UNIT-I

INTRODUCTION.

Security trends - legal, ethical and Professional Aspects of security, Need for security at Multiple levels, security policies - Model of network security - Security attacks, services and mechanisms -OSI Security architecture - classical encryption techniques; substitution techniques, transposition techniques., Stegnagraphy - Foundations of modern cryptography; perfect security - information theory - product cryptosystem - cryptanalysis.

Introduction :-

Security - Security is protecting the information from information risk.

Why security is important?

As security is ubiquotous. There is need four security due to the advent of electronic transactions and e-commerce process.

Solution:-

Here CNS (cryptography) technique for the information security problems.

Cryptography - It is the process of storing and transferring data in a particular form. Hence only the intended persons can able to read and write.

This is the study and technique of building the ciphers to maintain and ensure confidentiality and integrity.

-> Information -ti Communication technique derived from mathematical model / calculation -> algorithm. lies

Information is considered as an Asset. Hence, the Asset, information needs to be secured from any kind of attacks.

Three security Goals:- (CIA triad).

Confidentiality - protect the information from unauthorized third party access.

Integrity - protect the information from unauthorize change.

Availability - The information must be available to the authorized entity, when it is needed.

-> confidentiality is acheived by restricting the acces

-> Integrity is acheived by restricting the data manipulation

-> Availabity can be acheived by providing acess to authorized person all time.

Examples:-

Confidentiality - Concealment of information in milit

Integrity - In Bank, account transaction has to be updated by authorized entities only.

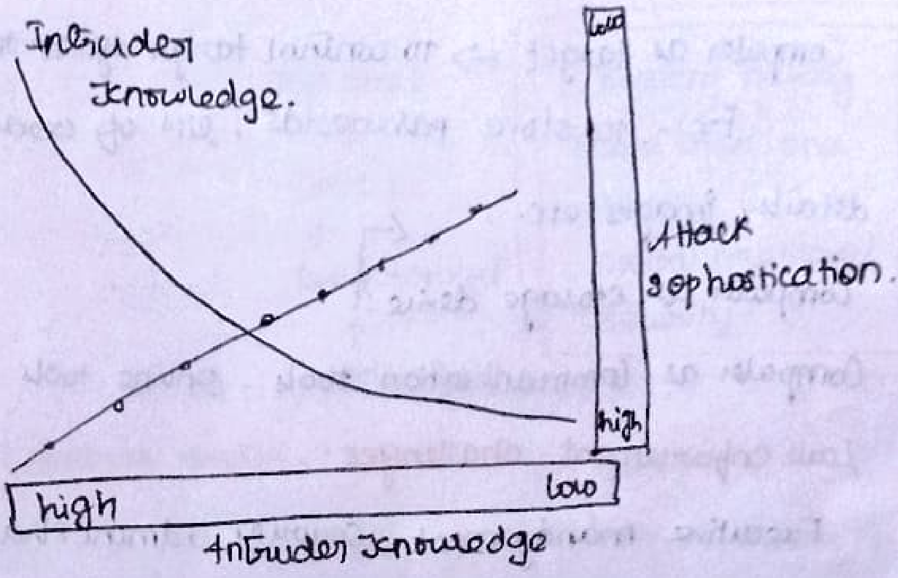
Availabity - Unavailabity becomes harmful to the org

Computer Security - Collection of tools designed to data collection and thwart hackers.

Network Security - measure to protect data, during transmission.

Internet security - measures to protect data during transmission. ↓
This subject focus.

Security trends.



hence intruder knowledge at starting years and decreased in recent year due to stronger cryptographi-cal Techniques.

Legal, ethical and Professional aspects of security.

Cyber crime + computer crime

↓ involves Computer Networks for criminal activities.

↓ involves computers for criminal activity, may or maynot Networks.

Here cryptography is used for secure transactions and to safe gaurd the personal Identifiable information.

-> To prevent tampering of document

-> To create trust between the servers.

Cryptography -> invented by claude shannon. works at Bell lab.

↓ father of mathematical cryptography.

scytale - earlier device of cryptography

Engima Enigma machine - Germany.

Modern cryptography uses Algorithms.

Computer crime :- Types .

Computer as target -> To control target system to acquire info

Ex:- To store passwoords , list of credit card details, images etc. , <-

Computer as storage device :-

Computer as communication tools - Online tools .

Law enforcement challenges :-

Executive management , security, administrators have to check on law enforcement , tools, human factors etc...

