Cryptography & Network Security

FOR DIPLOMA STUDENTS

PREPARED BY :PRATIBHA PATNAIK

Chapter -1

Network security:

- Network security is any activity designed to protect the usability and integrity of your network and data.
- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network.

Need for security:

An internet is being used by us for every application. So there is every chance of our data or information may be attacked by the attacker. So the confidentiality of the message is lost. Therefore, cryptography & network security is used to protect our information while it is transmitted from sender to receiver.

Security Approaches:

An organization can take several approaches to implement security model, so these are

a) Security models
b) Security management practices

Security Models:

i. **No security:** In this case, the approach could be decision to implement no security at all.
ii. **Security through obsecurity:** In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.
iii. **Host security:** In this model the security for each host is enforced individually.
iv. **Network security:** In this model, the whole network is provided with a security instead of individual host security.

Security Management Practice:

Good security management practices deal with a security policy which contains the following 4 key aspects.

I. **Affordability:** How much money & efforts does these security implementation cost?
II. **Functionality:** What is the mechanism of providing security?
III. **Cultural issues:** Does the policy satisfy the people's expectations, working style & belief?

IV. **Legality:** Does the policy meet the legal requirements?

Principles of security:

There are 6 types of principles of security.

1) Confidentiality
2) Authentication
3) Integrity
4) Non-repudiation
5) Access control
6) Availability

Confidentiality:

- ➢ The principle of confidentiality specifies that only the sender and the intended recipients should be able to access the contents of a message.
- ➢ Confidentiality gets compromised if an unauthorized person is able to access a message.
- ➢ This type of attack is called interception.
- ➢ Interception causes loss of message confidentiality.

Authentication:

- ➢ Authentication mechanisms help establish proof of identities.
- ➢ The authentication process ensures that the origin of an electronic document is correctly identified.
- ➢ This type of attack is called fabrication.
- ➢ Fabrication is possible in absence of proper authentication mechanisms.

Integrity:

- ➢ When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient which means the integrity of the message is lost.
- ➢ This type of attack is called as modification.

Non-repudiation:

- There are situations where a user sends a message and later on refuses that he had sent that message. This is called repudiation.
- The principle of non-repudiation does not allow the sender of a message to refuse the claim of not sending that message.

Access control:

- The principle of access control determines who should be able to access what.
- This mechanism is divided into two areas.

  i. Role management

  ii. Rule management

Role management:

Role management concentrates on the user side (which user can do what).

Rule management:

Rule management focuses on the resource side (which resource is accessible and under what circumstances).

Based on the decisions an access control matrix I prepared, which list the user against the list of items they can access. An Access Control List (ACL) is a subset of an access control matrix.

Availability:

The principle of availability states that resources (i.e. information) should be available to authorized parties at all times.

Ex: Interruption puts availability of resources in danger.

Types of attacks:

There are 2 types of attacks.

1. Attacks: a general view
2. Attacks: a technical view

Attacks: a general view:

It can be classified into 3 types.

i. Criminal attacks

ii. Publicity attacks

iii. Legal attacks

Criminal attacks:

The aim of the attackers is to maximize financial gain by attacking computer systems.

Ex: Fraud, scam, identity theft, intellectual property theft etc.

Publicity attack:

Publicity attack occurs because the attacker wants to see their names appear on television news channel and newspaper.

Ex: to damage the webpage of a site by attacking it.

Legal attacks:

In this attack, the attacker tries to make the judge or jury doubtful about the security of a computer system. This works as follows.

The attacker attack computer system & the attacked party manages to take the attacker to the court.

While the case is being fought, the attacker tries to convince the judge that there is inherent weakness in the computer system and he has done nothing wrongful.

The aim of the attacker is to exploit the weakness of the judge in technology matters.

Attacks: Technical view:

From the technical points of view, the attacks on computer system or the network system can be classified into 3 types.

1. Theoretical concepts
2. Practical side of attacks
3. Programs that attack

Theoretical concepts:

Theoretical concepts of attacks can be classified into 2 types.

i. Passive attacks

ii. Active attacks

Passive attacks:

Passive attacks do not involve any modification to the contents of an original message. It can be classified again into 2 types.

A. Release of message contents

B. Traffic analysis

A. Release of message contents:

In this attack the attacker can be able to access the contents of the message without modifying the contents.

B. Traffic Analysis:

In this attack the attacker can attack the encoded message so as to decode it to know the contents of the message.

Active attacks:

In this attack, the attacker only releases the contents of the message but also performs the modification in the original message or create a false a message & send it to the receiver. It is of 3 types.

i. Interruption

ii. Modification

iii. Fabrication

Interruption (Masquerade) attacks:

Masquerade is caused when an unauthorized entity pretends to be another entity.

Modification:

In this attack, the attacker may modify the values in the database, so that integrity of the message is lost. It is of 2 types.

i. Replay attacks

ii. Alterations

i. Replay attacks:

In this attack a user captures a sequence of events or some data units and resends them.

Ex: Suppose A & C have bank accounts in the bank B. A is the sender & B is the receiver. A is sending a message to B that pay Rs. 1000/- to C. Someday C captures the message send by A to bank B. Then C resends the same message of A to bank B. So bank B will pay 2 times in the account of C.

ii. Alteration attacks:

Alteration attacks means the attacker can make some changes in the original message.

Fabrication (DOS) attacks:

This attack make attempt to prevent legitimate (authorized) users for accessing some services which their eligible form.

Ex: An unauthorized user might send too many log in requests to a server using random user IDs one after another very quickly. So as to flood the network and deny other legitimate users from using the network facilities.

