
Use A's private key to sign the document
User B received the document with signature attached
Verify the signature by A's public key stored at the directory
User B

www.kushalgaihre.com.np

- Digital Signature is a type of electronic signatures that encrypts the documents with digital codes that are particularly difficult to duplicate
- Digital a signature is a mathematical scheme for demonstrating the authenticity of a digital message or document.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender

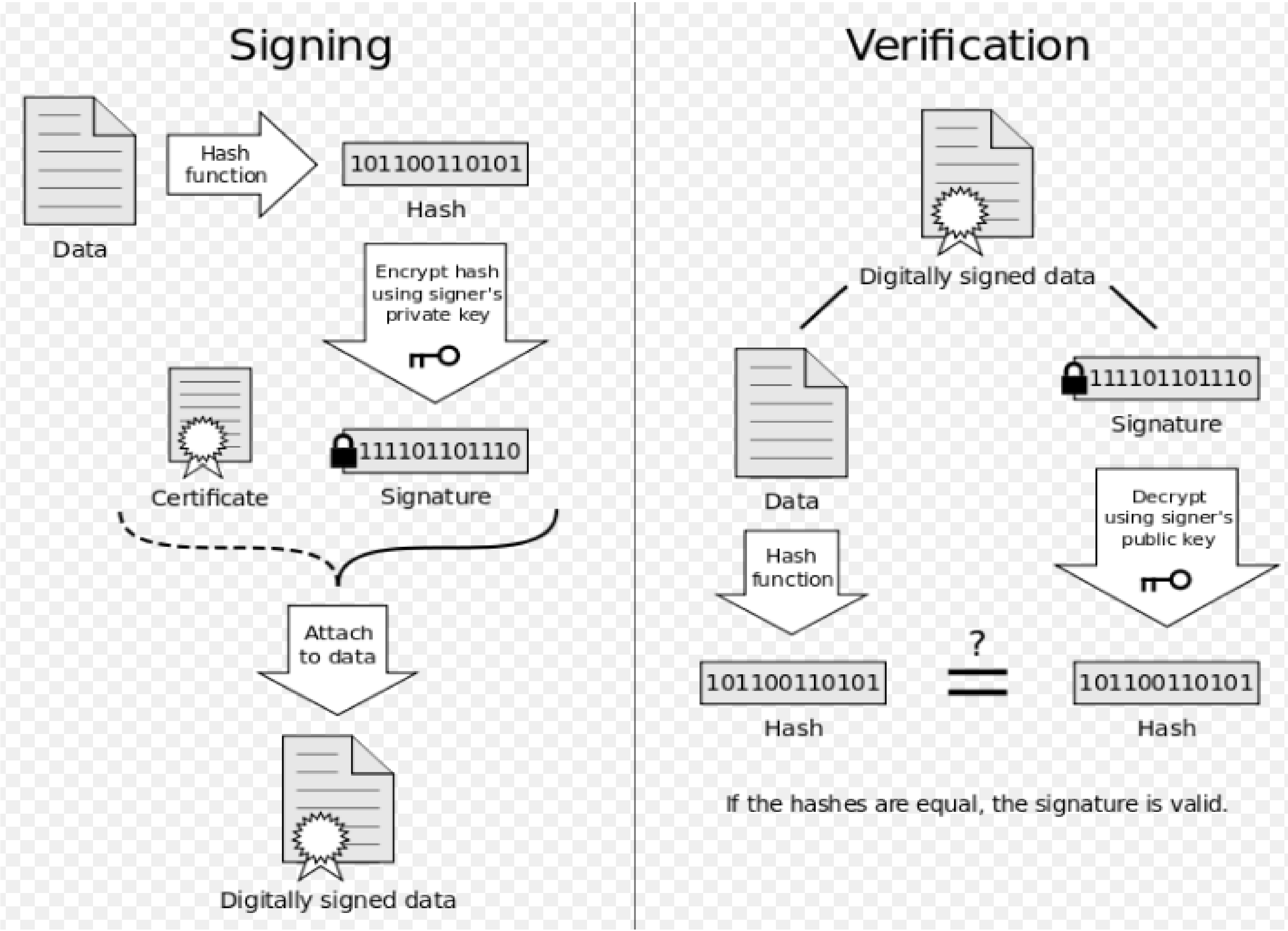
- Thus it can be used to achieve authentication, non-repudiation and integrity.
- Digital signature are commonly used for software distribution, financial transaction etc.

- A digital signature is a type of asymmetric cryptography and simulates security properties of a handwritten signature on paper.
- Digital signature schemes normally give two key generation algorithms, one for signing which involves the user’s secret key or private key, and one for verifying signatures which involves the user’s public key

- A digital signature scheme typically consists of three algorithms:

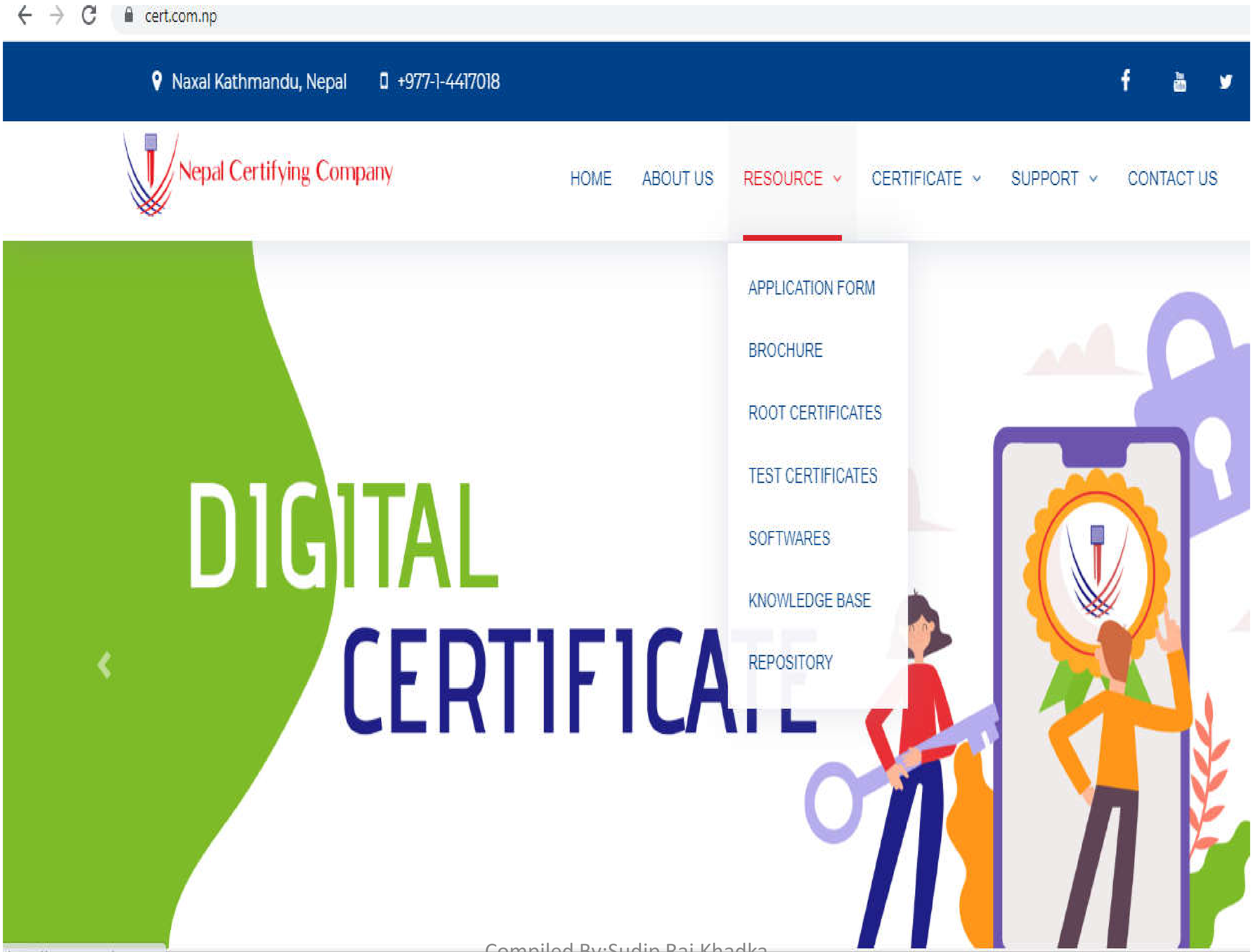
- ➢ Key generation algorithm: this algorithm randomly produces a pair of public and private key, where private key is used to generate signature and public key is used to verify signature
- ➢ Signing algorithm:
- ➢ Signature verifying algorithm

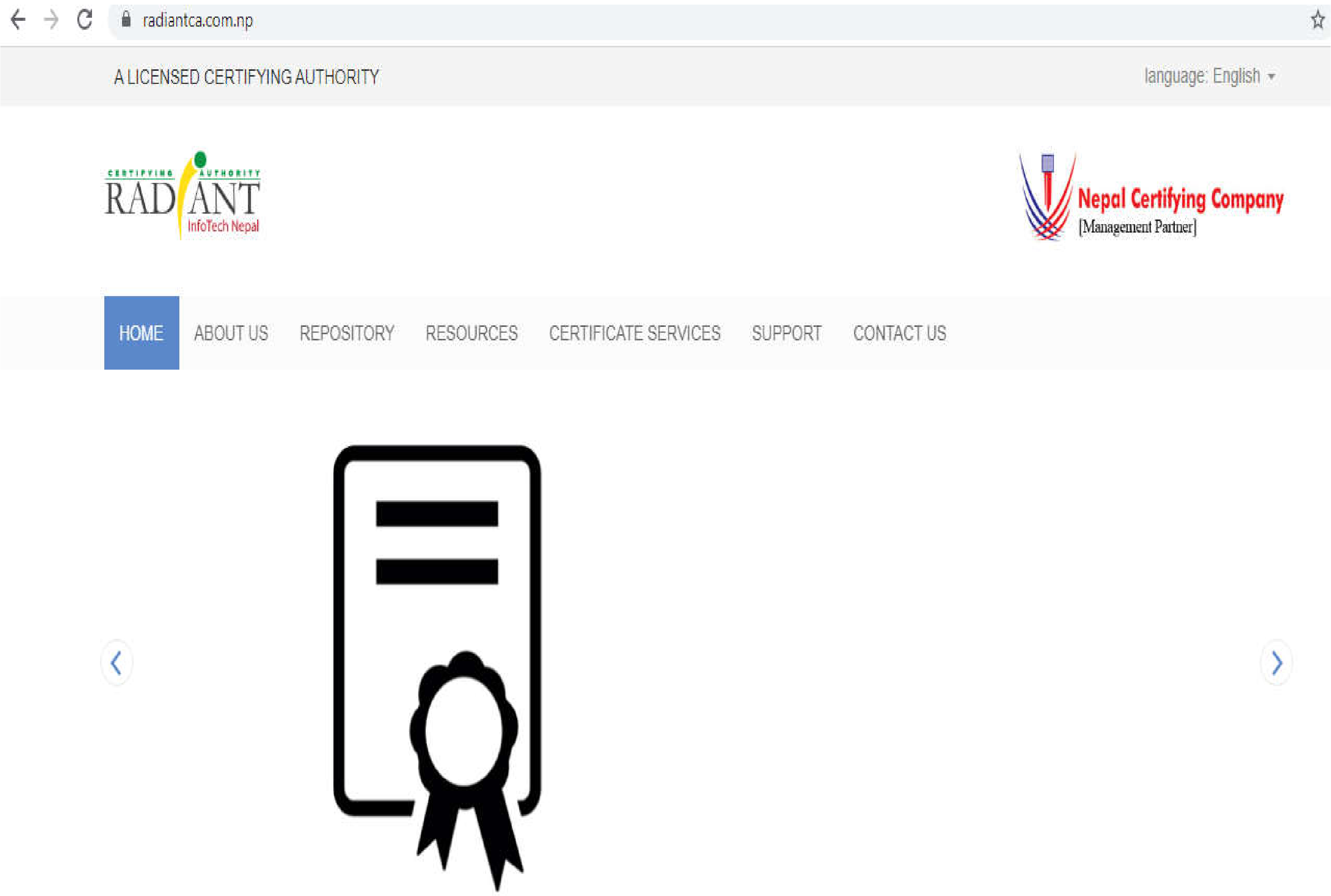
- Signing algorithm: this algorithm takes a message and private key as input and produces a signature that can be attached with documents
- Signature verifying algorithm: this algorithm takes the message and public key as input and verifies the validity of attached signature.