* relies on Technical and people skills .

-> org. should have proper criminal investigation process.

Intellectual property :-

↓

Intangiable assets , human ideas .

includes

↓

attacks

-> Copyright -> unauthorized use

-> trade mark -> unauthorized colorable of trademark

-> patents -> unauthorized selling of patents

↓

Infringement (attacks) on IP attack .

DMCA -> Digital millennium copyright.

This can be obtained when we store our own rights or content in digitialized manner.

DRM -> Digital rights management .

ensuring the DMCA and checks bug meet work flow .

Privacy :- securing private information

↓

-> European union data protection directive

-> United States privacy initiatives .

-> organizational response

Need foor security at multilevel :-

why multilevels?

Top seret
↑
Secret
↑
Confidential
↑
unclassified.

'X' system having more than one security level is called multilevel security.

-> Bell la padula model

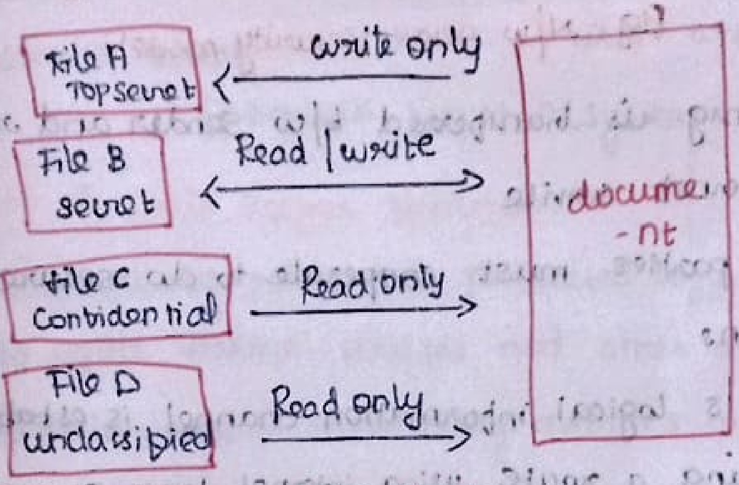


Fig: Ex MLS system

Security level objects and subjects :-

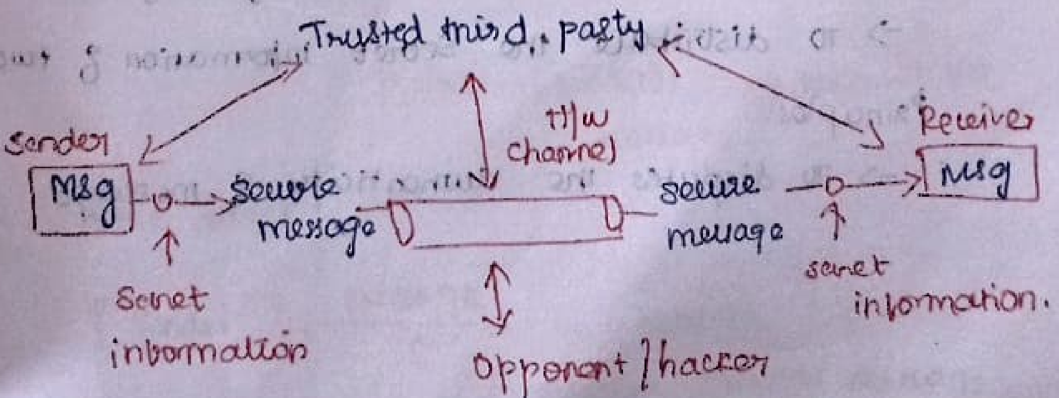
Two entities :- -> sensitivity -> secret and Top secret
-> categories -> Non hierarchical attributes.

Security levels on objects -> classifications.

Security levels on subjects -> clearance.

Model for Network Security model :-

This model has sender and reeiver.



