UNIT –I

Introduction:

This is the age of universal electronic connectivity, where the activities like hacking, viruses, electronic fraud are very common. Unless security measures are taken, a network conversation or a distributed application can be compromised easily.

Some simple examples are:

- Online purchases using a credit/debit card.
- A customer unknowingly being directed to a false website.
- A hacker sending a message to a person pretending to be someone else.

Network Security has been affected by two major developments over the last several decades. First one is introduction of computers into organizations and the secondone being introduction of distributed systems and the use of networks and communication facilities for carrying data between users & computers. These two developments lead to 'computer security' and 'network security', where the computer security deals with collection of tools designed to protect data and to thwart hackers. Network security measures are needed to protect data during transmission. But keep in mind that, it is the information and our ability to access that information that we are really trying to protect and not the computers and networks.

Why We Need Information Security?

Because there are threats

Threats

A threat is an object, person, or other entity that represents a constant danger to an asset

The 2007 CSI survey

- 494 computer security practitioners
- 46% suffered security incidents
- 29% reported to law enforcement
- Average annual loss $350,424
- 1/5 suffered _targeted attack'
- The source of the greatest financial losses?
- Most prevalent security problem
- Insider abuse of network access
- Email

Threat Categories

- Acts of human error or failure
- Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attack
- Forces of nature
- Deviations in quality of service
- Technical hardware failures or errors
- Technical software failures or errors

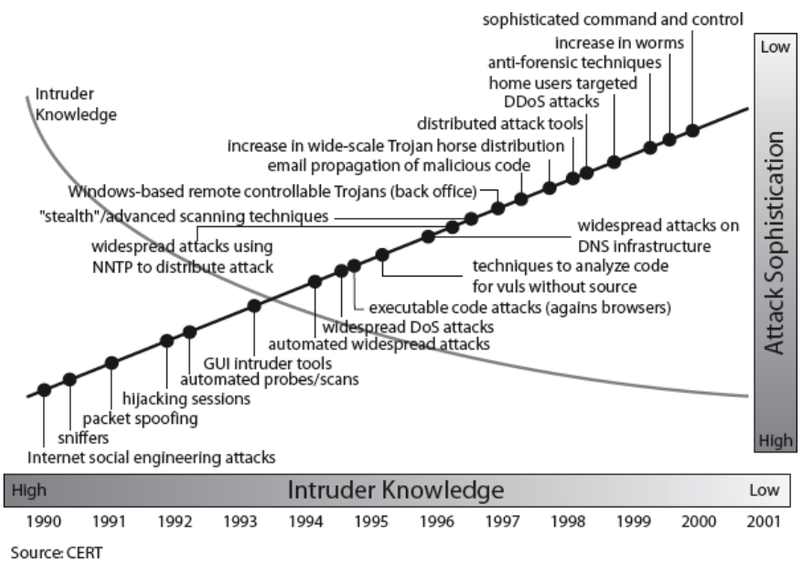
Technological obsolesce

Definitions

- **Computer Security** - generic name for the collection of tools designed to protectdata and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over acollection of interconnected networks

our focus is on **Internet Security**

which consists of measures to deter, prevent, detect, and correct securityviolations that involve the transmission & storage of information



ASPECTS OF SECURITY

- consider 3 aspects of information security:
  - *Security Attack*
  - **Security Mechanism**
  - *Security Service*

SECURITY ATTACK

- any action that compromises the security of information owned by anorganization
- information security is about how to prevent attacks, or failing that, to detectattacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks

can focus of generic types of attacks

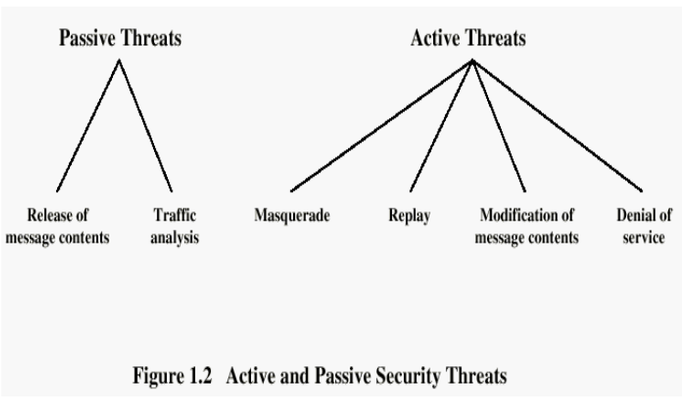
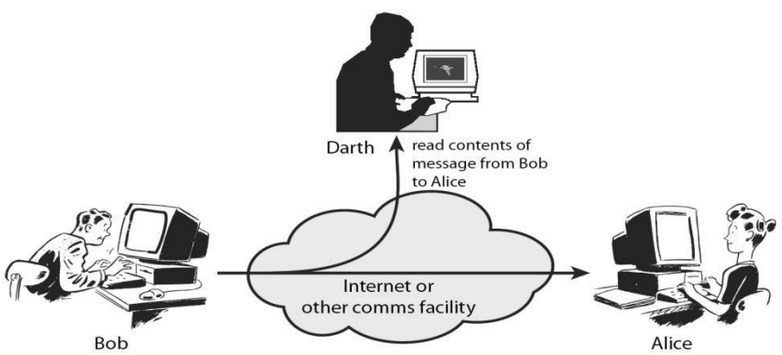
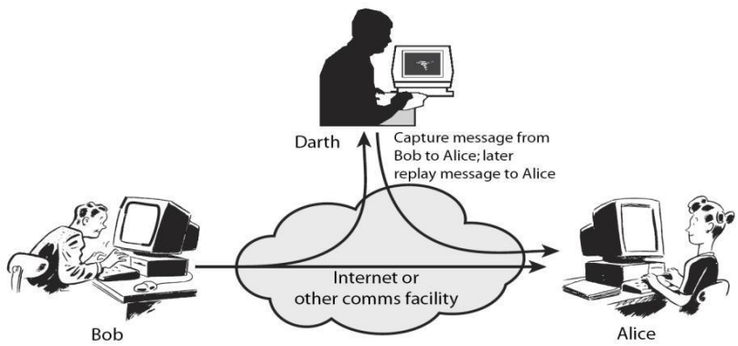


Figure 1.2 Active and Passive Security Threats

Passive Attack



Active Attack



INTERRUPTION

An asset of the system is destroyed or becomes unavailable or unusable. It is anattack on availability.

Examples:

- Destruction of some hardware
- Jamming wireless signals
- Disabling file management systems

INTERCEPTION

An unauthorized party gains access to an asset. Attack on confidentiality.

Examples:

- Wire tapping to capture data in a network.
- Illicitly copying data or programs
- Eavesdropping

MODIFICATION

When an unauthorized party gains access and tampers an asset. Attack is onIntegrity.

Examples:

- Changing data file
- Altering a program and the contents of a message

FABRICATION

An unauthorized party inserts a counterfeit object into the system.

Attack on Authenticity. Also called impersonation

Examples:

- Hackers gaining access to a personal email and sending message
- Insertion of records in data files
- Insertion of spurious messages in a network

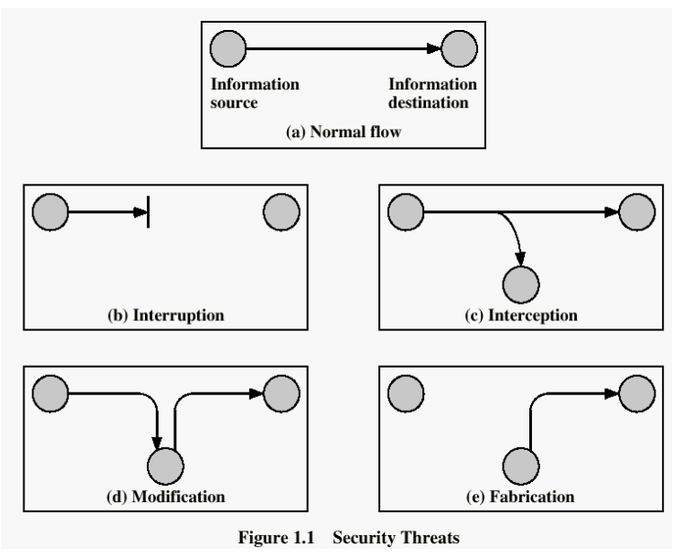


Figure 1.1 Security Threats

SECURITY SERVICES

It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.

Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems. It has been defined as "ensuring that information is accessible only to those authorized to haveaccess".

The other aspect of confidentiality is the protection of traffic flow from analysis.

Ex: A credit card number has to be secured during online transaction.

Authentication

This service assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties.

Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties. Two specific authentication services defines in X.800 are

Peer entity authentication: Verifies the identities of the peer entities involved in communication. Provides use at time of connection establishment and during data transmission. Provides confidence against a masquerade or a replay attack

Data origin authentication: Assumes the authenticity of source of data unit, but does not provide protection against duplication or modification of data units. Supports applications like electronic mail, where no prior interactions take place between communicating entities.

Integrity

Integrity means that data cannot be modified without authorization. Like confidentiality, it can be applied to a stream of messages, a single message or selected fields within a message. Two types of integrity services are available. They are

Connection-Oriented Integrity Service: This service deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. Destruction of data is also covered here. Hence, it attends to both message stream modification and denial of service.

Connectionless-Oriented Integrity Service: It deals with individual messages regardless of larger context, providing protection against message modification only.

An integrity service can be applied with or without recovery. Because it is relatedto active attacks, major concern will be detection rather than prevention. If a violation is

detected and the service reports it, either human intervention or automated recovery machines are required to recover.

Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. This capability is crucial to e-commerce. Without it an individual or entity can deny that he, she or it is responsible for a transaction, therefore not financially liable.

Access Control

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be

identified or authenticated, so thataccess rights can be tailored to the individuals.

Availability

It is defined to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity. The availability can significantly be affected by a variety of attacks, some amenable to automated counter measures i.e authentication and encryption and others need some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

SECURITY MECHANISMS

According to X.800, the security mechanisms are divided into those implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. X.800 also differentiates reversible & irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted, whereas irreversible encipherment include hash algorithms and message authentication codes used in digital signature and message authentication applications

Specific Security Mechanisms

Incorporated into the appropriate protocol layer in order to provide some of theOSI security services,

Encipherment: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys.

Digital Signature: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

Access Control: A variety of techniques used for enforcing access permissions to the system resources.

Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange: A mechanism intended to ensure the identity of an entity bymeans of information exchange.

Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control: Enables selection of particular physically secure routes for certain dataand allows routing changes once a breach of security is suspected.

Notarization: The use of a trusted third party to assure certain properties of a data exchange

Pervasive Security Mechanisms

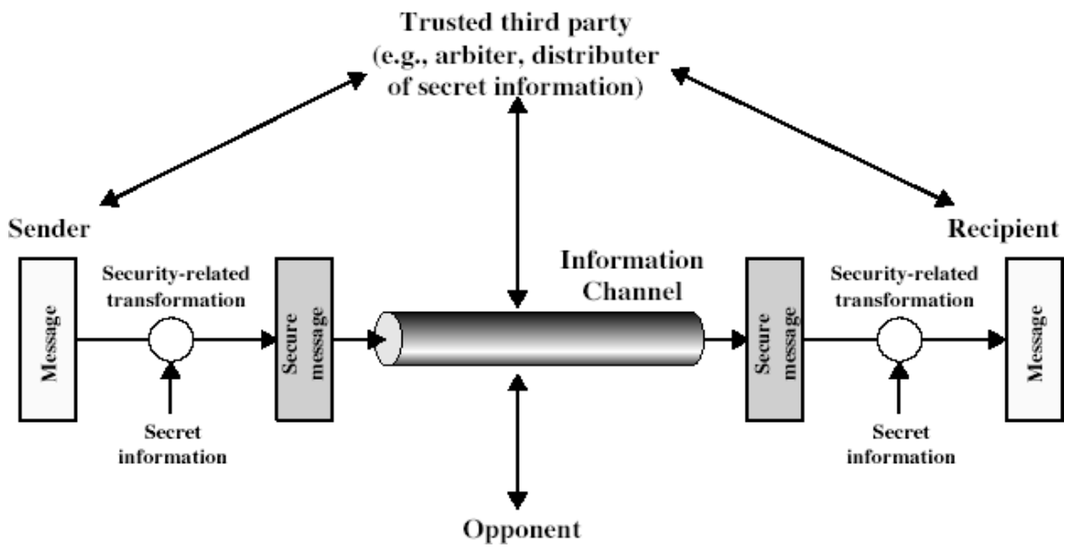
These are not specific to any particular OSI security service or protocol layer.