Signing
Data
Hash function
101100110101
Hash
Encrypt hash using signer's private key
Certificate
111101101110
Signature
Attach to data
Digitally signed data
Verification
Digitally signed data
Data
111101101110
Signature
Hash function
Decrypt using signer's public key
101100110101
Hash
?
=
101100110101
Hash
If the hashes are equal, the signature is valid.

Digital certificate

- A **Digital Certificate** is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI).
- Digital Certificate is also known as a **public key certificate** or **identity certificate.**
- It provides a means of providing an identity in electronic transactions and assures business associates an online services that the electronic information receipt is authenticated


cert.com.np
Naxal Kathmandu, Nepal
+977-1-4417018
Nepal Certifying Company
HOME
ABOUT US
RESOURCE
CERTIFICATE
SUPPORT
CONTACT US
APPLICATION FORM
BROCHURE
ROOT CERTIFICATES
TEST CERTIFICATES
SOFTWARES
KNOWLEDGE BASE
REPOSITORY
DIGITAL
CERTIFICATE



radiantca.com.np

A LICENSED CERTIFYING AUTHORITY

- It provides a means of providing an identity in electronic transactions and assures business associates an online services that the electronic information receipt is authenticated
- Digital certificates are the electronic counterparts to driver licenses, passport etc.
- A digital certificate is issued by a certification authority (CA)

- Digital certificate normally contains:
  - Public key of the certificate owner
  - Name of owner
  - Validity date
  - Name of issuing authority
  - Serial number of the certificate
  - Digital signature of the issuer

Authentication

- Authentication is the process to verify the identity of user as the user login with the network trust relationship for further interactions
- Authentication is the process of determining whether someone or something is, in fact, who or what it declares...

Contd….

- A common example is entering a username and password when you log in to a website.
- Entering the correct login information lets the website know
  - 1) who you are and
  - 2) that it is actually you accessing the website.

Third party authentication

- In third party authentication system, the password or encryption key itself never travels over the network
- Authentication server maintains a file of obscure facts about each file
- At the log-on time, the server demands the entry of randomly chosen facts

- The server uses token to complete a task
- The server then transmits an encrypted message containing token, which can be decoded with the user’s key.
- The message contains an authentication token that allows users to log on to the network services
- E.g kerberos

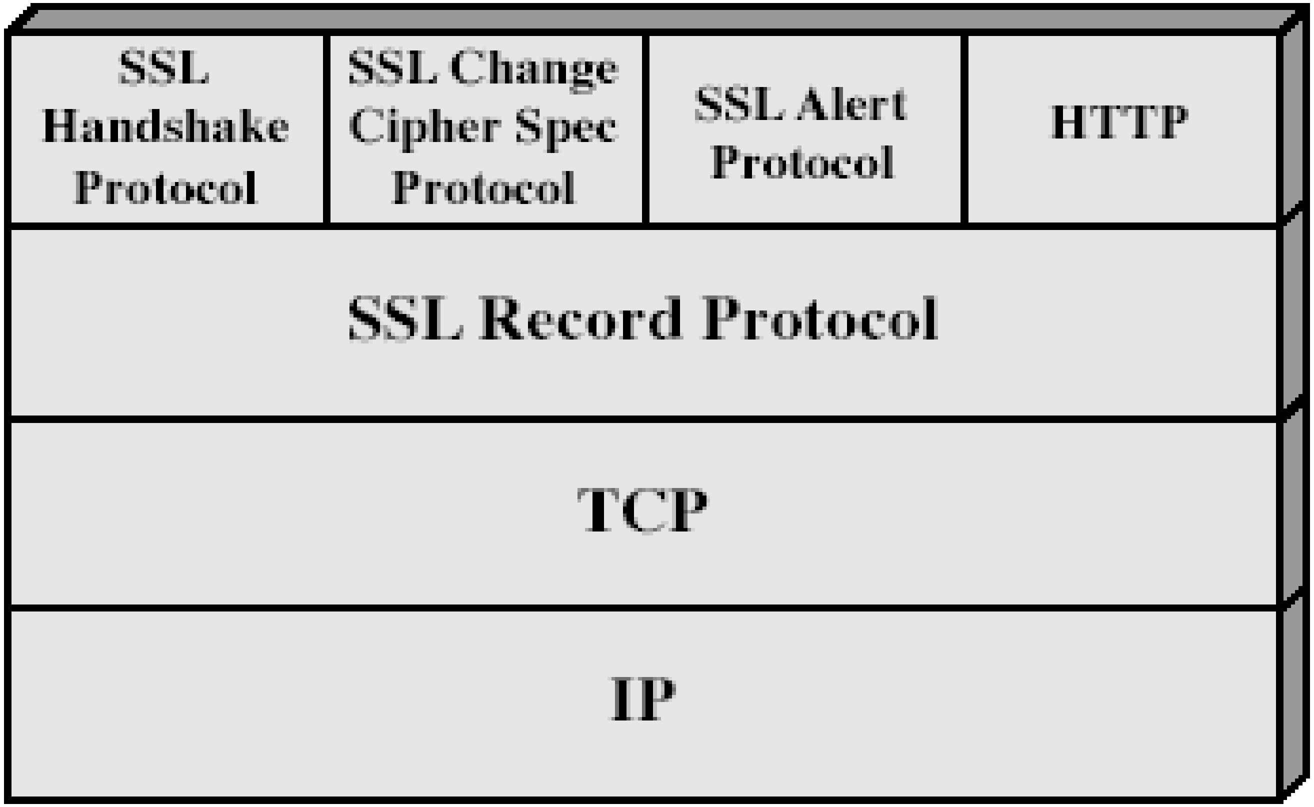
Secure Socket Layer (SSL)