Practical sides of attacks:

This can be classified into 2 types.

i. Application level attacks

ii. Network level attacks

i. **Application level attacks:**

These attacks happen at an application level in the sense that the attacker attempts to access, modify or prevent access to information of a particular application or to the application itself.

Ex: The attacker trying to get someone credit card information on the internet.

ii. **Network level attacks:**

These attacks generally aim at reducing the capability of a network by a no. of possible means. These attacks may can attempt to either slow down or completely bring to halt of a computer network.

Programs that attacks:

There are few programs that attacks computer system to cause some damage or to create confusion. These are as follows:

i. Virus

ii. Worm

iii. Trojan horse

iv. Applets and Active X controls

Virus:

A virus is a computer program that attaches itself to another legitimate program & causes damage to the computer system or to the network.

During its lifetime a virus goes through 4 phases.

1. **Dormant phase:**

   Here the virus is idle, it gets activated based on some action or event.

2. **Propagation phase**

   In this phase a virus copies itself & each copy starts creating more copies of self thus propagating the virus.

3. **Triggering phase**

A dormant virus moves into this phase when the action or event for which it was waiting is initiated.

4. **Execution phase**

This is the actual work of the virus, which could be harmless or destructive.

Virus can be classified into the following types.

a) **Parasitic virus:** This is the most common form of viruses. Such a virus attaches itself to executable files and keeps replicating. Whenever the infected file is executed, the virus looks for other executable files to attach itself & spread.

b) **Memory resident virus:** This type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.

c) **Boot sector virus:** This type of virus infects the master boot record of the disk and spreads on the disk when the operating system starts booting the computer.

d) **Stealth virus:** this virus has intelligence built in, which prevents anti-virus software programs from detecting it.

e) **Polymorphic virus:** A virus that keeps changing its signature i.e. identity on every execution making it very difficult to detect.

f) **Metamorphic virus:** In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

g) **Macro virus:** This virus can affect only specific application software like MS word, MS Excel etc.

Worm:

Similar in concept to a virus a worm does not perform any destructive actions & instead only consumes system resources to bring it down.

Trojan horse:

A Trojan horse allows an attacker to get some confidential information about a computer or network.

Java applets & Active X controls:

These are small client side programs, which may come from the web server with a http request from the client. These small programs may cause security problems if used by the attackers with a bad intension.

Cryptography Concepts

Cryptography:

Cryptography is the art & science of achieving security by encoding messages to make them non-readable.

Cryptanalysis:

It is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

Cryptology:

It is the combination of cryptography & cryptanalysis.

Plain text & Cipher text:

- Plain text signifies a message that can be understood by the ender, receiver & also by anyone else who gets and access to that message.
- When a plain text is codified using any suitable scheme, the resulting message is called as cipher text.

Techniques to convert plain text to cipher text:

There are two techniques/methods to convert plain text to cipher text.

1. Substitution technique
2. Transposition technique

Substitution techniques:

In substitution cipher technique the characters of plain text message are replaced by other characters, numbers or symbols.

The substitution techniques are many types.

1. Ceaser Cipher
2. Modified version of ceaser cipher
3. Monoalphabetic cipher
4. Homophonic substitution cipher
5. Polygram substitution cipher
6. Polyalphabetic substitution cipher
7. Playfair cipher
8. Hill cipher

Ceaser cipher:

In this technique each alphabets in the plain text is replaced by an alphabet 3 places down the line.

It was developed by Julius Ceaser. So it was called as ceaser cipher.

Ex: Plain text: WELCOME
Cipher text: ZHOFRPH

Modified version of ceaser cipher:

In the modified version of ceaser cipher in which all the alphabets in the given plain text message are replaced by a fixed alphabet down the line or up the line.

Howevereach alphabet can be replaced by any other alphabet available in the alphabet set.

Ex: A can be replaced by B to Z.
B can be replaced by C to Z & A.

Ex:Plain text: WELCOME
Cipher text: YGNEQOG

Monoalphabetic cipher:

Monoalphabetic cipher is also one form of modified version of ceaser cipher in which all the alphabet in the given plain text message are replaced by any other alphabet using random substitution technique.

Homophonic substitution cipher:

Homophonic substitution cipher also involves substitution cipher also involves substitution of one plain text character with a cipher text character at a time. However the cipher text character can be any one of the chosen set.

Polygram substitution cipher:

Polygram substitution cipher technique replaces one block of plain text with a block of cipher text. It doesn't work on a character by character basis.

Polyalphabetic substitution cipher:

This cipher uses multiple one character keys. Each of the key encrypts one plain text character. The 1st key encrypt the 1st plain text character, the 2nd key encrypt the 2nd plain text character & so on.

