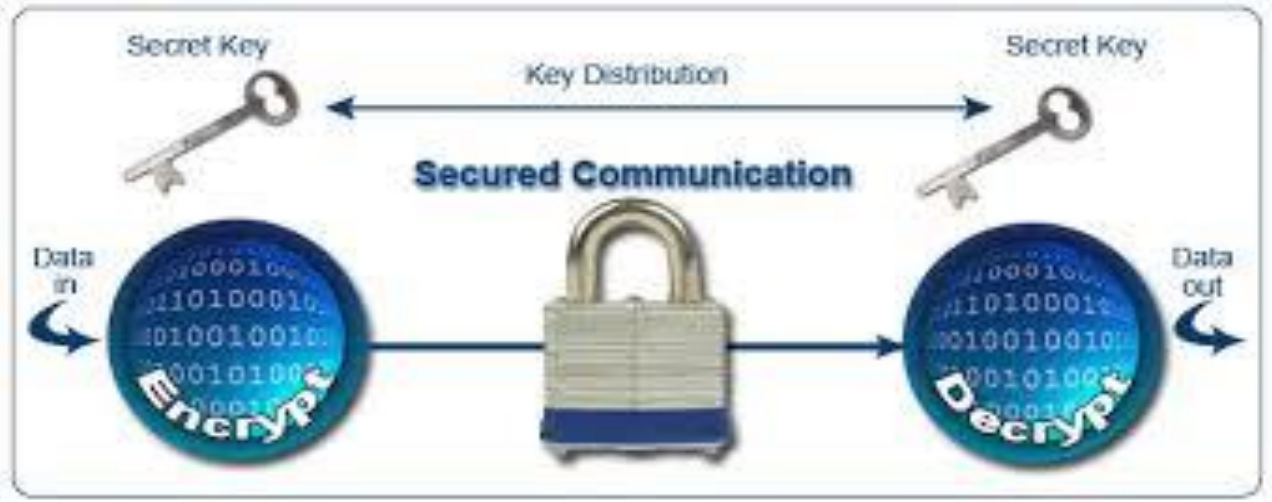
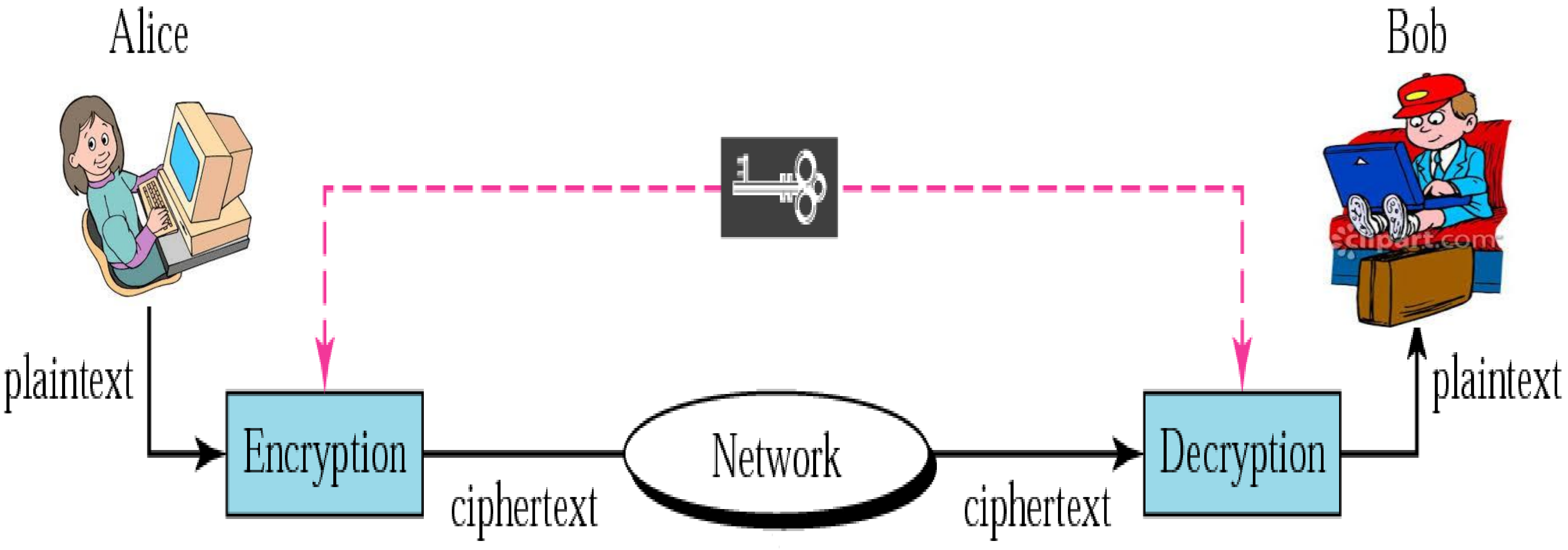
Chapter – VIII
Communication Security

Cryptography



Basic situation in cryptography

- It is nothing but a secret writing.
- Art of achieving security by encoding messages to make them non-readable.



Basic situation in cryptography

- A(lice) sends a message (or file) to B(ob) through an open channel (say, Internet), where E(vil, nemy) tries to read or change the message

- A will encrypt the plaintext using a key transforming it into a “unreadable” cipher

- B also has a key (say, the same key) and decrypts the cipher to get the plaintext

Terminology – cryptoterms

- Cryptology – The science of secure (often secret) communication
- Cryptography – The study of principles and techniques through which information can be hidden in a cipher (= secret writing)
- Cipher – secret or disguised writing (= zero)
- Cryptanalysis – The science and art to recreate the information in a cipher without knowing the key (before hand)
- Cryptanalyst is a person who attempts to break a cipher text message to obtain the original plain text message.

Cryptography Techniques………

- Substitution Techniques - *plaintext characters are replaced by other characters ,numbers or symbols.*
  - Caesar Cipher
  - Modified Caesar Cipher
  - Mono-alphabetic Cipher
  - Homophonic Cipher
  - Polygram Cipher
  - Poly-alphabetic Cipher
  - Playfair Cipher

- Transposition Techniques – *Performs some permutations over the plain text characters.*
  - Rail Fence Technique
  - Simple Columnar Technique
  - Vernam Cipher (One-Time pad)

Substitution Technique

Caesar Cipher

- Scheme is proposed by Julian Caesar.
- Replace each letter of the alphabet with the letter standing 3 places further down the alphabet
- It is very weak technique.

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

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
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

Substitution Technique

Modified Caesar Cipher

Substitution Techniques

- Caesar Cipher
- **Modified Caesar Cipher**
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

- Each alphabet in PT is not necessarily be replaced by an alphabet 3 places down the line but instead can be any places down to form CT.

i.e. Plain text (PT) characters can be replaced by 5 places down to generate Cipher text (CT)
Or Plain text (PT) characters can be replaced by 6 places down to generate Cipher text (CT)
Or Plain text (PT) characters can be replaced by 8 places down to generate Cipher text (CT) etc

Substitution Technique

Mono-alphabetic Cipher

- Rather than using a uniform scheme for all the alphabets in a given PT, the random substitution is used.

- Each alphabet in PT,
  - each A can be replaced by any other alphabet (B through Z),
  - B can be replaced by A or C through Z and so on.

Substitution Technique

Homophonic Cipher

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

- One PT alphabet can map to more than one CT alphabet.