- Secure Socket Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet.
- The SSL Security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

- SSL is a standard security technology for establishing an encrypted links between a server and a client- typically a web server and a web browser
- SSL allows sensitive information to be transmitted securely

- If SSL is not used, data sent between browsers and web servers is in plain text then If attacker is able to intercept all data being sent between a browser and web server, they can see and use information
- SSL is built into all major browsers and web servers.
- The primary goal of SSL is to provide privacy and reliability between two communicating applications

SSL Architecture



There are four layers of SSL protocol

- SSL handshake protocol: this protocol is responsible for establishing a secure session between two parties
- Change cipher space protocol: this protocol used in SSL to indicate that the communication is shifted from unencrypted to encrypted form

SSL Alert Protocol:

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- Alert messages are encrypted and compressed, as specified by the current connection state
- this protocol allows signals to be sent between peers.
- These signals are mostly used to inform the peer about the cause of a protocol failure

- **SSL Record protoco**l: functions of this protocol are:

- Breaking down the data from application layer, with fixed length
- Compress the data
- Add message authentication code
- Encrypt the packet
- Add SSL header in the packet

Secure Electronic transaction (SET)

- SET is an open encryption specification designed to protect credit card transactions on the internet
- It is not itself a payment system but the set of security protocols and format that enables users to employ the existing credit card payment infrastructure on an open network

- SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay.
- SET protocol includes Certification Authorities for making use of standard Digital Certificates

Requirements in SET :

- SET protocol has some requirements to meet, some of the important requirements are :
  - It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
  - It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
  - It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
  - SET also needs to provide interoperability and make use of best security mechanisms

- SET protocol provides three services:
  - Provides a secure communication channel among all parties involved in a transaction
  - Provides trust by use of digital certificates
  - Ensure privacy because the information is only available to parties in a transaction when and where necessary

SET Functionalities

- **Provide Authentication**
- **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution..
- **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not

Functionalities Contd…

- **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
- **Provide Message Integrity** : SET doesn’t allow message modification with the help of signatures. Messages are protected against unauthorized modification

Key features of SET

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

Participants in SET

- **Cardholder –** customer
- **Issuer –** customer financial institution
- **Merchant**
- **Acquirer –** Merchant financial
- **Certificate authority –** Authority which follows certain standards and issues certificates to all other participant

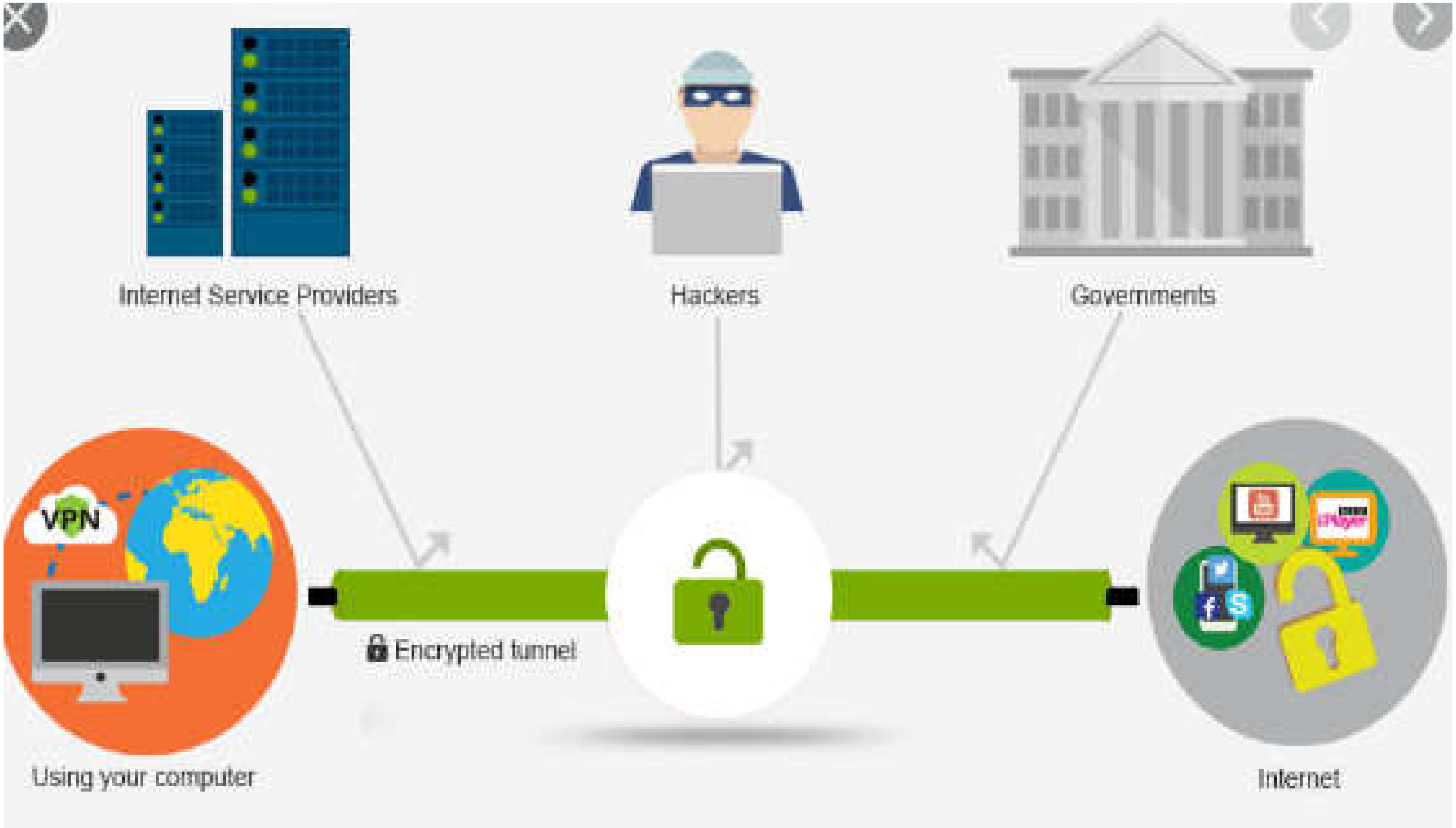
sequence of events required for e-commerce transaction by using SET protocol is as follows:

- The customer open an account
- The customer receives a certificate
- The customer places an order
- The merchant is verified:certificate verification
- Order and payment are sent
- Merchant request payment authorization
- Merchant confirms the order
- The merchant ships
- The merchant request payment

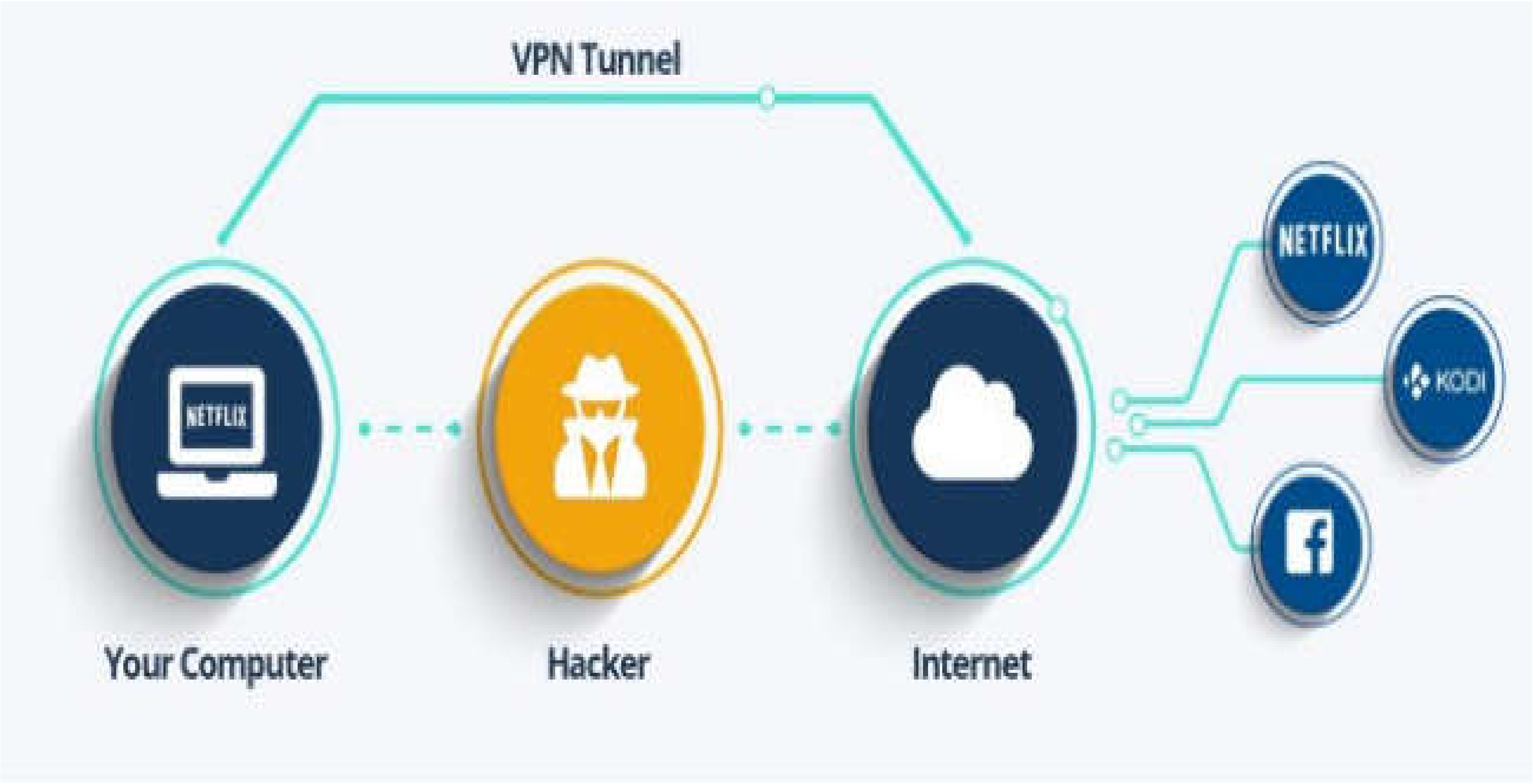
Virtual Private Network (VPN)

- A VPN is a private network that uses a public network to connect remote sites or users together.
- The VPN uses virtual connections routed through the internet form the business's private network to the remote site
- By using a VPN businesses ensure security- anyone intercepting the encrypted data can't read it
- A VPN works by tunneling itself to the internet in an encrypted way and can usually be acquired for little to no cost.

VPN(Virtual Private Network)