Ex: vigenere cipher

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Example:

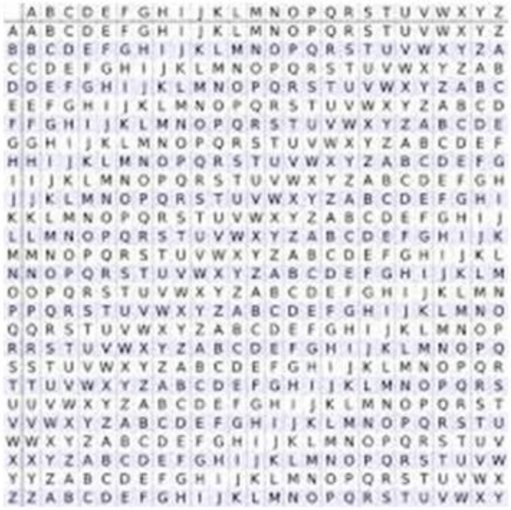
Input:Plaintext: GEEKSFORGEEKS

Keyword AYUSH

Output: Ciphertext: GCYCZFMLYLEIM

For generating key, the given keyword is repeatedin a circular manner until it matches the length of the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

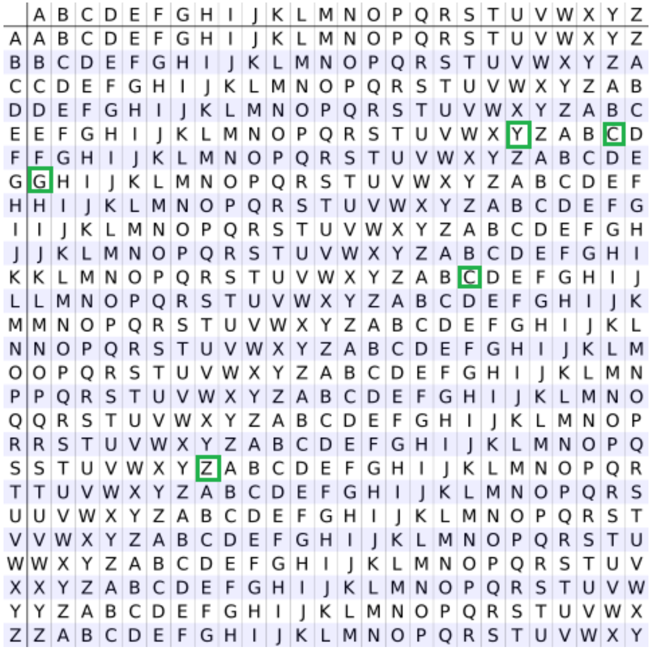


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

vigenere table

Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar way.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Playfair cipher:

The Playfair cipher is also called as Playfair square is a cryptography technique that is used for manual encryption of data.

This was invented by Charles Wheatstone in 1854. This method uses the following 2 steps.

1. Creation population of matrix
2. Encryption process

Creation population of matrix:

The Playfair cipher makes uses of 5*5 matrix or table, which is used to store a keyword.
The following rules are used for matrix creation & population.

Generate the key Square (5×5):

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Encryption process:

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

Example:

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Rules for Encryption:

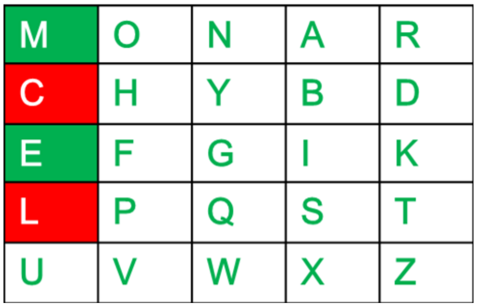
- **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
  For example:

Diagraph: "me"

Encrypted Text: cl

Encryption:

m -> c
e -> l



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
  For example:

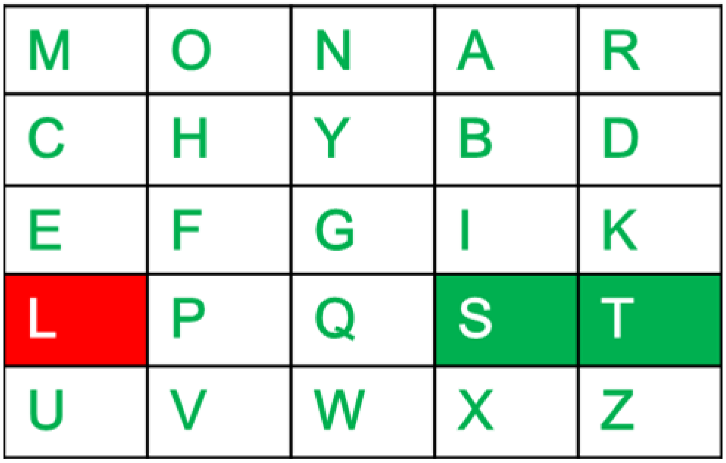
Diagraph: "st"

Encrypted Text:tl

Encryption:

s -> t

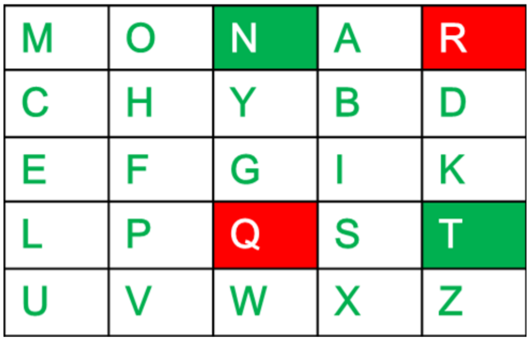
t -> l



M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
  For example:

Diagraph: "nt"
Encrypted Text:rq
Encryption:
n -> r
t -> q

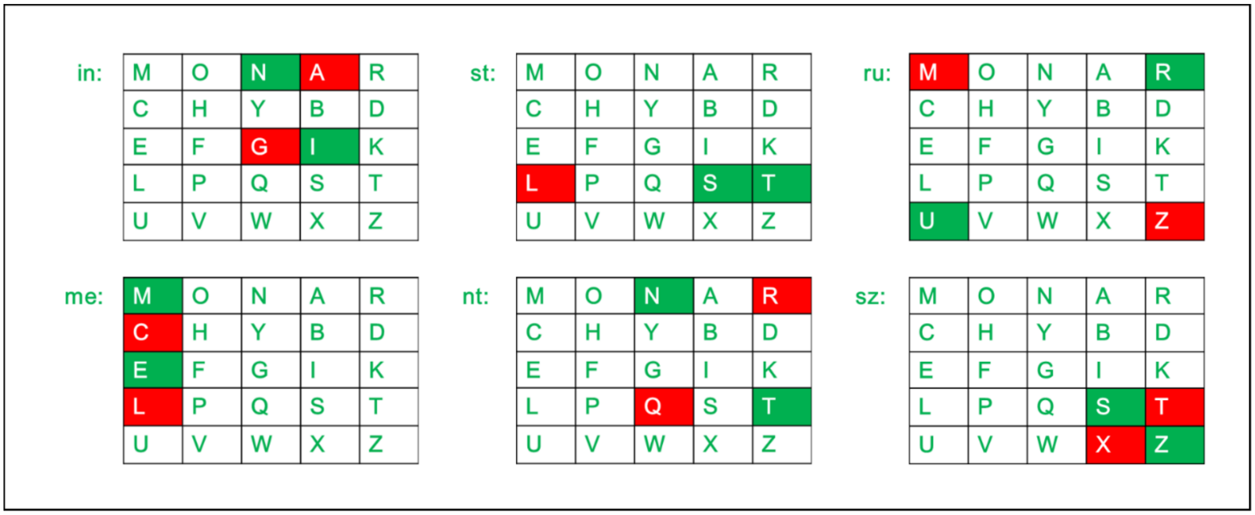


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "instrumentsz"
Encrypted Text:gatlmzclrqtx
Encryption:
i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
e -> l
n -> r

t -> q
s -> t
z -> x



Hill cipher:
Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:
Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

Input : Plaintext: GFG

Key: HILLMAGIC

Output : Ciphertext: SWK

Encryption

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of ‘POH’

Internet Security Protocols

SSL:

- Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server.
- Netscape originated secure Socket Layer.

The objectives of SSL are:

- Data integrity: Data is protected from tampering.
- Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
- Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server.

- SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission.
- It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read.

- It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.
- This information could be anything sensitive or personal, which can include credit card numbers and other financial information, names and addresses.

TLS:

Transport Layer Securities (TLS) are designed to provide security at the transport layer.
TLS is used to secure Web browsers, Web servers, VPNs, database servers and more. TLS protocol consists of two different layers of sub-protocols:

- TLS Handshake Protocol: Enables the client and server to authenticate each other and select a encryption algorithm prior to sending the data
- TLS Record Protocol: It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services.

There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

HTTPS:

- HTTPS stands for Hypertext Transfer Protocol Secure. It is the protocol where encrypted HTTP data is transferred over a secure connection.
- HTTPS ensures data security over the network - mainly public networks like Wi-Fi.
- HTTPS encryption is done bi-directionally, which means that the data is encrypted at both the client and server sides.
- Only the client can decode the information that comes from the server.
- It allows the secure transactions by encrypting the entire communication with SSL.
- It is a combination of SSL/TLS protocol and HTTP. It provides encrypted and secure identification of a network server.

Advantages of HTTPS

- In most cases, sites running over HTTPS will have a redirect in place. Therefore, even if you type in HTTP:// it will redirect to an https over a secured connection
- It allows users to perform secure e-commerce transaction, such as online banking.
- SSL technology protects any users and builds trust
- An independent authority verifies the identity of the certificate owner. So each SSL Certificate contains unique, authenticated information about the certificate owner.

Difference between HTTP and HTTPS:

Parameter	HTTP	HTTPS
Protocol	It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
Security	It is less secure as the data can be vulnerable to hackers.	It is designed to prevent hackers from accessing critical information. It is secure against such attacks.
Starts with	HTTP URLs begin with http://	HTTPs URLs begin with https://
Used for	It's a good fit for websites designed for information consumption like blogs.	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
Scrambling	HTTP does not scramble the data to be transmitted. That's why there is a higher chance that transmitted information is available to hackers.	HTTPS scrambles the data before transmission. At the receiver end, it descrambles to recover the original data. Therefore, the transmitted information is secure which can't be hacked.
Protocol	It operates at TCP/IP level.	HTTPS does not have any separate protocol. It operates using HTTP but uses encrypted TLS/SSL connection.
Domain Name Validation	HTTP website do not need SSL.	HTTPS requires SSL certificate.
Data encryption	HTTP website doesn't use encryption.	HTTPS websites use data encryption.
Search Ranking	HTTP does not improve search rankings.	HTTPS helps to improve search ranking.
Speed	Fast	Slower than HTTP
Vulnerability	Vulnerable to hackers	It Is highly secure as the data is encrypted before it is seen across a network.

Time Stamping Protocol:

- The Time-stamp protocol is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure.
- The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time.
- Timestamp based protocols start working as soon as a transaction is created.

Secure Electronic Transaction (SET):

- SET is an open encryption and security specification designed to protect credit card transactions on the internet.
- A set of security protocols and formats enables users to use the credit card payment infrastructure on an open network.
- It was first used in February 1996 and was proposed by Visa and Master Card.
- SET is in effect a set of protocols for ensuring security and confidentiality.

Key Features of SET:

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

Confidentiality of information:

- A credit card holder's personal and payment information is secured as it travels across the network.
- SET is that merchant/seller never sees the credit card number; this is only provided to the issuing bank.