- i.e. If from PT, alphabet A can be replaced by different alphabets like D, H, P, B, X for their every occurrence in the PT.

Substitution Technique

Polygram Cipher

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

- A block of alphabet from PT is replaced by a another block of alphabets to form CT.
- For e.g every *THIS* in the PT could be replaced by *PHAL* and *IS* could be replaced by *JK*.

Substitution Technique

Poly-alphabetic Cipher

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

- Invented by Leon Battista in 1568.
- Vigenere Cipher & Beaufort Cipher are the examples.

- Uses multiple one character keys.
- Each of the keys encrypts one PT character . First key encrypts the first PT character, second key encrypts second & so on.
- After all the keys are used, they are recycled.

Substitution Technique

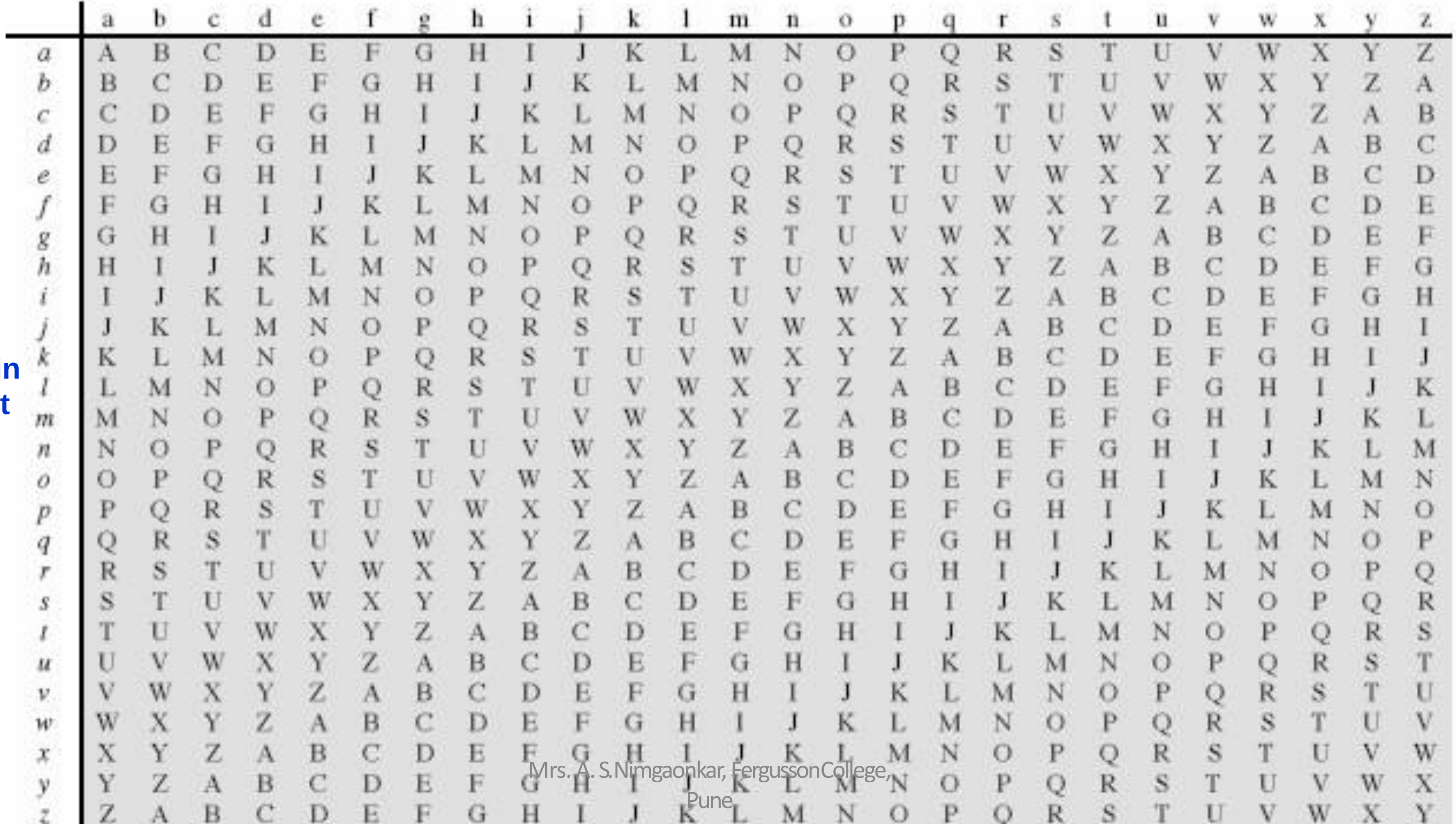
Poly-alphabetic Cipher

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

Key

Plain text



	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

Substitution Technique

Playfair Cipher

Substitution Techniques

- **Caesar Cipher**
- **Modified Caesar Cipher**
- **Mono-alphabetic Cipher**
- **Homophonic Cipher**
- **Polygram Cipher**
- **Poly-alphabetic Cipher**
- **Playfair Cipher**

- The Playfair Cipher is an example of multiple-letter encryption.

- Invented by *Sir Charles Wheatstone* in 1854, but named after his friend Baron Playfair who championed the cipher at the British foreign office.

- Based on the use of a 5x5 matrix in which the letters of the alphabet are written (**I** is considered the same as **J**)

- This is called *key matrix* or *keyword*.

Substitution Technique

Playfair Cipher

Substitution Techniques

- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

Creation & Population of a matrix

- A 5X5 matrix of letters based on a keyword
- Fill in letters of keyword (no duplicates)
- Left to right, top to bottom
- Fill the rest of matrix with the other letters in alphabetic order

Substitution Technique

Playfair Cipher

Encrypting and decrypting with Playfair

- The plaintext is encrypted two letters at a time:

1. Break the plaintext into pairs of two consecutive letters
2. If a pair is a repeated letter or only one is left, insert a filler like 'X‘ in the plaintext, eg. "balloon" is treated as "ba lx lo on"
3. If both letters fall in the same row of the key matrix, replace each with the letter to its right.
4. If both letters fall in the same column, replace each with the letter below it.
5. Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair.

Substitution Technique

Playfair Cipher

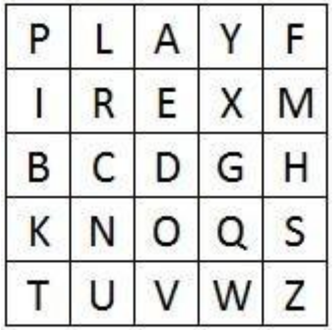
Encrypting and decrypting with Playfair

Substitution Techniques

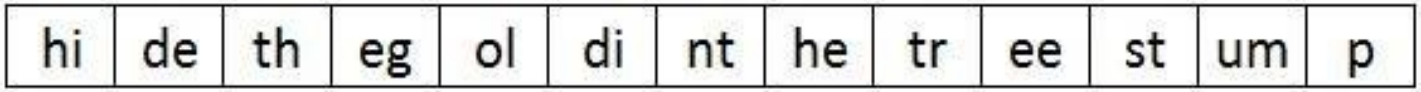
- Caesar Cipher
- Modified Caesar Cipher
- Mono-alphabetic Cipher
- Homophonic Cipher
- Polygram Cipher
- Poly-alphabetic Cipher
- Playfair Cipher