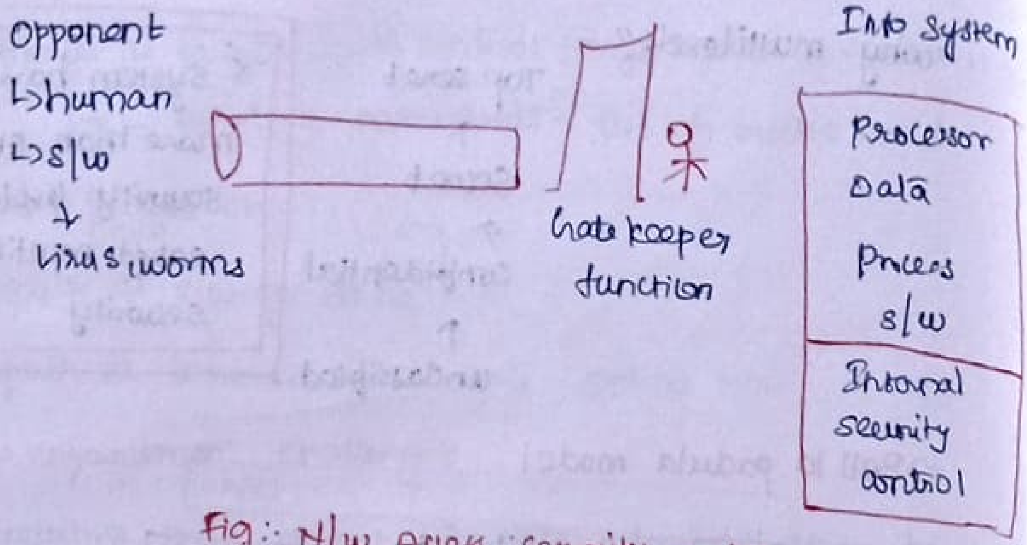


Fig:: N/w Access security model.

→here msg is transferred b/w sender and receiver via Internet service.

→ Two parties must cooperate to do secure transactions.

→There is logical information channel is established by defining a route using internet from source to destination with the help of communication protocol such as TCP/IP.

Here the security has two main component

→security related transformation

↳ encrypting the messages.

↳ Some seret information → encrypting keys

Trusted third party work are as follows

→ To distribute the secret information & two Principles.

→ To disputes the authenticity & message.

+ Steps in designing a security service :

-> Design an algorithm with security related transformation

-> Generate the secret information with encryption

-> Generate methods for sharing the information

-> specify protocol with two principles.

Two kinds of threats :-

↳ Information access threats -> modify data onbehalf on users who is unauthorized

↳ service threat

↳ exploits flaws in system.

Use of Gate keeper function:-

↳ To include password protected login procedures to reject worms, viruses and other attacks.

↳ To implement monitoring activities to analyze the stored information from unwanted intruders.

SECURITY ATTACKS, SERVICES & MECHANISMS :-

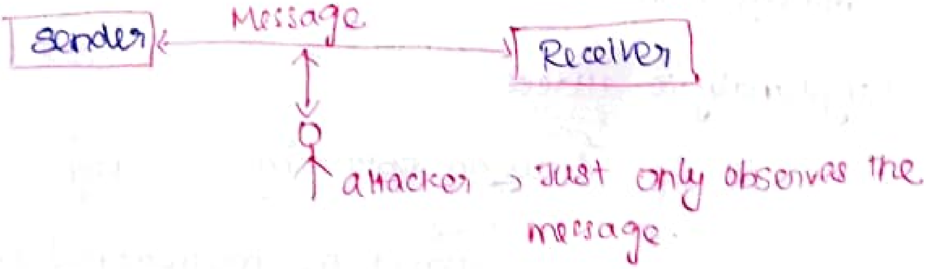
-> Two types of attacks :-

↳ passive & Active.

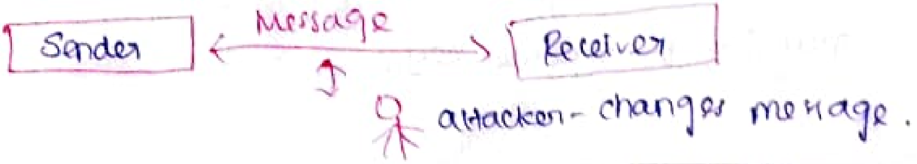
-> security services

-> security mechanisms.

Passive attack:-



Active attack :-



PASSIVE attack:

↳ It is like Eavesdropping ([illegible]).

↓ monitoring of transmissions.

↳ It is difficult to identify. as there is no any modification

↳ But we can prevent Somehow with encryption

Types:

↳ Release of message contents

↳ Traffic analysis.

↓ Eg: telephone conversation, email to get confidential information

↓ masking the information with encryption.

ACTIVE ATTACK:

↓ modification of message in the N/w and send to the receiver with other modified message.

4 catagories:

-> Masquerade.

↳ when we get information from unauthorized entity.