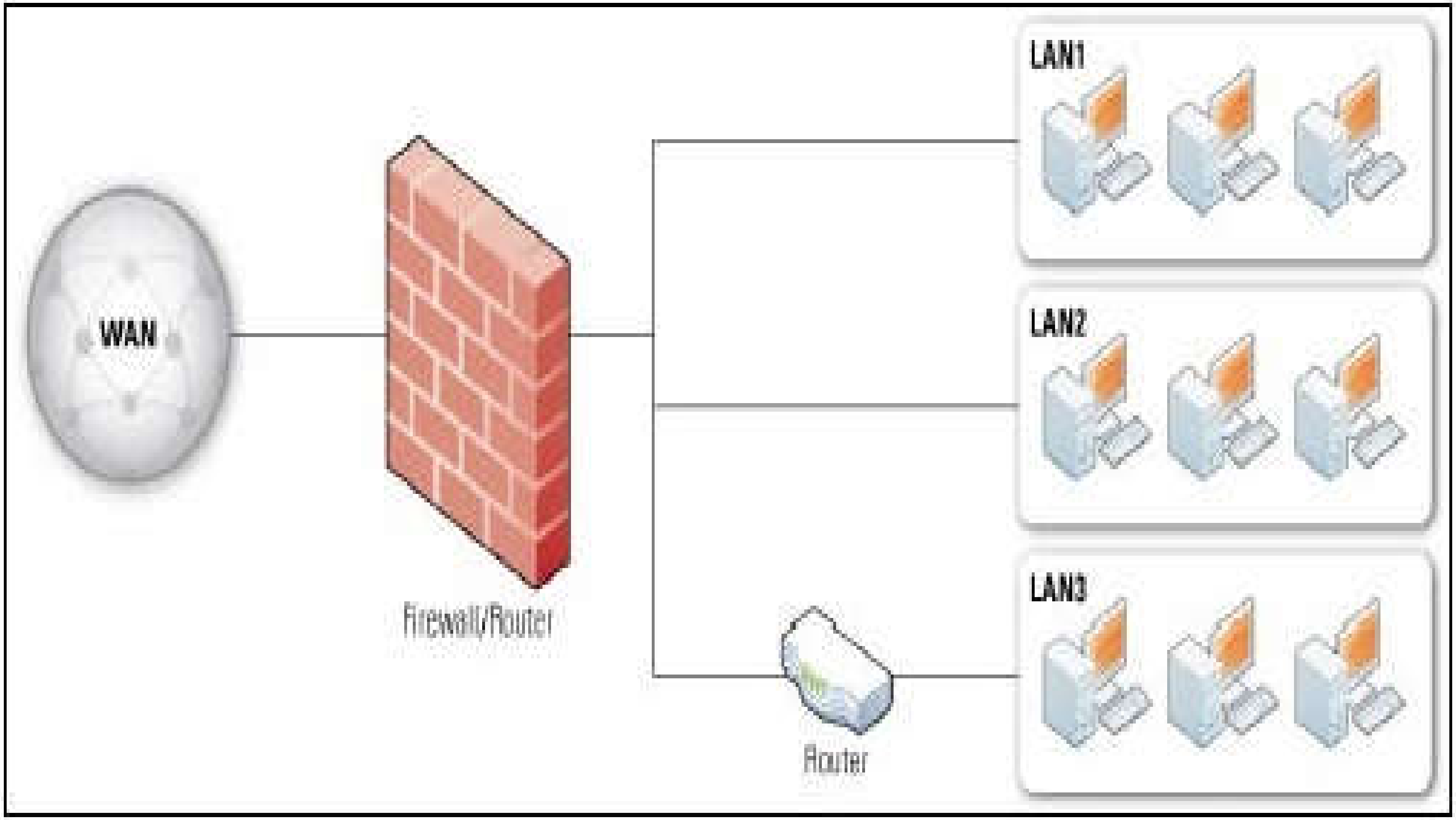
- A VPN, also known as a Virtual Private Network allows you to hide your IP address. Let's say my IP address is 123.456.789.123. If I use a VPN, I can generate a new IP address and that will actually turn into my actual IP, so now let’s say I just turned my VPN on. Instead of me being here in the Nepal I am now in China according to my new IP address
- A VPN works by tunneling itself to the internet in an encrypted way and can usually be acquired for little to no cost


VPN Tunnel
NETFLIX
Your Computer
Hacker
Internet
NETFLIX
KODI

Firewall

- A firewall is a system designed to prevent unauthorized access to or from a private network
- Firewall can be implemented in both hardware and software
- All the messages entering or leaving the private network pass through the firewall, which examine each message and blocks those that do not meet the specified security criteria
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*

- Hardware firewall can be purchased as a stand-alone product but are also typically found in routers and should be considered as an important part of system and network setup
- Software firewall are installed on your computer and we can customized it; allowing us some control over its function and protection criteria



Simple Routed Network with Firewall Device

Source: National Institute of Standards and Technology

http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Types of firewall

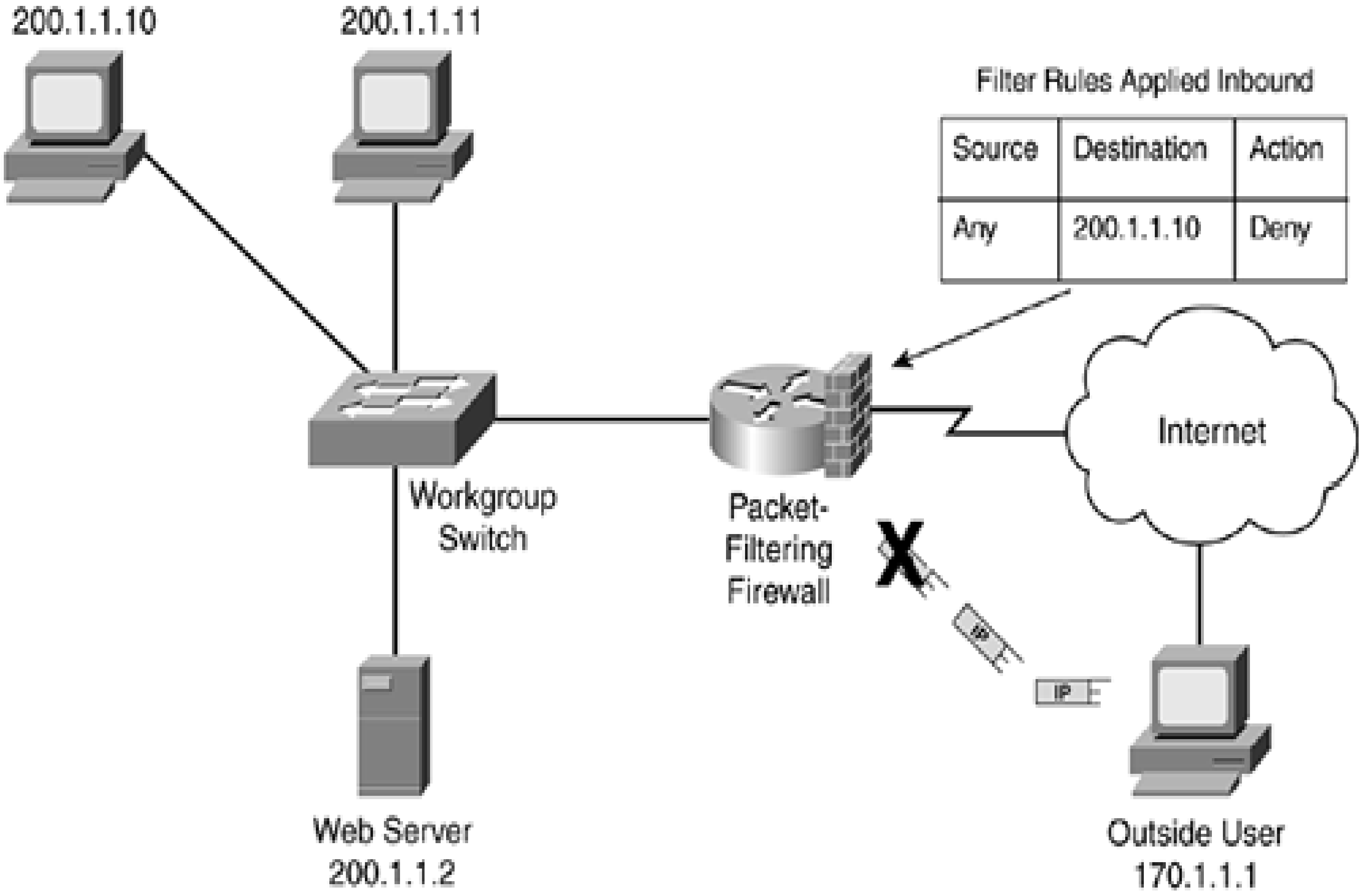
A. Packet filter
B. Application Gateways
C. Circuit-level Gateways
D. Stateful inspection firewall