Eg: hide the gold in the tree stump

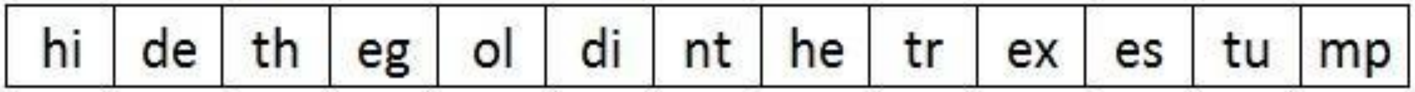
Keyword: Playfair



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

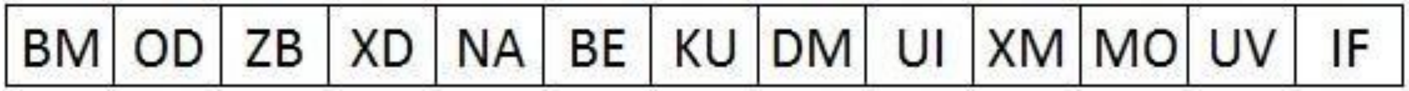


hi	de	th	eg	ol	di	nt	he	tr	ee	st	um	p



hi	de	th	eg	ol	di	nt	he	tr	ex	es	tu	mp

Decryption



BM	OD	ZB	XD	NA	BE	KU	DM	UI	XM	MO	UV	IF

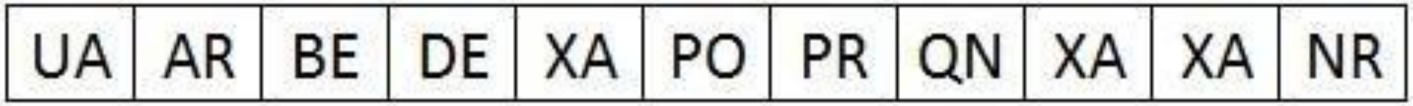
Substitution Technique

Playfair Cipher

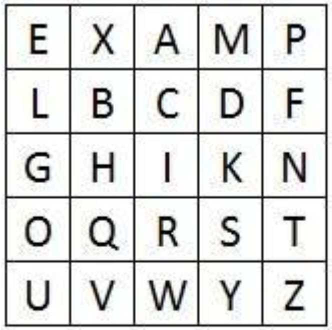
Encrypting and decrypting with Playfair

Eg: UA ARBED EXAPO PR QNXAXANR

Keyword: Example

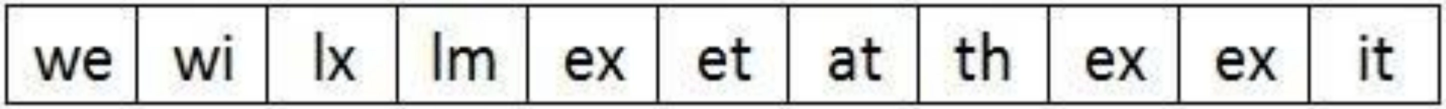


UA	AR	BE	DE	XA	PO	PR	QN	XA	XA	NR



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

Encryption



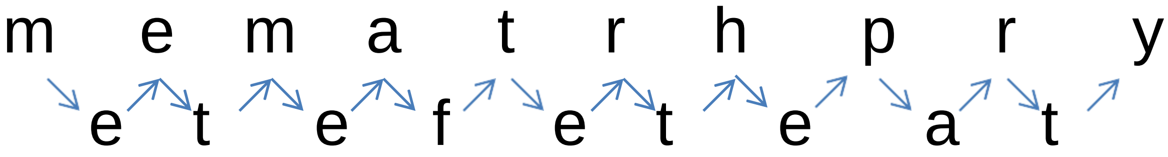
we	wi	lx	lm	ex	et	at	th	ex	ex	it

Plain Text: We will meet at the exit

Transposition Technique

Rail Fence Technique

- Write plaintext letters diagonally over a number of rows, then read off cipher row by row.
- E.g., with a rail fence of depth 2, to encrypt the text “meet me after the party”, write message out as:



m e m a t r h p r y

e t e f e t e a t

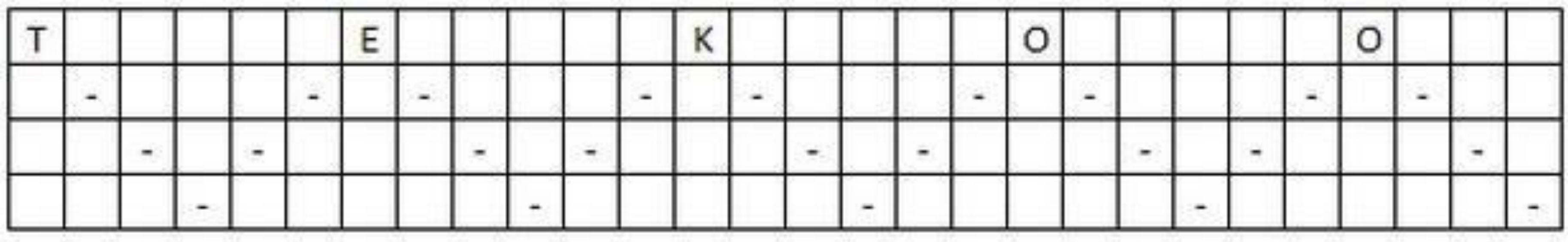
Transposition Technique

Transposition Techniques

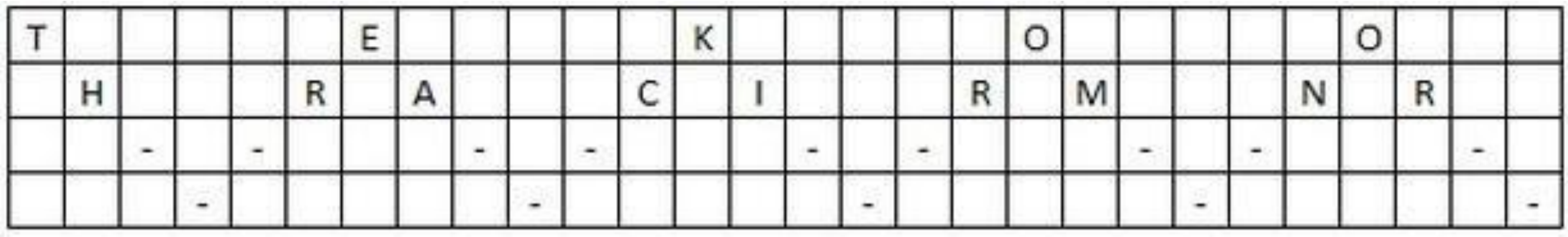
- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

Rail Fence Technique

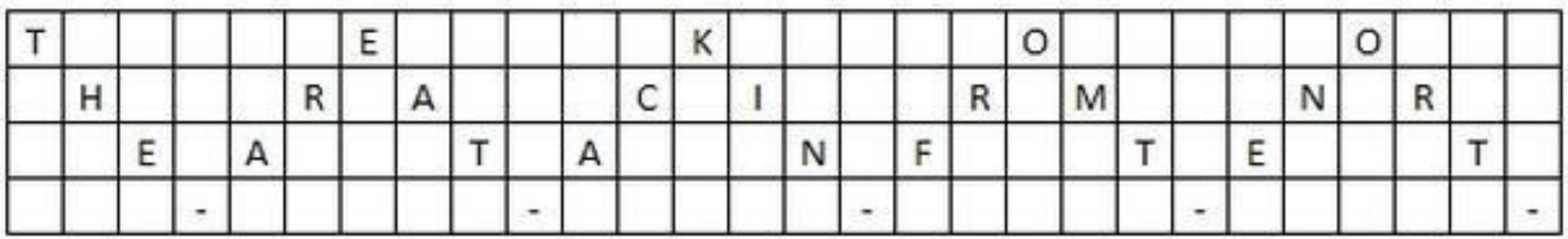
- Cipher text: TEKOOHRACIRMNREATANFTETYTGHH