-> Replay: Repeatation of masquerade.

-> modification:

Cryptanalytic attacks:-

↓ focus on obtaining secret keys.

↓ inspect the mathematical properties

here attacker gues the keys, try for the keys otherwise they try for another key.

Non cryplanalytic attacks:

→ They do not look for mathematical issue. -> focus on CIA.

Security attacks

Snooping	modification	DOS
Traffic analysis	masquerading	Threat of availability
(Threat to confidentiality)	Replaying	
	Repudiation	
	Threat of integrity	

Snooping - unauthorized access. | interception of Data.

→ encryption can be done.

Traffic analysis - monitor online traffic.

-> finds email address, guess transactions.

Modification - After attacking, user modifies the information.

masquerading (spoofing) - impersonates somebody

Ex:- attacker steal Bank PIN to access the card.

Replaying - copy the message and use it again.

Repudiation - This is done by either sender or by receiver. Ex:- deny of payment.

DOS - common attack.

→ Intercepts the server system.

P.- Snooping, Traffic analysis -> conf

A - modification of messages, DOS - Int, availability.

P - passive A - active.

Servies and Mechanisms:-

5 servies by ITU-T (X.800)

↓

Data Confidentiality

Data integrity

Authentication

Non Repudiation

Acess control.

Data integrity :- connection oriented integrity services.

↳ Anti change

↳ Anti Replay.

Authentication:

↳ Peer entity

↳ Data Origin

Non Repudiation

↳ Proof of origin

↳ Proof of delivery.

Confidentiality - Protecting data from passive attack

↓ TCP connection establishment.

Acess control

↳ ACL list / matrix.

Data confidentiality.

↳ Connection confidentiality

↳ Connectionless Confidentiality

↳ selective field → particular

↳ Traffic flow → providing Security acc. to traffic flow

Protection to all users

→ protection to all users using single data blocks.

SECURITY MECHANISMS:-

OSI service for security :- Specific security mechanisms ar

→ Encipherment - encryption

→ Digital signature → S'men - sdata → hashalgo → hash o/p → Encryption ↓ digitally Sind doc

→ Acess control

→ Data integrity

-> Authentication exchange -> conforming identity q user

-> Traffic padding -> hiding traffic pattern -> inserting a dummy traffic in n/w.

-> Routing control -> allocates secure route for data exchange

-> Notarization
↳ uses trusted 3rd party in communication.

Pervasive security mechanisms are as follows

-> Trusted functionality -> Implementation of security policies.

-> security label -> set q security related information
↓
track the label & objects.

-> Event detection -> security related events.

-> Security Audit Trial
↳ systematic evaluation q security's organization Information policy

Internal audit
↓
To check whether org relies on own side th policies

External audit
↓
outside group conducts audit th check for govt. rules and regulations.

-> Security Recovery.
↓
event handling, taking security actions.

OSI security architecture :-

Security attacks

Security services

Security mechanisms.

↓ helps managers to organize the tasks to provide security.

Threat - possible danger that exploits vulnerability.

Attack - violate the security policy of a system.

CLASSICAL ENCRYPTION TECHNIQUES

Cryptography :-

Process of converting plain txt to cipher text.

-> enciphering. Reverse process is called - deciphering.

Study of encryption techniques - Cryptography.

Encryption -> has secret key + encryption process

Symmetric
↓
both encryption + decryption done using same keys

Asymmetric
↓
Encryption and decryption is done by two different keys.

Attack on encryption
↓
-> breaking of code.

-> Cryptanalysis -> Reveals properties of encryp. algo.

-> Brute force attack -> trying all possible keys.

Transposition cipher:-

-> Substitutes text into cipher text.

Rotor machines :-

H/w device which performs substitution ciphers.

Stegnagraphy:

hiding secret message into image.

Conventional Encryption.

plain text -> Encryption algorithm —Transmitted / cipher text-> Decryption algorithm -> plain text

Encryption algorithm
↓
using secret Shared key

Decryption algorithm
↓
using secret shared key.