Trusted Functionality: That which is perceived to b correct with respect to some criteria**Security Level:** The marking bound to a resource (which may be a data unit) that namesor designates the security attributes of that resource.

Event Detection: It is the process of detecting all the events related to network security. **Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery: It deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

MODEL FOR NETWORK SECURITY



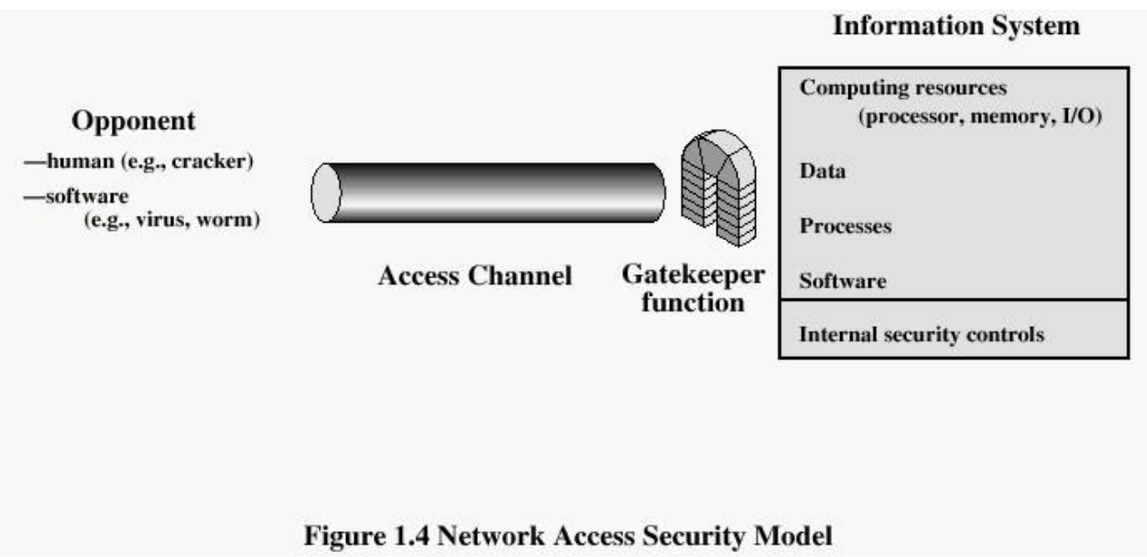


Figure 1.4 Network Access Security Model

Data is transmitted over network between two communicating parties, who

must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination by use of communication protocols by the two parties. Whenever an opponent presents a threat to confidentiality, authenticity of information, security aspects come into play. Two components are presentin almost all the security providing techniques.

A security-related transformation on the information to be sent making it unreadable by the opponent, and the addition of a code based on the contents of the message, used to verify the identity of sender.