T						E						K						O						O			
	-				-		-				-		-				-		-				-		-		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-



T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-



T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		E		A				T		A				N		F				T		E				T	
			-						-						-						-						-

Transposition Technique

Transposition Techniques
- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

Rail Fence Technique

- Cipher text: TEKOOHRACIRMNREATANFTETYTGHH

T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		-		-				-		-				-		-				-		-				-	
			-						-						-						-						-

T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		E		A				T		A				N		F				T		E				T	
			-						-						-						-						-

T						E						K						O						O			
	H				R		A				C		I				R		M				N		R		
		E		A				T		A				N		F				T		E				T	
			Y						T						G						H						H

Plain Text: "they are attacking from the north".

Transposition Technique

Rail Fence Technique

Decrypt the following with the key 5

ASNODANETISOTNMVNEMEGWFBAOGSWEREIHALVNSBTLI

Transposition Technique

Transposition Techniques

- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

Simple Columnar Technique

- Write letters of message out in rows over a *specified number of column*.
- Reading the *cryptotext column-by-column*, with the columns permuted according to some key.
- Example:“attack is postponed until two am” with key 3421567

Transposition Technique

Simple Columnar Technique

Example :

Encrypt Plain text ***“the tomato is a plant in the nightshade family”***

using keyword ***tomato***.

Transposition Technique

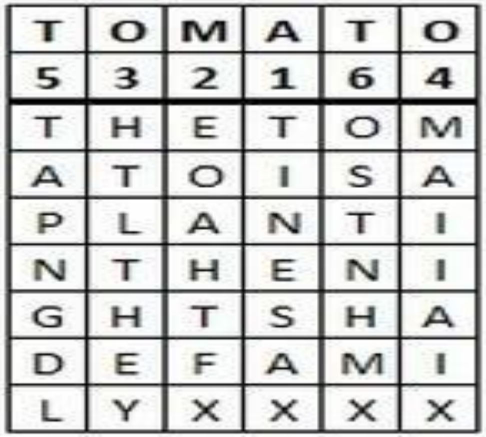
Simple Columnar Technique

Encryption:

1. Write letters of message out in rows over a *specified number of column.*
2. the number of columns is the number of letters in the keyword.
3. We take the letters in the keyword in alphabetical order, and read down the columns in this order.
4. If a letter is repeated, we do the one that appears first, then the next and so on.

Plain Text: The tomato is a plant in the nightshade family

Keyword: *tomato*

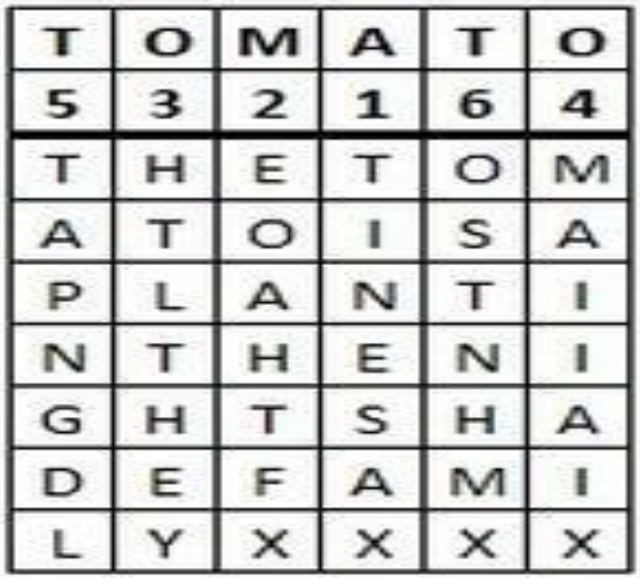


T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

Transposition Technique

Simple Columnar Technique

Encryption:



T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

- Starting with the column headed by "A“- "TINESAX“
- "TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / TAPNGDL/ OSTNHMX"
- The final cipher text TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX

Transposition Technique

Simple Columnar Technique

Transposition Techniques
- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

Decryption:

- Write down keyword & alphabetical order of the keyword
- Count the number of cipher text characters. Say **CT_Count**
- Count the number of Keyword characters. Say **Key_Count**
- **Calculate No_rows = CT_count / Key_Count**
- Start Writing the cipher text from 1st numbered(which we numbered in sequence) column until you reach last row.
- For generating Plain text back read the grid row wise

Tip : Write Column-wise, read row-wise

Transposition Technique

Simple Columnar Technique

- Decryption:

  "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" ,keyword *potato*

Transposition Techniques

- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

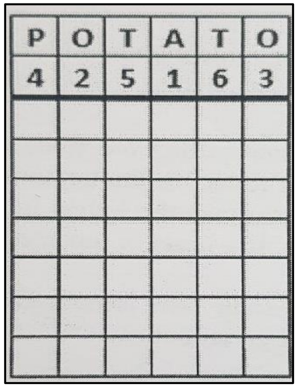
Transposition Technique

Simple Columnar Technique

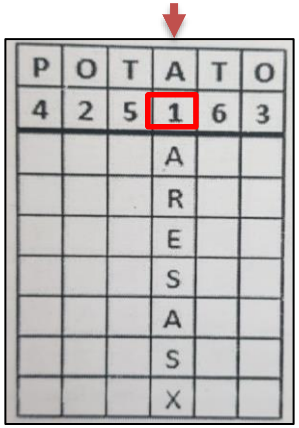
- Decryption:

"ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" ,keyword *potato*

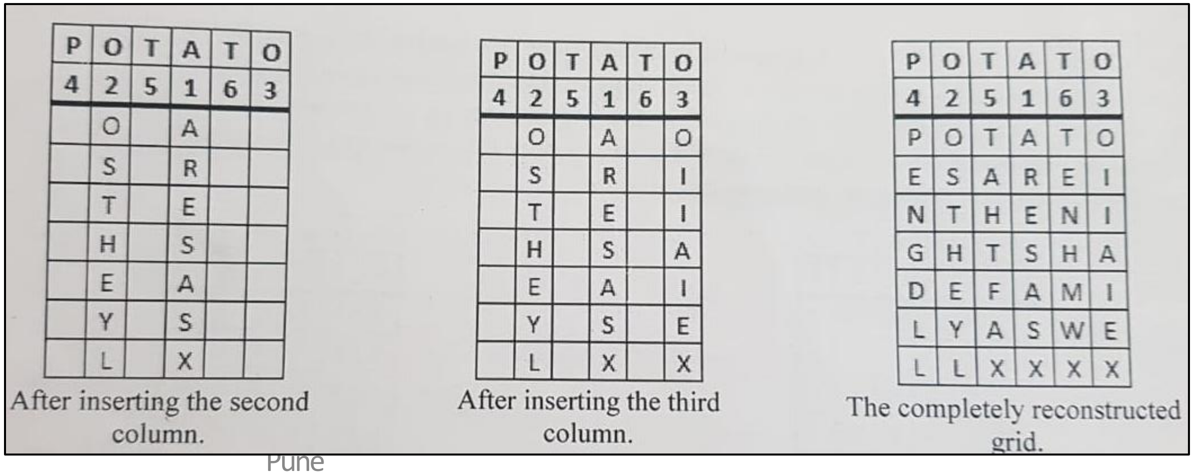
1. Write down keyword & alphabetical order of the keyword
2. Count the number of cipher text characters. Say **CT_Count = 42**
3. Count the number of Keyword characters. Say **Key_Count = 6**
4. **Calculate No_rows = CT_count / Key_Count = 42/6 = 6**
5. Start Writing the cipher text from 1st numbered(which we numbered in sequence) column until you reach last row.
6. For generating Plain text back read the grid row wise



P	O	T	A	T	O
4	2	5	1	6	3



P	O	T	A	T	O
4	2	5	1	6	3
			A		
			R		
			E		
			S		
			A		
			S		
			X		



P	O	T	A	T	O
4	2	5	1	6	3
	O		A		
	S		R		
	T		E		
	H		S		
	E		A		
	Y		S		
	L		X		

After inserting the second column.