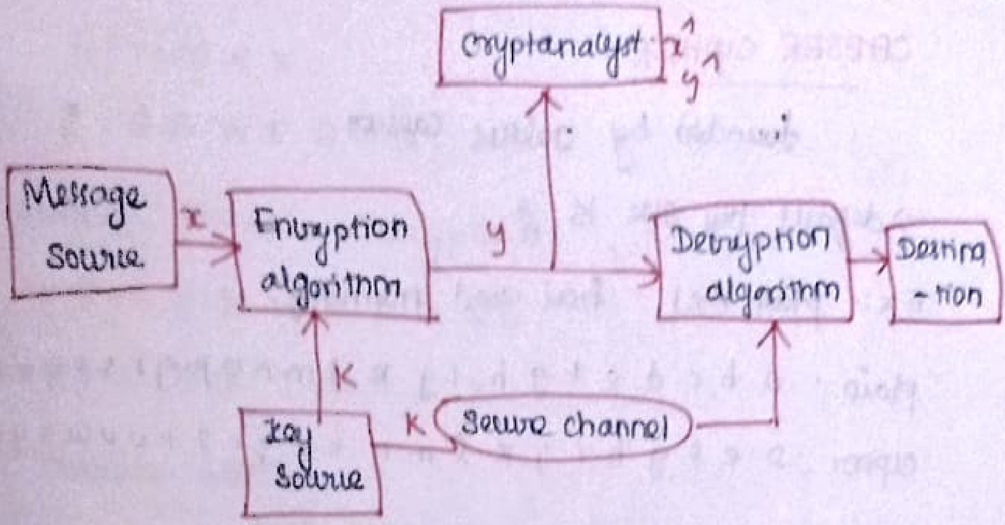


Fig:- Conventional cryptosystem.

3 dimensions of cryptography:-

-> transforming plain text to cipher text

-> Numbers of keys used

-> way in which plaintext is processed.

↳

Block cipher - one block at a time

Stream cipher - takes i/p element continously

Types of attacks:-

cryptanalyst

-> cipher text only -> En. algo

-> Known plaintext -> one or more plain text, ciphertext pair

-> chosen plaintext -> plaintext by cryptanalyst, secret key

-> chosen ciphertext

↳ ciphertext by cryptanalyst.

-> chosen text

↳ Both encrypted and decrypted text

SUBSTITUTION TECHNIQUES:-

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or by symbols.

↓

Encryption is unconditionally secure when cipher text is strong enough which cannot be predicted.

-> Computation secure -> when cost of breaking exceeds value + lifetime of cipher text.

CAESER CIPHER:-

founded by Julius caesar.

→ default key size is 3.

Ex:- plain text hai good morning.

plain : 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

cipher : 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 to z = 0 to 25 number equivalent.

Algorithm:-

$E = E(P+K) \bmod 26$

$C = E(3, P) = (P+3) \bmod 26$. $P = C(C-K) \bmod 26$

but it can be any key between 1 to 25.

25 keys are possible for brute force attack.

MONO ALPHABETIC CIPHER

Since there is no security for caeser cipher.

Playfair cipher:-

Multiple letter encryption.

mono alphabetic example:-

↓

It is a substitution cipher in which for a given key the cipher aphabet for each plain alphabet is fixed

Ex:. D is replaced by A means - Its for all occurence in the plain text.

If key = 3, then 3! = 6 combinations are possible

Ex: PT = NETWORK

key = hello how are you.

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

h e l o w a r y u a b c d f g i j k m n p q s t v x z

NETWORK.

g · SBWEDGQ

Reverse process - Decryption.

CT - S B W E D G Q

PT - N E T W O R K.

Possible attacks

Once A is replaced by E, means every occurence is replaced by E.

PLAYFAIR CIPHER:

This is the best known multiple letter encryption and this treats plaintext as single units and translates the units into ciphertext diagrams.

->Based on 5x5 matrices using keywords.

Rules:- Ex:- Occurence

-> No repeating letters eg: ocuren

->Create a table

↳either left to right or top to bottom

↳ I/J should be in same box

PT- fall trees

keyword:- occurence

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

Prepare message:

→ split The pt into plain text

→ If there is duplication of letters by separating by 'x'.

→ If there is odd number of letters. add 'x' at end.

Tall trees → Ta lx lt re es.

This can be done. Same pa
means have to insert 'x'.

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

Ta = DF Rule 3

Lx - IZ

LT - TZ Rule 1

RE - EO Rule wrap round

ES - RT

CT - PFIZTZEORT.

Ad:

→ It difficult to particular diagram

→ Freq analysis is very difficult.

Disad:

→ Easy to break

→ Sufficient Ho q ciphertext is small.

HILL CIPHER:-

Developed by mathematician lester Hill 1929.