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

A trusted third party may be needed to achieve secure transmission. It is responsible for distributing the secret information to the two parties, while keeping it away from any opponent. It also may be needed to settle disputes between the two partiesregarding authenticity of a message transmission. The general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose
2. Generate the secret information to be used with the algorithm
3. Develop methods for the distribution and sharing of the secret information
4. Specify a protocol to be used by the two principals that makes use of the securityalgorithm and the secret information to achieve a particular security service

Various other threats to information system like unwanted access still exist. The existence of hackers attempting to penetrate systems accessible over a network remains a concern. Another threat is placement of some logic in computer system affecting various applications and utility programs. This inserted code presents two kinds of threats.

Information access threats intercept or modify data on behalf of users who should not have access to that data

Service threats exploit service flaws in computers to inhibit use by legitimate users Viruses and worms are two examples of software attacks inserted into the system by means of a disk or also across the network. The security mechanisms needed to cope withunwanted access fall into two broad categories.

Some basic terminologies used

- **CIPHER TEXT** - the coded message
- **CIPHER** - algorithm for transforming plaintext to ciphertext

- **KEY** - info used in cipher known only to sender/receiver

ENCIPHER (ENCRYPT) - converting plaintext to ciphertext

- **DECIPHER (DECRYPT)** - recovering ciphertext from plaintext

- **CRYPTOGRAPHY** - study of encryption principles/methods
- **CRYPTANALYSIS (CODEBREAKING)** - the study of principles/ methods of decipheringciphertext *without* knowing key
- **CRYPTOLOGY** - the field of both cryptography and cryptanalysis

CRYPTOGRAPHY

Cryptographic systems are generally classified along 3 independent dimensions:

Type of operations used for transforming plain text to cipher text

All the encryption algorithms are abased on two general principles: **substitution**, in which each element in the plaintext is mapped into another element, and **transposition**, in which elements in the plaintext are rearranged.

The number of keys used

If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption**. If the sender and receiver use different keys then it is said to be **public key encryption**.

The way in which the plain text is processed

A **block cipher** processes the input and block of elements at a time, producing output block for each input block. A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

CRYPTANALYSIS

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst. **There are various types of cryptanalytic attacks** based on the amount of information known to the cryptanalyst.

Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: substitution andtransposition.

SUBSTITUTION TECHNIQUES

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

CAESAR CIPHER

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet. e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped
around,so that letter following „z‟
is „a‟.
For each plaintext letter p, substitute the cipher text
letter csuch that C = E(p) = (p+3) mod 26
A shift may be any amount, so that general Caesar algorithm is C = E (p) = (p+k) mod 26Where k takes on a value in the range 1 to 25.
The decryption algorithm is simply P = D(C) = (C-k) mod 26

MONOALPHABETIC CIPHERS

Here, Plaintext characters are substituted by a different alphabet stream of characters shifted to the right or left by n positions. When compared to the Caesar ciphers, these monoalphabetic ciphers are more secure as each letter of the ciphertext can be any permutation of the 26 alphabetic characters leading to 26! or greater than 4 x1026 possible keys. But it is still vulnerable to cryptanalysis, when a cryptanalyst is awareof the nature of the plaintext, he can find the regularities of

the language. To overcome these attacks, multiple substitutions for a single letter are used. For example, a letter can be substituted by different numerical cipher symbols such as 17, 54, 69….. etc. Even this method is not completely secure as each letter in the plain text affects on letter in the ciphertext.

Or, using a common key which substitutes every letter of the plain text.

The key *ABCDEFGHIIJ*

KLMNOPQRSTUVWXYZ

QWERTYUIIOPAS DFGHJ KLZXCV

BNM

Would encrypt the message

II think therefore

II am into

OZIIOFAZIITK

TYGKTOQD

But any attacker would simply break the cipher by using frequency analysis by observingthe number of times each letter occurs in the cipher text and then looking upon the English letter frequency table. So, substitution cipher is completely ruined by these attacks. Monoalphabetic ciphers are easy to break as they reflect the frequency of the original alphabet. A countermeasure is to provide substitutes, known as homophones fora single letter.