Packet Filter Fire Wall

- Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model.
- Packet-filtering firewalls make processing decisions based on network addresses, ports, or protocols.
- Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make

Packet filter contd..

- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.
- Packet-filtering firewalls are considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port. So there could be malicious traffic being sent, but as long as it’s on an acceptable port, it will not be blocked.



Filter Rules Applied Inbound

Source	Destination	Action
Any	200.1.1.10	Deny

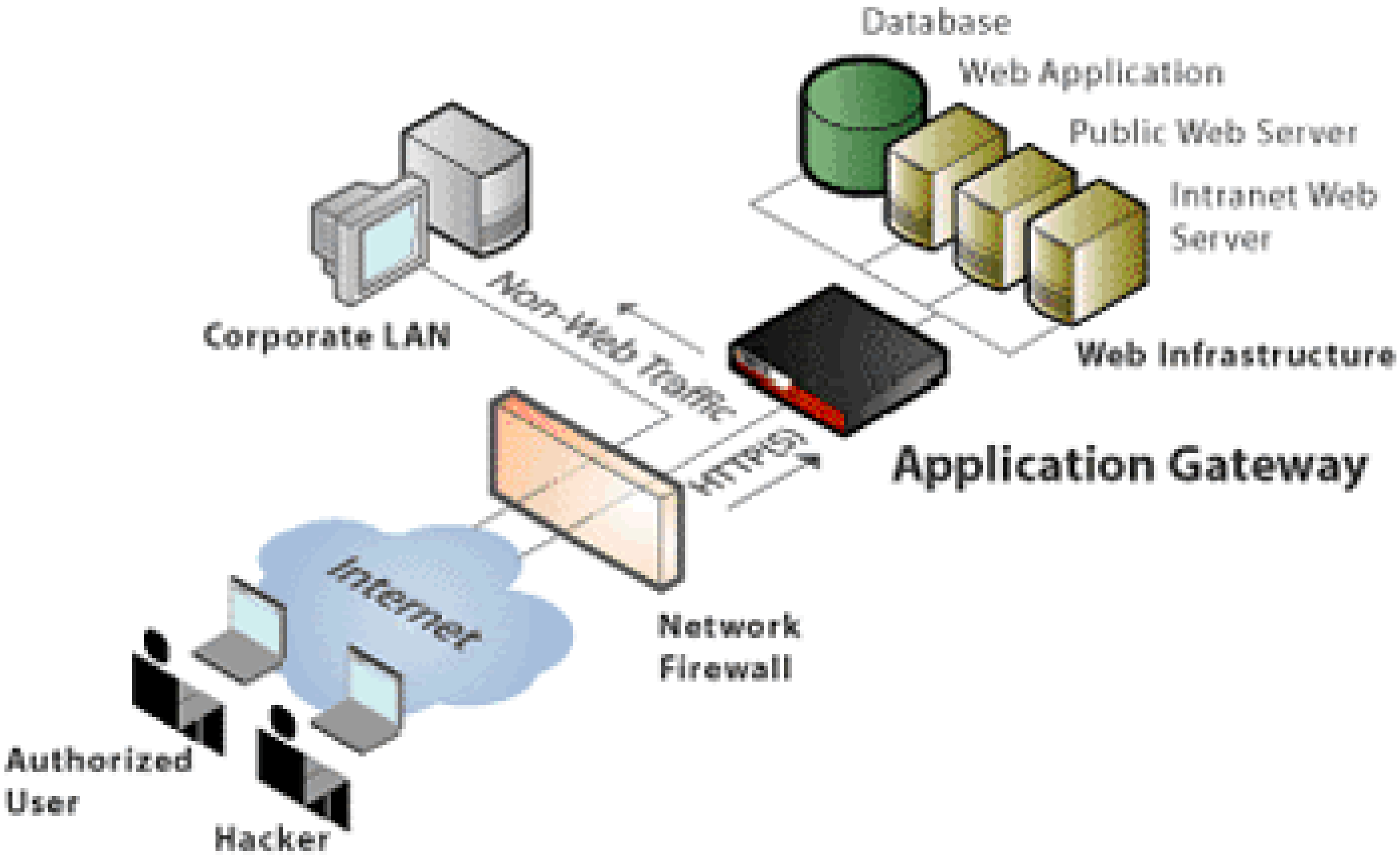
Application Gate Way Firewall

- Application gateway firewalls operate at the application layer (Layer 7) of the OSI model.
- They filter access based on application definitions. Application definitions can include not only port numbers but also specific application information like acceptable HTTP verbs.
- Application gateway firewalls are considered to be some of the most secure firewalls available because of their capability to inspect packets and ensure the packets are conforming to application specifications.