P	O	T	A	T	O
4	2	5	1	6	3
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

After inserting the third column.

P	O	T	A	T	O
4	2	5	1	6	3
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L	X	X	X	X

The completely reconstructed grid.

Transposition Technique

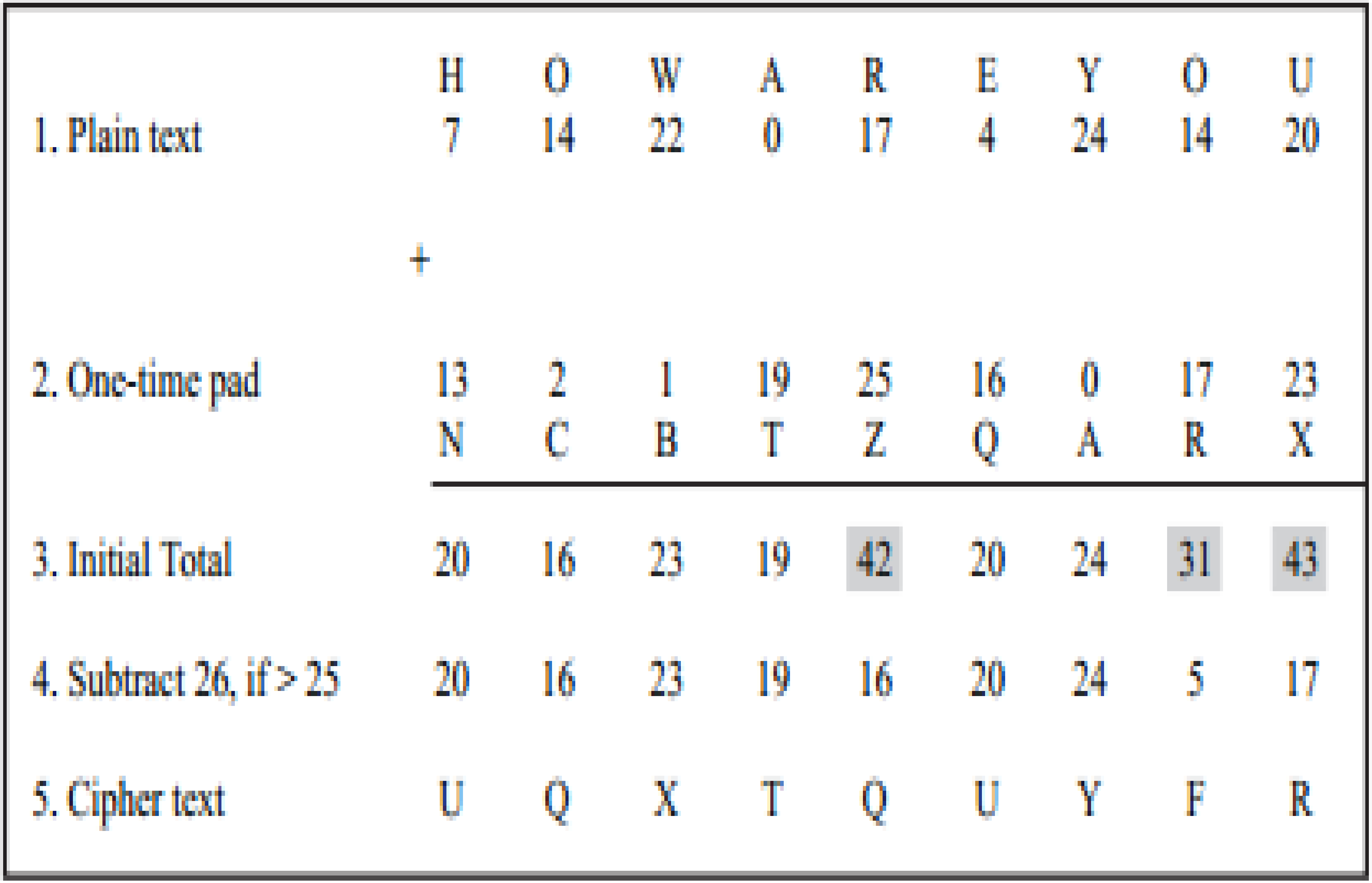
Vernam Cipher – One time pad

Transposition Techniques
- Rail Fence Technique
- Simple Columnar Technique
- Vernam Cipher (One-Time pad)

- Gilbert Sandford Vernam – inventor
- Unbreakable if and only if
  - Key is same length as plain text.
  - Key is never re-used hence one time pad.
- Steps :

1. Treat each plain text character as a number in an increasing sequence.
2. Do the same for input cipher text (key).
3. Add plain text & input cipher text.
4. If the sum produced is greater than 26, subtract 26 from it.
5. Translate each number back to alphabet.

Example of Vernam Cipher



	H	O	W	A	R	E	Y	O	U
1. Plain text	7	14	22	0	17	4	24	14	20
+									
2. One-time pad	13	2	1	19	25	16	0	17	23
	N	C	B	T	Z	Q	A	R	X
3. Initial Total	20	16	23	19	42	20	24	31	43
4. Subtract 26, if > 25	20	16	23	19	16	20	24	5	17
5. Cipher text	U	Q	X	T	Q	U	Y	F	R

Firewalls

What is a Firewall?

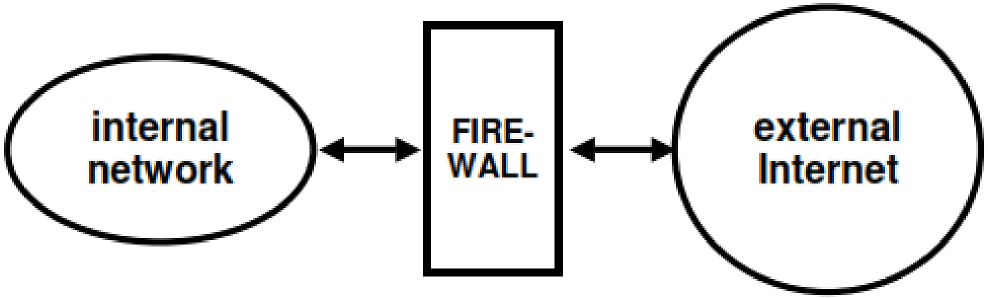
- A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources.

- You could think of a firewall as a traffic controller. It helps to protect your network and information by managing your network traffic.

What is a Firewall?

- Firewall is a specialized version of router.