Integrity of Data:

- Payment information sent from cardholders to merchants include order information, personal information and payment instructions.
- SET guarantees that these message contents are not altered in transit.
- RSA digital signatures, using SHA-1 hash codes provide message integrity.

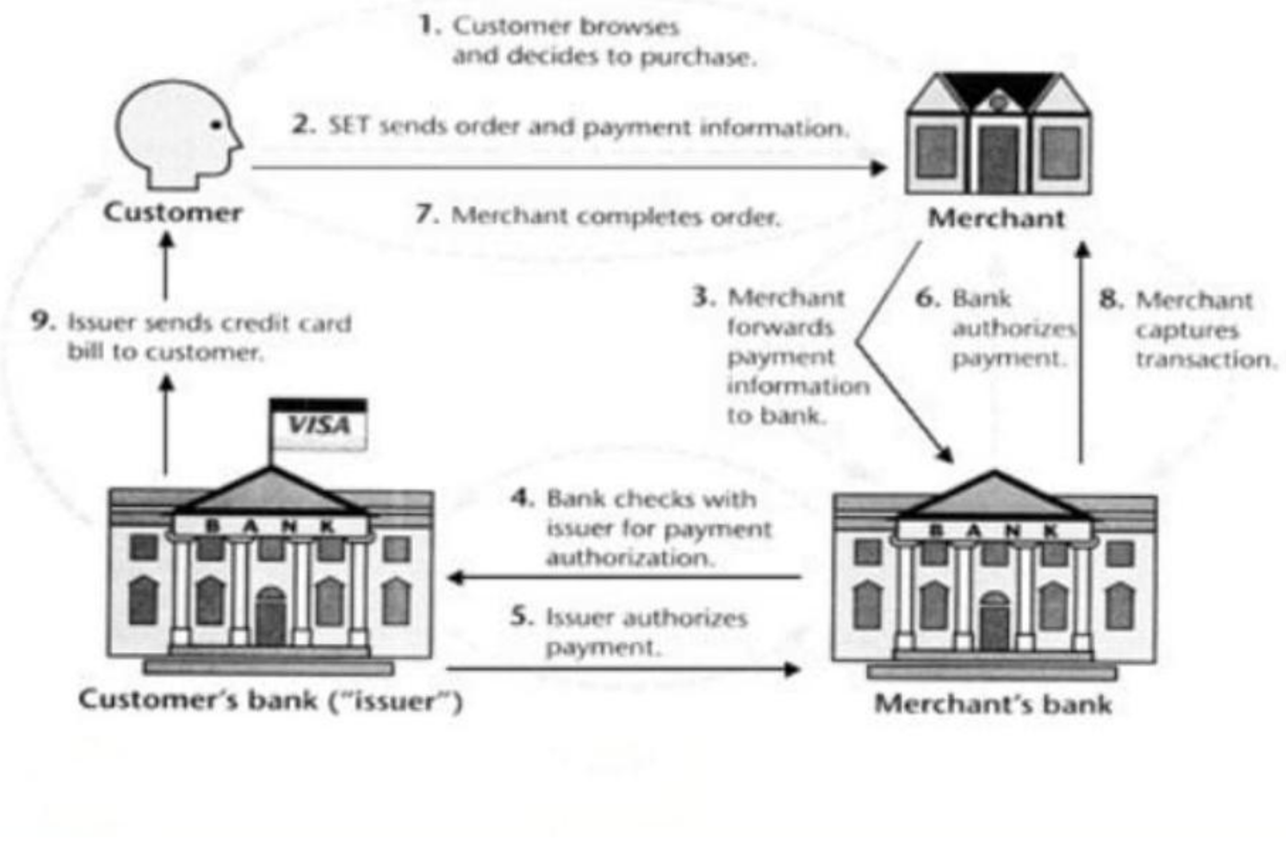
Cardholder account authentication:

- SET enables merchants to verify that a cardholder is legitimate user of a valid card account number.
- SET uses X.509v3 digital certificates with RSA signatures for this purpose.

Merchant authentication:

- SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards.
- SET uses X.509v3 digital certificates with RSA signatures for this purpose.

SET Transactions


1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
7. Merchant completes order.
Merchant
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
9. Issuer sends credit card bill to customer.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

User Authentication

- Authentication is the process of recognizing a user's identity.
- Authentication happens in two levels.
- A user or human visible level and a machine level.
- The human-level authentication is a simple login where you provide a net ID and a password to gain access.
- Machine level authentication is however more complex and involves a predetermined ID and password that only a machine authorized to access the network can know.
- These include both general authentication techniques (passwords, two-factor authentication [2FA], tokens, biometrics, transaction authentication, computer recognition, CAPTCHAs, and single sign-on [SSO]) as well as specific authentication protocols (including Kerberos and SSL/TLS).

Password:

- A password is a basic security mechanism that consists of a secret pass phrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination.

- A password is used to restrict access to a system, application or service to only those users who have memorized or stored and/or are authorized to use it.
- A password may also be called an access code, PIN or secret code.

Password authentication:

- Anyone who uses the internet is familiar with passwords, the most basic form of authentication. After a user enters his or her username, they need to type in a secret code to gain access to the network.
- If each user keeps their password private, the theory goes, unauthorized access will be prevented.
- To reduce this risk, users need to choose secure passwords with both letters and numbers, upper and lower case, special characters (such as $, %, or &), and no words found in the dictionary.
- It's also important to use long passwords of at least eight characters; each additional character makes it harder for a program to crack. Short, simple passwords such as "password" (one of the most common) and "12345" are barely better than no password at all.
- The most secure systems only allow users to create secure passwords, but even the strongest passwords can be at risk for hacking.
- Security experts have therefore developed more sophisticated authentication techniques to remedy the flaws of password-based systems.