Contd…

- Because of the amount of information being processed, application gateway firewalls can be a little slower than other firewalls.
- Application layer firewalls are hosts that run proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them

Application Gate way Firewall



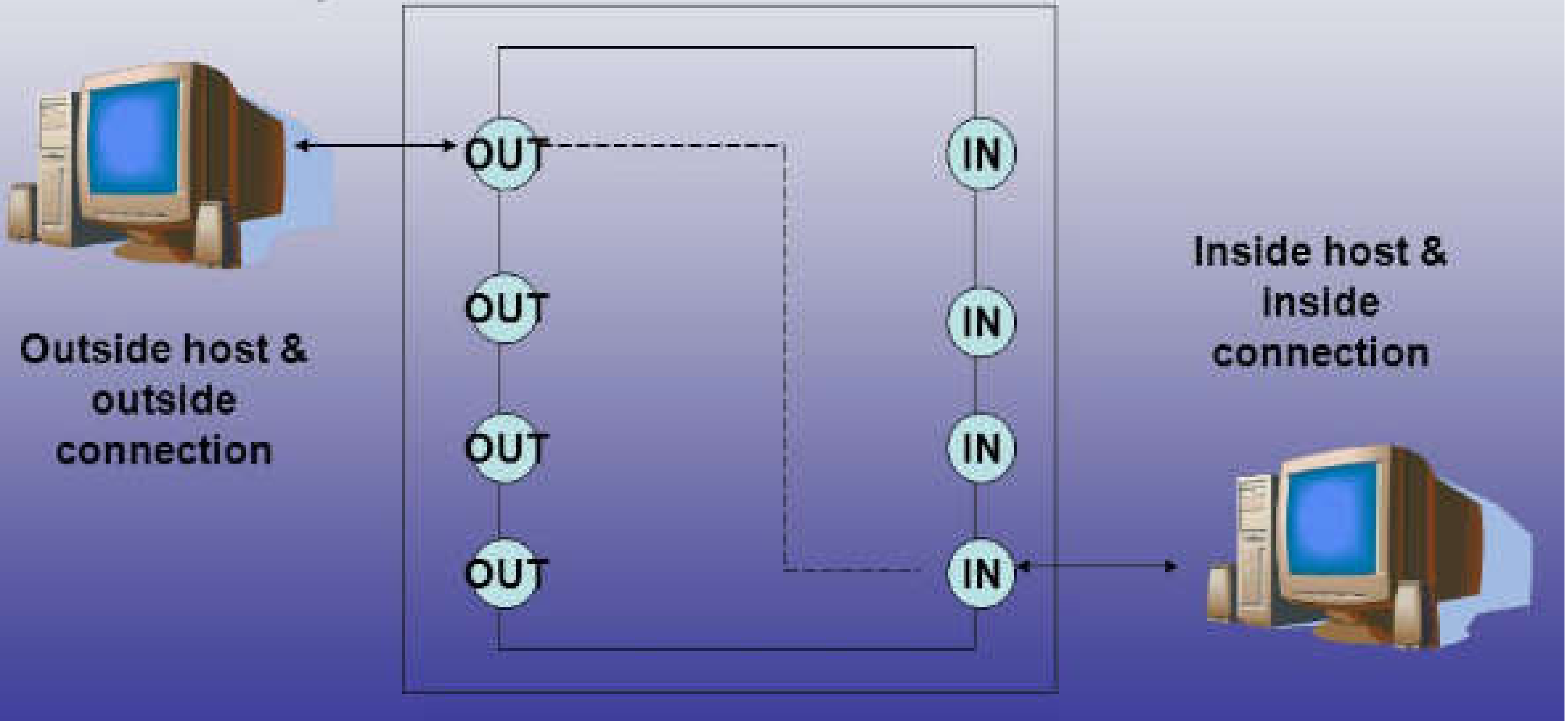
Circuit Level Firewall

- A circuit-level gateway monitors TCP handshaking between packets from trusted clients or servers to un trusted hosts and vice versa to determine whether a requested session is legitimate.
- To filter packets in this way, a circuit-level gateway relies on data contained in the packet headers for the Internet's TCP session-layer protocol.
- Because a circuit-level gateway filters packets at the session layer of the OSI model, this gateway operates two layers higher than a packet-filtering firewall does.

- Monitoring Handshaking--Circuitously. To determine whether a requested session is legitimate, a circuit-level gateway uses a process similar to the following:
  - A trusted client requests a service, and the gateway accepts this request, assuming that the client meets basic filtering criteria (such as whether DNS can locate the client's IP address and associated name).
  - A circuit-level gateway determines that a requested session is legitimate only if the SYN flags, ACK flags, and sequence numbers involved in the TCP handshaking between the trusted client and the un trusted host are logical

Circuit Level Gateway

- Circuit Level Gateway.



Outside host & outside connection

Inside host & inside connection

Statefull Inspection Firewall

- A stateful inspection firewall combines aspects of a packet-filtering firewall, a circuit-level gateway, and an application-level gateway. Like a packet-filtering firewall, a stateful inspection firewall operates at the network layer of the OSI model, filtering all incoming and outgoing packets based on source and destination IP addresses and port numbers

Contd…

- A stateful inspection firewall also functions as a circuit-level gateway, determining whether the packets in a session are appropriate. For example, a stateful inspection firewall verifies that SYN and ACK flags and sequence numbers are logical.

Contd…

- Finally, a stateful inspection firewall mimics an application-level gateway: The firewall evaluates the contents of each packet up through the application layer and ensures that these contents match the rules in your company's network security policy.