Basic mode calculation:-

27 mod 26 $\quad 26\overline{)27}(1$

$\quad\quad\quad\quad\ \ 26$

$\quad\quad\quad\quad\ \ \underline{\ \ 1\ \ }$ have to take remainder. 1

Inverse of mod operation:-

1) 9^{-1} mod 26

$9 \times ?$ mod 26 = 1 -> have to do get 1 as remainder.

9×1 mod 26 = 9 mod 26 = 9

9×2 mod 26 = 18 mod 26 = 18

9×3 mod 26 = 27 mod 26 = $\underline{1}$

$\boxed{\text{hence } 9^{-1} \text{ mod } 26 = 3.}$

Similarly 444^{-1} mod 26 = 11

441×25 mod 26 = 1

$\boxed{\text{hence } 441^{-1} \text{ mod } 26 = 25}$

Hill cipher:-

Plain text = HELP

key $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

cipher text $C = K p$ mod 26

Split the plain text into two-two letters. as 'HE' 'LP'

$P = HE = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$ -> as 7 and 4 are numbout to H and E.

hence $C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix}$ mod 26

$= \begin{bmatrix} 21 & 12 \\ 14 & 20 \end{bmatrix}$ mod 26 have to odd

$$\begin{bmatrix} 33 \\ 34 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 33 \\ 34 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 7 \\ 8 \end{bmatrix} \Rightarrow \begin{bmatrix} H \\ I \end{bmatrix}$$

Next $p = Lp = \begin{bmatrix} 11 \\ 16 \end{bmatrix}$

$$C = Kp \bmod 26$$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 33 & 45 \\ 22 & 75 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 78 \\ 97 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

Hence $\boxed{\text{cipher text: HELP = HIAT}}$

Decryption:-

Plain text $P^{-1} \to K^{-1}C \bmod 26$

$$K^{-1} = \frac{1}{|K|} \text{adj } K$$

$$|K| = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = 15 - 6 = 9 \qquad \text{adj } K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$ change sign

$$K^{-1} = \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 5(9)^{-1} & (-3)9^{-1} \\ (-2)9^{-1} & (3)9^{-1} \end{bmatrix}$$ we know $9^{-1} \bmod 26 = 3$.

$$\Rightarrow \begin{bmatrix} 5(3) & (-3)(3) \\ (-2)(3) & (3)(3) \end{bmatrix}$$

$$= \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \text{mod } 26$$

$-9 \text{ mod } 26$

$\Rightarrow -9+26 = \boxed{17}.$

$$\boxed{\begin{aligned} &= 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \text{mod } 26 \\ &= 3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix} \text{mod } 26 \\ &= \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix} \text{mod } 26 \end{aligned}}$$

$-3+26 = 23$

$-2+26 = 24$

additional step

$$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Hence $p = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \text{mod } 26 \Rightarrow \begin{bmatrix} 105 & 136 \\ 140 & 72 \end{bmatrix}$

$$= \begin{bmatrix} 241 \\ 212 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \Rightarrow \boxed{\begin{bmatrix} H \\ E \end{bmatrix}}$$

Similarly for AT

$$P = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 323 \\ 171 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ P \end{bmatrix}$$

hence HELP.

H/w:

Playfair - keyword monarchy

P.T- Balloon

Caesar cipher - PT- meet me after the toga party

key = 3.

Hill cipher:- "pay more money" - PT

key $\begin{bmatrix} 17 & 7 & 5 \\ 21 & 19 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

Ex:- 2 PT - Hillcipher

key = $\begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix}$. HCRZSSXNSP.

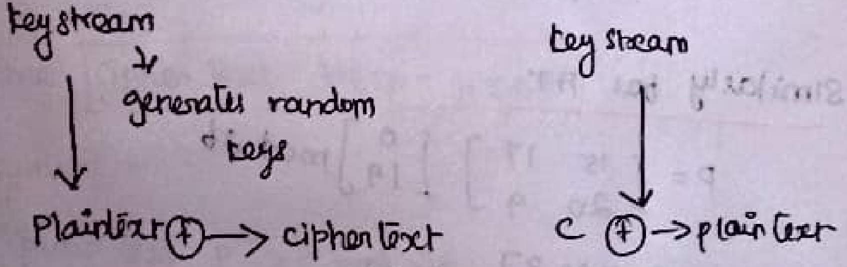
VERNAM CIPHER

It is a poly aplphabetic cipher.