PLAYFAIR CIPHERS

It is the best known multiple –letter encryption cipher which treats digrams in the plaintext as single units and translates these units into ciphertext digrams. The Playfair Cipher is a digram substitution cipher offering a relatively weak method of encryption. It was used for tactical purposes by British forces in the Second Boer War and in World WarI and for the same purpose by the Australians and Germans during World War II. This was because Playfair is reasonably fast to use and requires no special equipment. A typical scenario for Playfair use would be to protect important but non-critical secrets during actual combat. By the time the enemy cryptanalysts could break the message, theinformation was useless to them. It is based around a 5x5 matrix, a copy of which is held by both communicating parties, into which 25 of the 26 letters of the alphabet (normally either j and i are represented by the same letter or x is ignored) are placed in a random fashion. For example, the plain text is *Shi Sherry loves Heath Ledger* and the agreed key is *sherry*. The matrix will be built according to the following rules.

in pairs,

- without punctuation,
- All Js are replaced with Is.

- *SH IS HE RR YL OV ES HE AT HL ED GE R*
  - Double letters which occur in a pair must be divided by an X or a Z.
  - E.g. LI TE RA LL Y LI TE RA LX LY

- *SH IS HE RX RY LO VE SH EA TH LE DG ER* The alphabet square is prepared using, a 5*5 matrix, no repetition letters, no Js and key is written first followed by the remaining alphabets with no i and j.

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

For the generation of cipher text, there are three rules to be followed by each pair ofletters.

- letters appear on the same row: replace them with the letters to their immediate right respectively
- letters appear on the same column: replace them with the letters immediately below respectively
- not on the same row or column: replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.Based on the above three rules, the cipher text obtained for the given plain text is

HE GH ER DR YS IQ WH HE SC OY KR AL RY

Another example which is simpler than the above one can be given as:

Here, key word is *playfair*. Plaintext is *Hellothere hellothere* becomes --------*he lx lo th er ex* .

Applying the rules again, for each pair, If they are in the same row, replace each

with theletter to its right (mod 5)

he KG

If they are in the same column, replace each with the letter below it (mod 5)

lo RV

Otherwise, replace each with letter we'd get if we swapped their column indices

lx YV

So the cipher text for the given plain text is **KG YV RV QM GI KU**

$$\begin{bmatrix} p & l & a & y & f \\ i & r & b & c & d \\ e & g & h & k & m \\ n & o & q & s & t \\ u & v & w & x & z \end{bmatrix}$$

To decrypt the message, just reverse the process. Shift up and left instead of down and right. Drop extra x's and locate any missing I's that should be j's. The message will be back into the original readable form. no longer used by military forces because of the advent of digital encryption devices. Playfair is now regarded as insecure for any purpose because modern hand-held computers could easily break the cipher within seconds.

HILL CIPHER

It is also a multi letter encryption cipher. It involves substitution of '*m*' ciphertextletters for '*m'* successive plaintext letters. For substitution purposes using '*m'* linear equations, each of the characters are assigned a numerical values i.e. a=0, b=1, c=2, d=3,…….z=25. For example if m=3, the system can be defined as: **c1 = (k11p1 + k12p2 + k13p3) mod 26 c2 = (k21p1 + k22p2 + k23p3) mod 26 c3 = (k31p1 + k32p2 + k33p3) mod 26** If we represent in matrix form, the above

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \mod 26$$

statements as matrices and column vectors:

Thus, C = KP *mod26,* where C= Column vectors of length 3 P = Column vectors of length 3 K

= 3x3 encryption key matrix. For decryption process, inverse of matrix **K** i.e. **K-1** is required which is defined by the equation KK-1 = K-1K = I, where I is the identity matrix that contains only 0's and 1's as its elements. Plaintext is recovered by applying K-1 to the cipher text. It is expressed as C = EK(P) = KP *mod26* P = DK(C) = K-1C *mod26.* = K-1KP = IP = P

Example: The plain text is I can't do it and the size of m is 3 and key K is chosen as following

```
I can't do it
8 2 0 13 19 3 14 8 19
```

$$\begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix}$$

The encryption process is carried out as follows

$$\begin{pmatrix} 4 \\ 14 \\ 12 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 8 \\ 2 \\ 0 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 19 \\ 12 \\ 14 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 13 \\ 19 \\ 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 18 \\ 21 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 & 18 & 10 \\ 16 & 21 & 1 \\ 5 & 12 & 23 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \\ 19 \end{pmatrix} \pmod{26}$$

So, the encrypted text will be given as → **EOM TMY SVJ**

The main advantages of hill cipher are given below:perfectly hides single-letter

- It frequencies.
- Use of **3x3** Hill ciphers can perfectly hide both the single letter and two-letter frequency information.