Authentication Token:

- Token-based authentication is a protocol that generates encrypted security tokens. It enables users to verify their identity to websites, which then generates a unique encrypted authentication token.
- That token provides users with access to protected pages and resources for a limited period of time without having to re-enter their username and password.

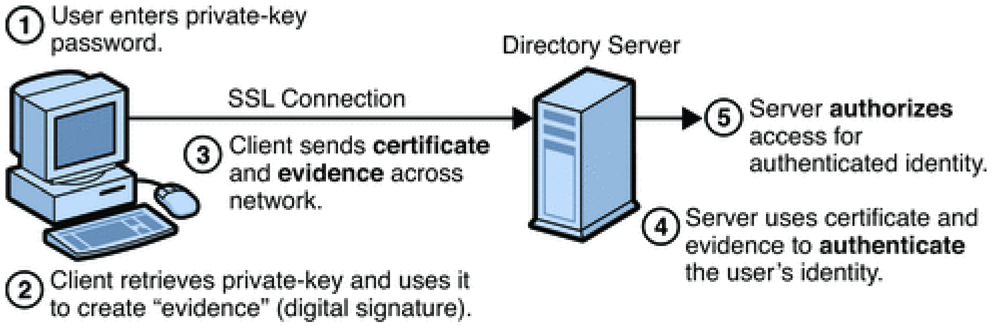
Token-based authentication works through this five-step process:

1. Request: The user logs in to a service using their login credentials, which issues an access request to a server or protected resource.
2. Verification: The server verifies the login information to determine that the user should have access. This involves checking the password entered against the username provided.
3. Token submission: The server generates a secure, signed authentication token for the user for a specific period of time.
4. Storage: The token is transmitted back to the user's browser, which stores it for access to future website visits. When the user moves on to access a new website, the authentication token is decoded and verified. If there is a match, the user will be allowed to proceed.
5. Expiration: The token will remain active until the user logs out or closes the server.

Certificate based authentication:

A certificate-based authentication server uses certificates and SSL (Single Sign On) to authenticate a user, machine or device. The method for authentication under the certificate method is quite simple.

- While authenticating a user to a server, the client has to digitally sign an electronically produced document or piece of data.
- Then, both the certificate and signed data are sent across the network.
- After the certificate and signed data are received, the server authenticates the user's identity based on the certificate.
- Then, the user is authenticated and allowed access to the network.


1 User enters private-key password.
Directory Server
SSL Connection
3 Client sends certificate and evidence across network.
5 Server authorizes access for authenticated identity.
4 Server uses certificate and evidence to authenticate the user's identity.
2 Client retrieves private-key and uses it to create "evidence" (digital signature).

Biometric authentication:

- Biometric systems are the cutting edge of computer authentication methods. Biometrics (meaning "measuring life") rely on a user's physical characteristics to identify them.
- The most widely available biometric systems use fingerprints, retinal or iris scans, voice recognition, and face detection (as in the latest iPhones).
- Since no two users have the same exact physical features, biometric authentication is extremely secure. It's the only way to know precisely who is logging in to a system.

- **Advantage:** Biometrics are very difficult to fake. Spy movies make it seem simple to lift someone's fingerprint with tape, or replicate their retina with a false contact lens, but it's far more complicated than that. Biometrics are so specific and unique that they're almost foolproof in terms of authentication.

- **Disadvantage:** The downside to this method is that it requires specialized scanning equipment, which is not ideal for some industries, and can be overly expensive for small businesses.

Chapter-7

TCP:

TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network. Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins. It then breaks large amounts of data into smaller packets, while ensuring data integrity is in place throughout the process.

IP:

IP is the main protocol within the internet layer of the TCP/IP. Its main purpose is to deliver data packets between the source application or device and the destination using methods and structures that place tags, such as address information, within data packets.

TCP/IP:

TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol.

The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

1. Network Access Layer –

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.
- It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
- We just talked about ARP being a protocol of Internet layer.

2. Internet Layer –

- This layer parallels the functions of OSI's Network layer.
- It defines the protocols which are responsible for logical transmission of data over the entire network.
- The main protocols residing at this layer are:

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.

IP has 2 versions:IPv4 and IPv6.

2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer – (Transport layer):

- This layer is analogous to the transport layer of the OSI model.
- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.
- The two main protocols present in this layer are:

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism.
2. **User Datagram Protocol (UDP) –** It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

- This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.
- It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

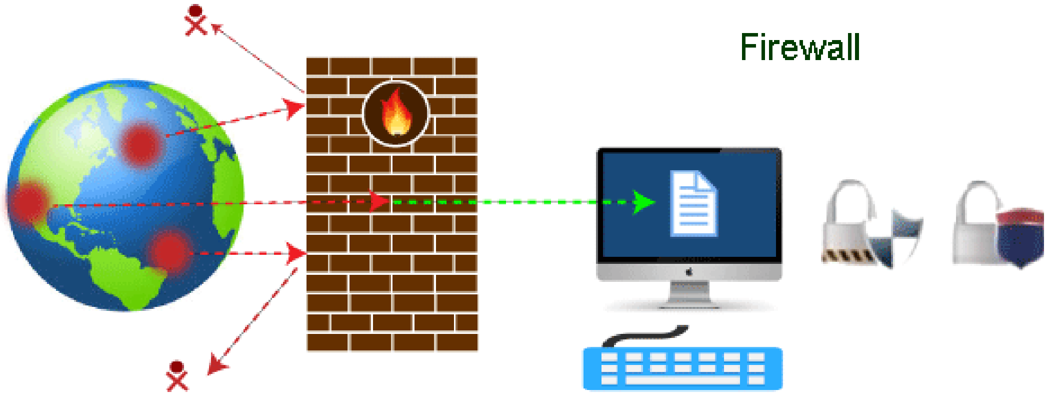
1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate and carry out bank transactions.
2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Firewall:

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules.
- It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the internet in infected computers.
- The firewall comes at both levels, i.e., hardware and software.
- A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router.
- On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

How does a firewall work?