-> main aim of cryptanalysis is to choose a keyword.

-> This was introduced by AT & T engineer Gilbert Vernam in 1918.

-> This works on binary data rather than letters.



$\boxed{C_i = P_i \text{ xor } K_i}$

P_i - binary digit of plaintext

K_i - binary digit of key.

C_i - binary digit of cipher text.

Ex:- Vernam cipher also caled OTP (one time pad).

plain text :- Hello

key - any random key where PT & key length should same.

Key :. NCBTA

Encryption :.

P : H E L L O

7 4 11 11 14

K : N C B T A (+)

13 2 1 19 0

20 6 12 30 14

-26

4 → There are only 26 alphabets. Hence we have to subtract 26 from 30.

cipher text : U G M E O

Decryption :- C-K

C : U G M E O

20 6 12 4 0

20 6 12 30 0 → Add 26 to avoid negative result

K : N C B T A

13 2 1 19 0

7 4 11 11 14

P : H E L L O → hence plain text.

Ans :.

PT :. WORLD

key : Tejas.

find CT.

Adv :.

→ The key is used for encryption and decryption and then that key can be discarded.

→ one time pad - is unbreakable.

→ There is no statistical relationship b/w PT, hence there is no simple way for breaking the code.

Polyalphabetic cipher :

Another way for improving simple monoalphabetic technique called polyalphabetic cipher.

→ vignere

↳ auto key system where key word is concatenated with plaintext to provide running key.

Ex :- attack at dawn

key! lemon.

A B C D E F G H I J K L M N O P Q P S T

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

a t t a c k a t d a w n
l e m o n l e m o n l e

ciphertext:- LXFOPVEFRNHR.
l e m o n l e m o n l e

a T o c
h a v

attack at dawn.

Method II:

using key table.

key: deceptivedeceptivedeceptive ->has to repeat the keyword.

PT: we are discovered y save yourself.

CT:: ZICVTWQNGRZGVTWAVZHCQYGLMGJ.

key:

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22

have to add key and PT

key	8	21	4	3	4	2	4	15	19	8	21	4
PT	18	0	21	4	24	14	20	17	18	4	11	5
CT	22	01	25	07	2	18	24	26	16	12	6	9

CRYPTANALYSIS:

This vignere cipher is unbreakable, due to the use of 26 different cipher alphabets.

Disadvantage:

-> If the key length is smaller then plaintext length, then key will be repeated.. due to repeating nature of key.

-> This is computationaly secured.

TRANSPOSITION TECHNIQUES

-> So far we have learned substitution Techniques.

-> Ex for transposition technique is Rail fence cipher

Railfence cipher :-

↓ Simplest technique in which plaintext is written down as a sequence of idiagnosis and then read off as a sequential rows.

It is fencing in railway track as

Ex:- PT : H E L L O W O R L D

depth K = 2

H L O O L
E L W R D

Ciphertext :- HLOOLELWRD.

Decryption :-

There are totally 10 letters in ciphertext. Make it as columns.

H		L		O		O		L	
	E		L		W		R		D

hence hello world. - by using fencing technique

If depth K = 3 means,

d1	H				O				L	
d2		E		L		W		R		D
d3			L			A	O			

-> decryption - helloword.

CT = HOLELWRDLO

Anomen memod:

1. PT: MEET ME TOMORROW

CT: Reverse of each word

Hence CT = TEEM EM WORROMOT.

2. Here key is provided

key:	4	3	1	2	5	6	7
PT:	t	o	m	e	e	t	a
	t	h	a	l	l	I	a
	m	t	h	e	r	e	a
	t	t	i	m	e	o	K

CT- have to use ranking from key

Here Rank is 1. so take and write the letters in 1 column.

mahielemohttttmtelretIeDaaaK.

This method is very difficult to cryptanalysis

STEGANOGRAPHY:

In general. plain text can be hidden in two ways

↳ Steganography - conceal the existence of message

↳ cryptography - render the message unintelligble to the outsiders by various transformation process.

Steganography - It is a time consuming process.

Ex: sequence of 1st letters of each words of overall message spells out the hidden message.

4 Techniques: - → character marking

→ Invisible Ink

→ pin punctures

→ Type writer correction ribbons.

Character marking :-

Selected letters of printed or typewritten text are overwritten in pencil and it is visible only in bright light.

Invisible Ink:-

visible trace is seen until some chemical is applied to the paper.