- Strong enough against the attacks made only on the cipher text.

But, it still can be easily broken if the attack is through a known plaintext.

POLYALPHABETIC CIPHERS

In order to make substitution ciphers more secure, more than one alphabet can be used. Such ciphers are called **polyalphabetic**, which means that the same letter of a message can be represented by different letters when encoded. Such a one-to-many correspondence makes the use of frequency analysis much more difficult in order to crack the code. We describe one such cipher named for *Blaise de Vigenere* a 16-th century Frenchman. The **Vigenere cipher** is a polyalphabetic cipher based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters. The procedure is based on the tableau shown below and the use of a keyword. The letters of the keyword determine the shifted alphabets used in the encoding process.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

For the message COMPUTING GIVES INSIGHT and keyword LUCKY we proceed by repeating the keyword as many times as needed above the message, as

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T

follows.

Encryption is simple: Given a key letter x and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled *x* and the column labeled *y*; so for L, the ciphertext letter would be N. So, the ciphertext for the given plaintext would be given as:

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L				
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T				<==MESSAGE
N	I	O	Z	S	E	C	P	Q	E	T	P	G	C	G	Y	M	K	Q	F	E				<==Encoded Message

Decryption is equally simple: The key letter again identifies the row and position of ciphertext letter in that row decides the column and the plaintext letter is at the top of that column. The strength of this cipher is that there are multiple ciphetext letters for each plaintext letter, one for each unique letter of the keyword and thereby making the letter frequency information is obscured. Still, breaking this cipher has been made possible because this reveals some mathematical principles that apply in cryptanalysis. To overcome the drawback of the periodic nature of the keyword, a new technique is proposed which is referred as an autokey system, in which a key word is concatenated with the plaintext itself to provide a running key. For ex In the above example, the key would be *luckycomputinggivesin* Still, this scheme is vulnerable to cryptanalysis as both the key and plaintext share the same frequency distribution of letters allowing a statistical technique to be applied. Thus, the ultimate defense against such a cryptanalysis is to choose a keyword that is as long as plaintext and has no statistical relationship to it. A new system which works on binary data rather than letters is given as

Ci = pi ki where, pi = ith binary digit of plaintext ki = ith binary digit of key Ci= ith binarydigit of ciphertext

= exclusive-or operation. Because of the properties of XOR, decryption is done byperforming the same bitwise operation.

pi = Ci ki A very long but, repeation key word is used making cryptanalysis difficult.

TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence is simplest of such cipher, in which the plaintext is written down as a sequenceof diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2,

We write the message as follows: m e a t e c o l o s e t t h s

h o h u eThe encrypted message is

MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute

the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the
school houseKey = 4 3 1 2 5 6 7
PT = m e e t a t t h e s c h o o
l h o u s eCT =
ESOTCUEEHMHLAHSTOE
TO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

STEGANOGRAPHY

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformationsof the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. e.g., (i) the sequence of first letters of each word of the overallmessage spells out the real (hidden) message. (ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been usedhistorically, some of them are

- **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is heldto an angle to bright light.
- **Invisible ink** – a number of substances can be used for writing but leave no visibletrace until heat or some chemical is applied to the paper.
- **Pin punctures** – small pin punctures on selected letters are ordinarily not visibleunless the paper is held in front of the light.
- **Typewritten correction ribbon** – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of Steganography

- Requires a lot of overhead to hide a relatively few bits of information.

Once the system is discovered, it becomes virtually worthless.