- A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.
- Typically, firewalls intercept network traffic at a computer's entry point, known as a port.
- Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules.
- Incoming traffic is allowed only through trusted IP addresses, or sources.



Features of firewall:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support

Prepared by: Pratibha Patnaik

- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

IP Security:

The IP security (IPsec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 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.

Uses of IP Security –

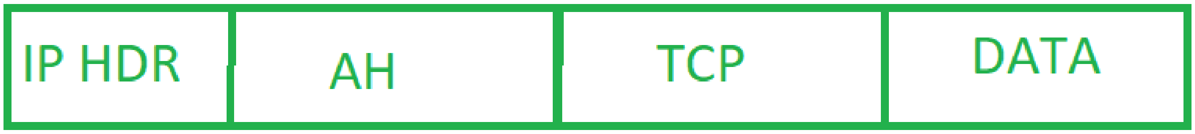
IPsec can be used to do the following things:

- 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 is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

Components of IP Security –

It has the following components:

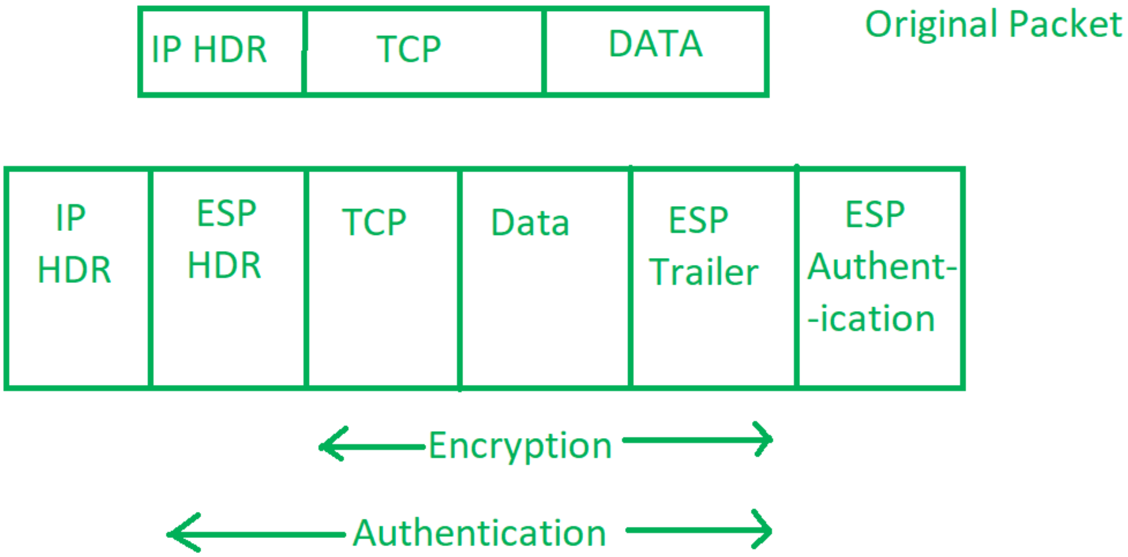
1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti-replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti-replay and it does not provide encryption. The anti-replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.



Internet Key Exchange (IKE) –

- It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
- The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.
- The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange.
- ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

- Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.
- The algorithm's IP sec users produces a unique identifier for each packet.
- This identifier then allows a device to determine whether a packet has been correct or not.
- Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

VPN:

A **virtual private network (VPN)** is a series of virtual connections routed over the internet which encrypts your data as it travels back and forth between your client machine and the internet resources you're using, such as web servers.

PCs, smartphones, tablets, dedicated servers, and even some IoT devices can be endpoints for a VPN connection.

Let's understand VPN by an example:

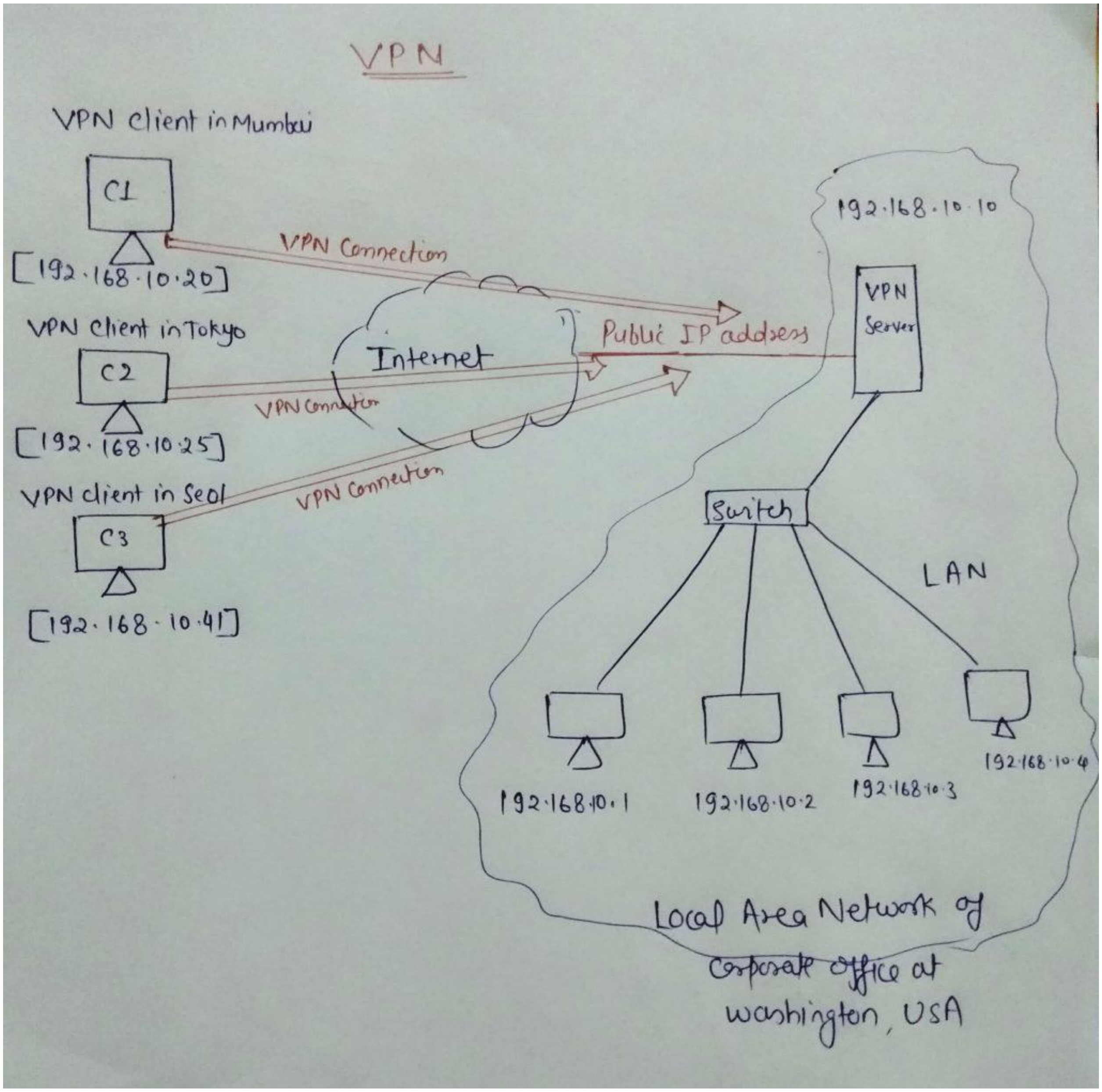
- Think of a situation where corporate office of a bank is situated in Washington, USA.
- This office has a local network consisting of say 100 computers. Suppose another branch of bank are in Mumbai, India and Tokyo, Japan.
- The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was very costly as well as troublesome job.
- VPN let us overcome this issue in an effective manner.

The situation is described below:

- All 100 hundred computers of corporate office at Washington are connected to the VPN server (which is a well configured server containing a public IP address and a switch to connect all computers present in the local network i.e., in US head office).
- The person sitting in the Mumbai office connects to The VPN server using dial up window and VPN server return an IP address which belongs to the series of IP addresses belonging to local network of corporate office.
- Thus, person from Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So, this is the intuitive way of extending local network even across the geographical borders of the country.

How does a VPN work?

- A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host.
- This means that if you surf online with a VPN, the VPN server becomes the source of your data.
- This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online.



What does a VPN hide?

1. Your browsing history

- It's no secret where you go on the internet. Your internet service provider and your web browser can track just about everything you do on the internet.
- A lot of the websites you visit can also keep a history.
- Web browsers can track your search history and tie that information to your IP address.
- These are just a few isolated examples.

- Keep in mind your internet service provider may be able to sell your browsing history.
- Even so-called private browsers may not be so private.

2. Your IP address and location

- Anyone who captures your IP address can access what you’ve been searching on the internet and where you were located when you searched.
- Think of your IP address as the return address you’d put on a letter. It leads back to your device.
- Since a VPN uses an IP address that’s not your own, it allows you to maintain your online privacy and search the web anonymously.
- You’re also protected against having your search history gathered, viewed, or sold. Keep in mind, your search history can still be viewed if you are using a public computer or one provided by your employer, school, or other organization.

3. Your location for streaming

- You might pay for streaming services that enable you to watch things like professional sports.
- When you travel outside the country, the streaming service may not be available.
- There are good reasons for this, including contractual terms and regulations in other countries.
- Even so, a VPN would allow you to select an IP address in your home country.
- That would likely give you access to any event shown on your streaming service. You may also be able to avoid data or speed throttling.

4. Your devices

- A VPN can help protect your devices, including desktop computer, laptop, tablet, and smart phone from prying eyes.

- Your devices can be prime targets for cybercriminals when you access the internet, especially if you’re on a public Wi-Fi network.

- In short, a VPN helps protect the data you send and receive on your devices so hackers won’t be able to watch your every move.

5. Your web activity — to maintain internet freedom

- Hopefully, you’re not a candidate for government surveillance, but who knows.
- Remember, a VPN protects against your internet service provider seeing your browsing history.
- So, you’re protected if a government agency asks your internet service provider to supply records of your internet activity.
- Assuming your VPN provider doesn’t log your browsing history (some VPN providers do), your VPN can help protect your internet freedom.