- A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.



Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall and vice a versa
  - Only authorized traffic (defined by the local security police) will be allowed to pass

How does a firewall work?

- Inspects each individual "packet" of data as it arrives at either side of the firewall inbound to or outbound from your computer
- Determines whether it should be allowed to pass through or if it should be blocked

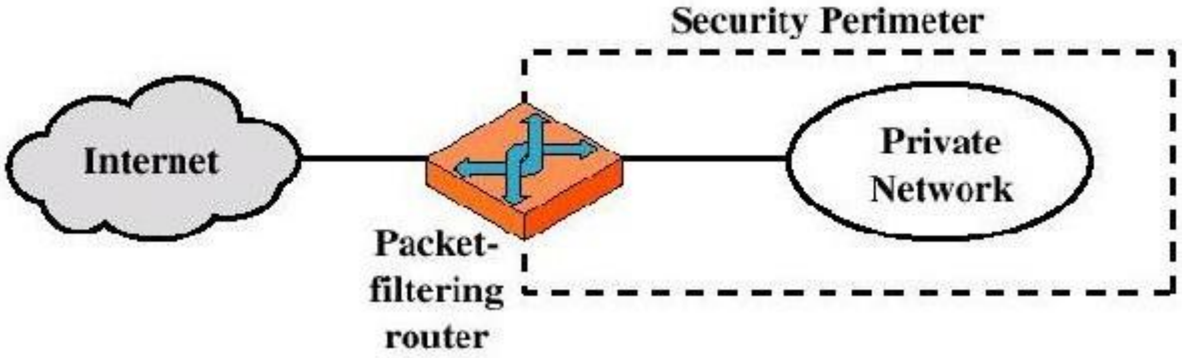
Firewall Rules

- Allow – traffic that flows automatically because it has been deemed as "safe" (Ex. Meeting Maker, Eudora, etc.)
- Block – traffic that is blocked because it has been deemed dangerous to your computer
- Ask – asks the user whether or not the traffic is allowed to pass through

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
    - Circuit-level gateways (Bastion host)

Packet-filtering Router..Screening router



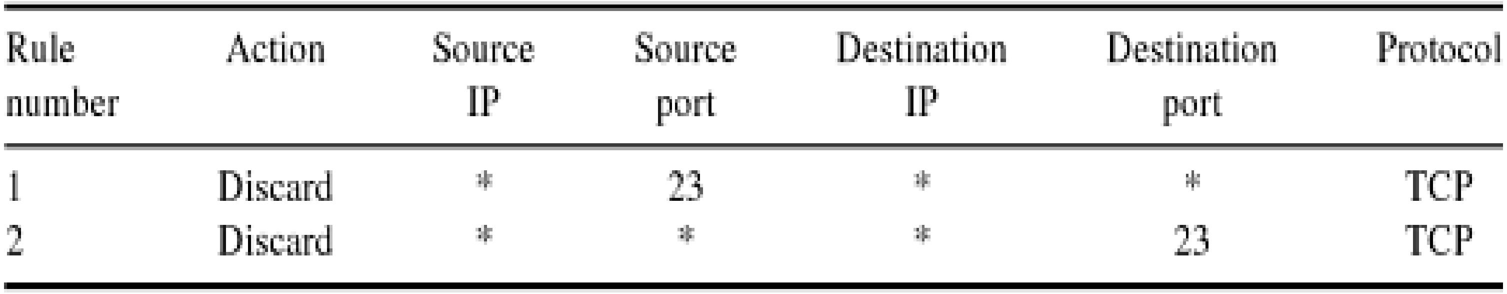
- Applies a set of rules to each incoming IP packet and then forwards or discards the packet

- Filter packets can pass in both directions

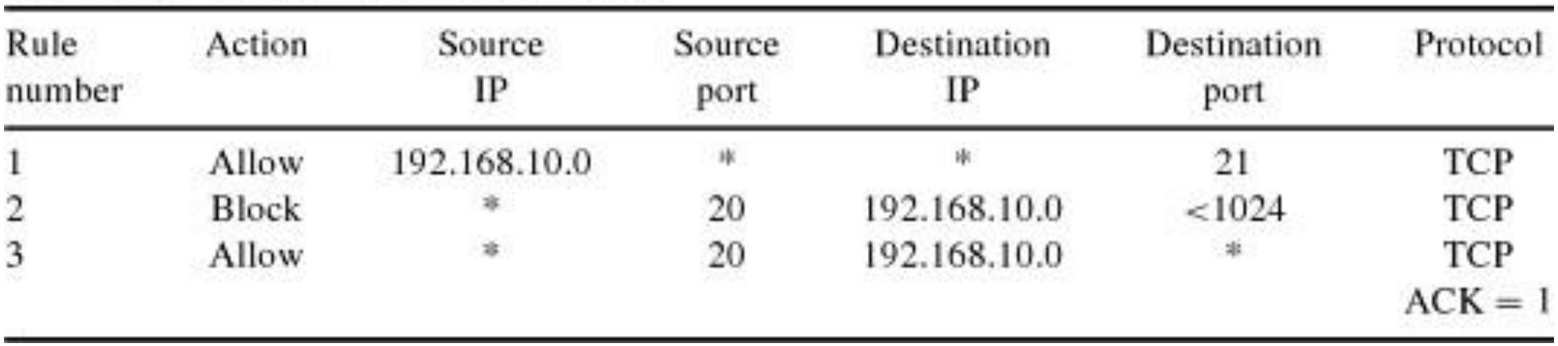
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header

- Two default policies (discard or forward)

Packet-filtering Router..Screening router



Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Discard	*	23	*	*	TCP
2	Discard	*	*	*	23	TCP



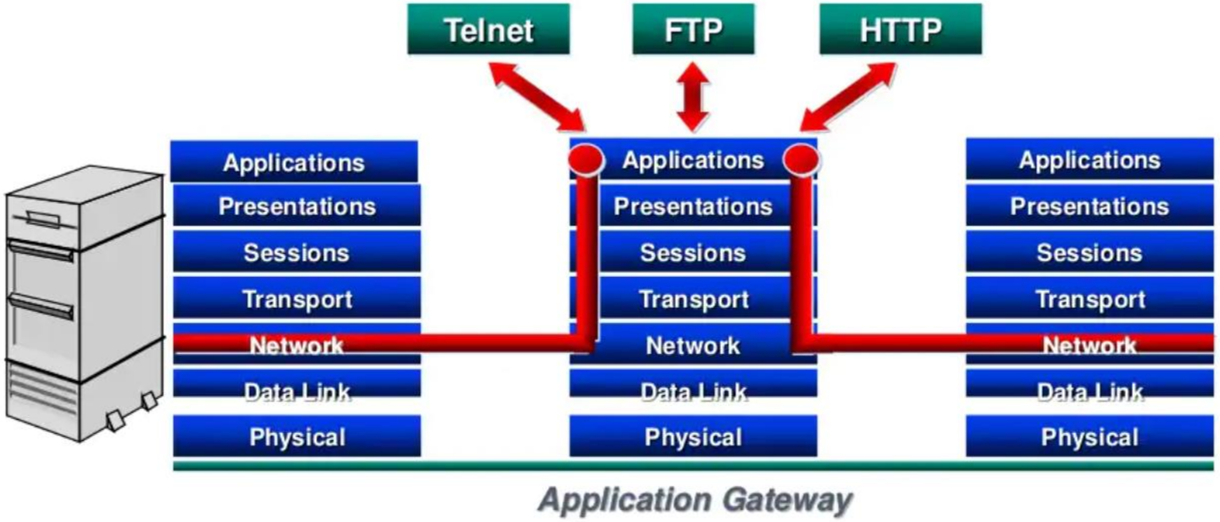
Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Allow	192.168.10.0	*	*	21	TCP
2	Block	*	20	192.168.10.0	<1024	TCP
3	Allow	*	20	192.168.10.0	*	TCP ACK = 1