Ex:- lemon. candle light

UV pen

Pin punctures :-

Small pin punctures on selected letters are ordinarily not visible and visible only in front of light.

Typewriter correction ribbon:-

used in type writter ribbon print.

Ex:. Kodak photo CD

Drawback:-

->requires overhead work to make small message

->once system is discovered, it become worthless.

Foundation of Modern Cryptography :-

Basic difference between classical cryptography and modern cryptography is that classical cryptography manipulates on traditional characters, while modern cryptography operates on binary character.

-> CC relies on security via obscurity while modern cryptography relies on mathematical coding.

-> CC needs entire cryptosystems while MC depends on parties interested in secure the communication.

-> modern cryptography relies on cryptographic keys with cryptographic algorithms.

-> This was founded by IBM crypto group in 1970's.

Modern cryptography :-

- Perfect security
  - one time pad
- Information theory
  - Properties of entropy
- Product Crypto systems
- cryptanalysis

Perfect security :-

one has to put massive effort to put into cryptanalysis in order to measure the strength and weakness of the Cryptosystem.

3 issues :-

-> same encryption / decryption process is used, so identification of security pattern is easy.

-> Easily we can get the ~~cryptotext~~ ciphertext, keys of plaintext.

-> There is need for more and more stronger encryption Process.

Table 1 :- Encrypt / decrypt rules

	m1	m2	m3	m4
k1.	C1	C2	C3	C4
k2	C5	C4	C2	C1
k3	C4	C1	C2	C3

To find :- Prob of cryptotext =>

C.T	C1	C2	C3	C4	C5
Prob	0.24	0.28	0.26	0.19	0.03

$$C1 = (m1 * k2) + (m4 * k2) + (m2 * k3)$$
$$= (0.1 \times 0.2) + (0.4 \times 0.3) + (0.2 * 0.5)$$

Table 2 :- Prob of messages.

Key	m1	m2	m3	m4
Prob	0.1	0.2	0.3	0.4

Table 3 :- Prob of keys.

Key	k1	k2	k3
Prob	0.2	0.3	0.5

system is perfect security.

$$p(m|c) = p(m)$$

$$p(m|c) = \frac{p(c|m)(P(m))}{p(c)}$$ Bayes Theorem.

Shanon Theorem:

-> every $m \in M$, $c \in M$, unique $k \in k$

-> The system is perfectly secured if only if every one is used with equal probability.

$$P(k_i(c_i)) = P(k_j(c_j)) = m_1$$

All keys must be used with same Probability.

OTP:- one time pad.

Information theory:- consider experiment with some possible outcome -> outcomes are caled event.

x-outcome

x_i-value of outcome.

Before conduction of experiment, outcome is unknown.

Entropy: measure of information content.

Ex:- Take any 8 value -> 8 bit 000, 001, 010, 011, 100, 101, 110

$P = 1/8$. 110 - if we have partial infor $b_2 = 1$

50% reduction in uncertainty

If $b_0 = 0$ uncertainty becomes 25%.

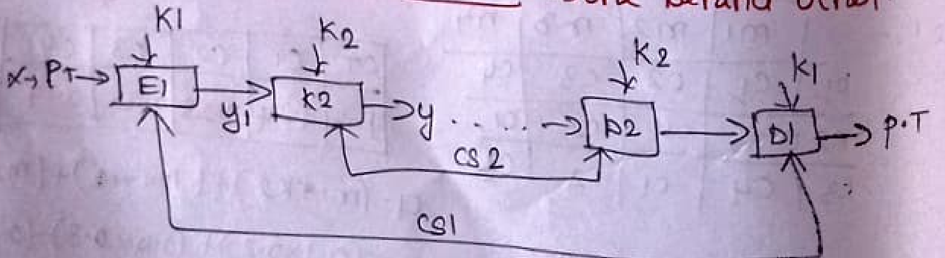
-> we can get information using 75% reduction

b_2	b_1	b_0	
0	0	1	
0	0	1	
0	1	0	
0	1	1	
1	0	0	Or
1	0	1	
1	1	0	Or
1	1	1	

Product cryptosystem:-

-> All cryptosystem are subject to attacks.

-> To solve, we use product cryptosystem which uses two crypto system in tandem -> one behind other.



Cryptanalysis:

Breaking the code is caled cryptanalysis.

-> Brute force attack

-> know plain text attack

-> chosen plain text attack

-> known cipher text

-> cryptotext only text attack.