Packet-filtering Router..Screening router

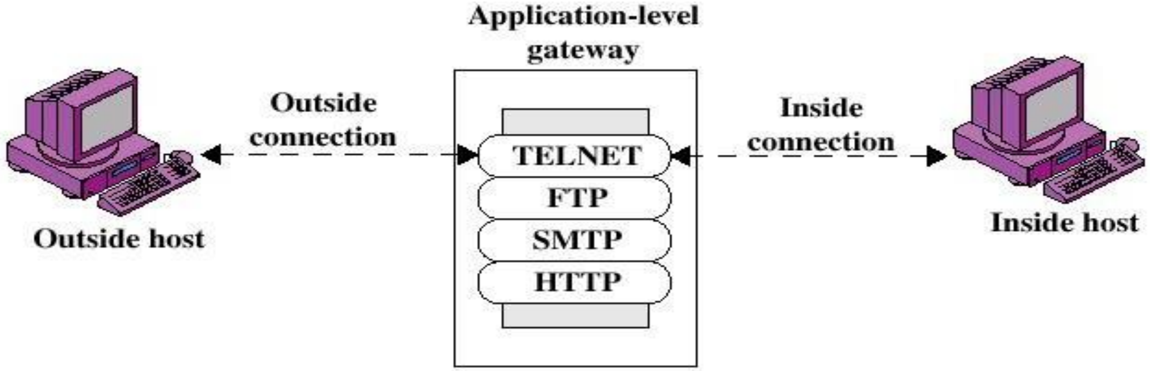
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication
- Possible attacks
  - IP address spoofing
  - Tiny fragment attacks

Application-level Gateway – Proxy server

- In such type of firewall remote host or network can interact only with proxy server, proxy server is responsible for hiding the details of the internal network
- i.e. intranet.
- User uses TCP/IP applications, such as FTP and Telnet servers.
- This is very effective, but can impose a performance degradation.

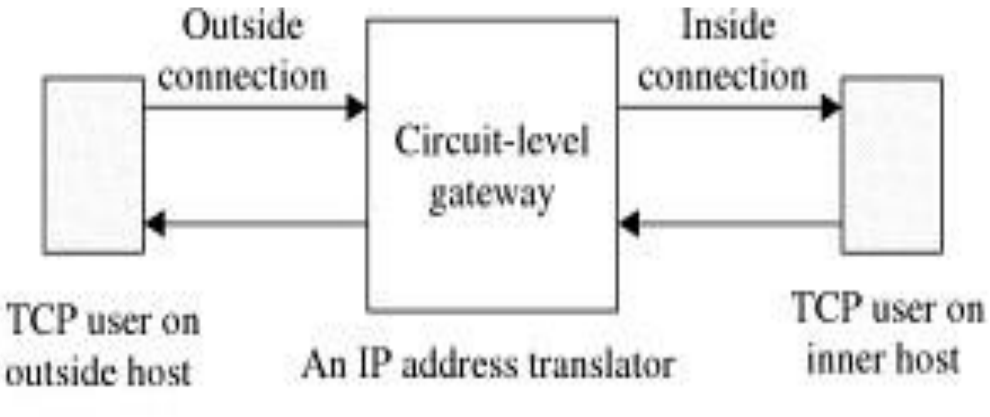


Application-level Gateway – Proxy server



- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)

Circuit-level Gateway – Specialized application gateway



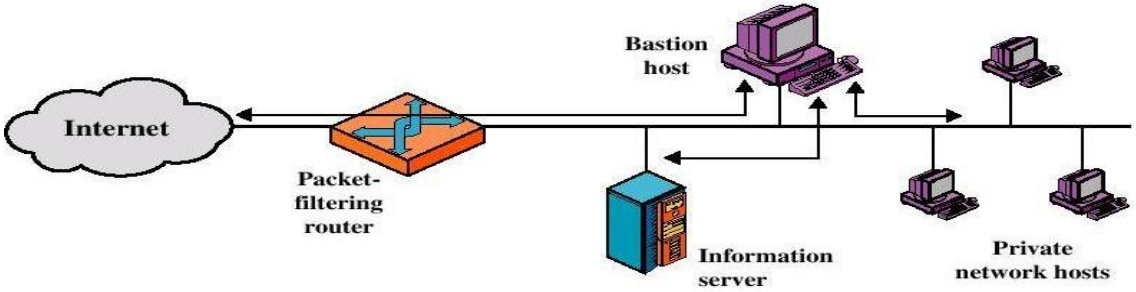
- Stand-alone system
- Sets up two TCPconnections
- The gateway typically relays TCP segments from one connection to the other without examining the contents

Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible

Firewall Configurations

- Screened host firewall system (single- homed bastion host)



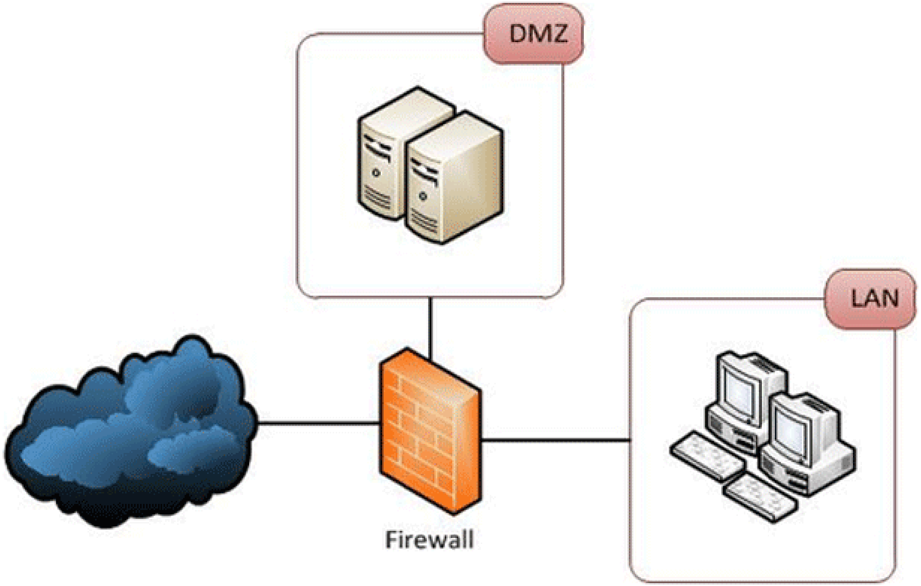
- Screened host firewall, single-homed bastion configuration
- Firewall consists of two systems:
  - A packet-filtering router
  - Application gateway(bastion host)

Demilitarized Zone (Networks) - DMZ

- Firewalls can be arranged as DMZ.
- It is required only if the organization has servers that it needs to make available to the outside world(web server, FTP)
- A DMZ is a **network (physical or logical) used to connect hosts that provide an interface to an untrusted external network** – usually the internet – while keeping the internal, private network – usually the corporate network – separated and isolated form the external network.

Demilitarized Zone (Networks) - DMZ

- Three network interfaces:
  - One interface connects to internal private network.
  - Other connects to external public network.(internet)
  - Last connects to the public servers.



Limitations of Firewalls

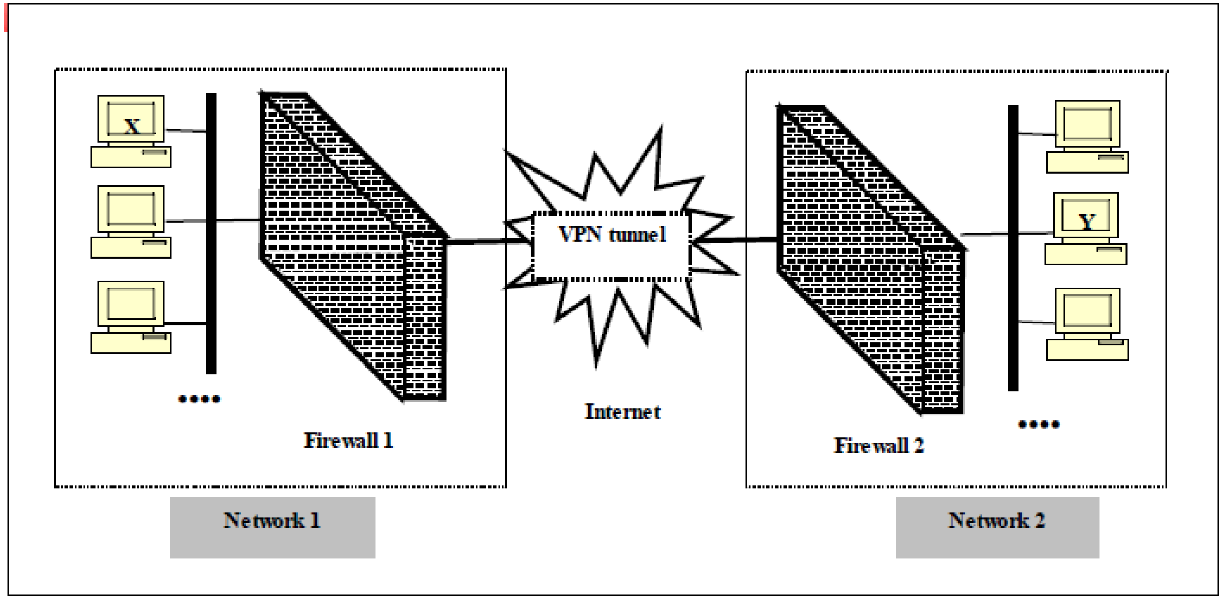
- Insider's intrusion:
  - If insider attacks the internal network, firewall cannot prevent such an attack.
- Direct internet traffic:
  - Effective only if it is the only entry exit point of an organization's network.
- Virus attack:
  - Cannot protect internal network from virus threat.
  - Cannot check every possible file or packet for virus content.
  - Separate virus detection is required.

Virtual Private Network VPN

Prepared by : Mrs. Arati Nimgaonkar

Introduction

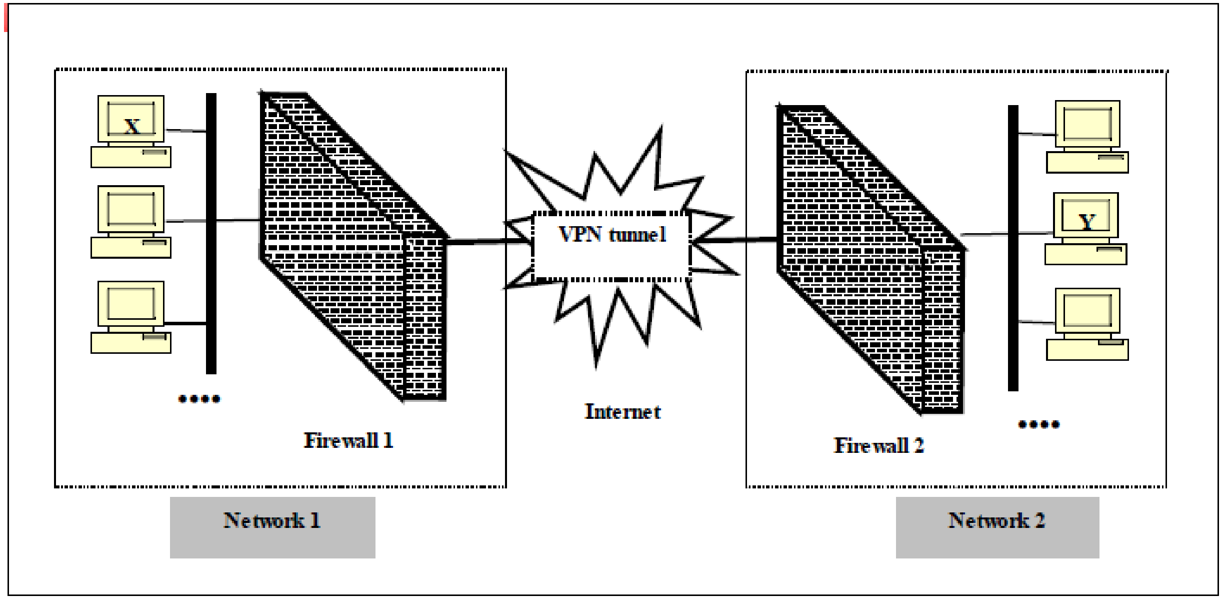
- **Public Network:** is a large collection of communicators who are unrelated to each other.
- Eg: public telephone network, internet.
- They are less expensive to use and also easily available.
- **Private Network:** is made up of computers owned by single organization, which share information with each other.
- Eg: LAN, WAN, MAN
- They are secure and available.
- A firewall separates a private network from a public network.



- A VPN can connect distant networks of an organization or it can be used to allow travelling users to remotely access private network (organization network) securely over Internet.
- A VPN is used to simulate a private network over the public network.
- Virtual Connections are temporary and do have physical existence.

VPN Architecture

- Organization wants to connect its two networks , Network1 and network 2 which are physically apart from each other through the VPN.
- Two firewalls are set up, firewall1 and firewall2, which are virtually connected to each other over the internet.
- VPN protects traffic passing between any two hosts on two different networks.



- X on Network 1 wants to send data to Y on network 2. the transmission process:
- Host creates a packet with its own IP address as source and IP address of Y as the destination address.
- The packet reaches the firewall1, which adds its own header.
- The new header contains the IP address of the firewall1 as the new source address and IP address of firewall2 as the new destination address.
- It performs the encryption, authentication and sends the packet.

Intrusion

Prepared by : Mrs. Arati Nimgaonkar

Definitions

- ***Intrusion detection:*** is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *intrusions (incidents).*
- ***Intrusion detection system (IDS):*** is software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities.
- ***Intrusion prevention system (IPS):*** is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Intrusion Detection System(IDS)

- Two categories of IDS –
  - Statistical based –
    - Behavior of users over time is captured as statistical data and processed.
    - Rules are applied to test whether the user behavior was legitimate or not.
- Rule base Detection
  - Set of rules is applied to see if a given behavior is suspicions to be classified as an attempt to intrude.

Honeypots

- Modern intrusion detection systems make use of honey pots.
- It is a trap which attracts potential attackers.
- A **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

- It consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.
- They have sensors , loggers which alarm the administrators of any user actions.