Topics Covered

1. What is Cryptography? (Introduction)
2. Types of Cryptography – Symmetric
   – Asymmetric
   – Hashing
3. CIA Triad | Security Goals and Security Services.
4. Security Attacks in Cryptography.
5. Security Mechanisms in Cryptography.
6. Substitution and Transposition Techniques
   - monoalphabetic cipher
   - polyalphabetic cipher
7. Rail fence & Row Transposition techniques
8. keyless and keyed " "
9. Caesar Cipher
10. Playfair cipher.
11. Vigenere Cipher. method-1

position techniques
- monoalphabetic cipher
- Polyalphabetic cipher

7. Rail fence & Row Transposition techniques
8. keyless and keyed " "
9. Caesar Cipher
10. Playfair cipher.
11. Vigenere Cipher. method-1
12. Vigenere Cipher method-2
13. Hill Cipher (encryption + Decryption)
14. (3x3) example
15. Stream & Block cipher and their difence b/w
16. Shannons Theory of Confusion & Diffusion.
17. fiestel structure | cipher
18. DES in detail
19. key genera[illegible] in DES
20. Vernam Cipher.

Security Goals

CIA triad in crypto

1) CONFIDENTIALITY - It is the most common aspect of info. security.

* It allows authorized users to access sensitive & protected data.
The data sent over the network shouldnot be accessed by unauthorized users/individuals.

Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data so that even if attacker gains access, he/she will not be able to decrypt it.

2) INTEGRITY - [eg] In a bank, when we deposit/withdraw money the balance needs to be maintained.

Integrity means that changes need to be done only

Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data so that even if attacker gains access, he/she will not be able to decrypt it.

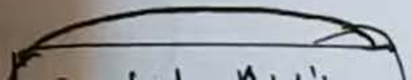
2) INTEGRITY – [eg] In a bank, when we deposit/withdraw money, the balance needs to be maintained.

Integrity means that changes need to be done only by the authorized entities and through authorized mechanisms, and nobody else should modify our data.

3) Availability → data must be available to the authorized user.

Info is useless if we cannot access it.

eg) what would happen if we cannot access our bank accounts for transactions.



withdraw money, the balance needs to be maintained.

Integrity means that changes need to be done only by the authorized entities and through authorized mechanisms and nobody else should modify our data.

---

3) Availability → data must be available to the authorized user.

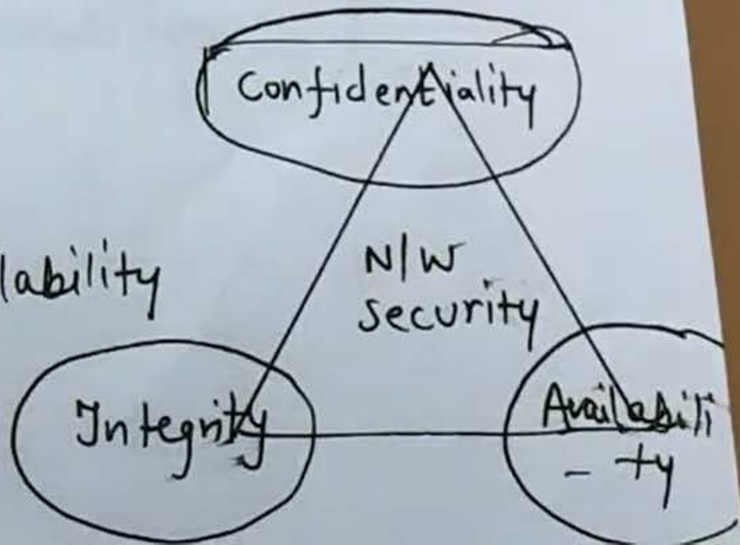
Info is useless if we cannot access it.

eg) what would happen if we cannot access our bank accounts for transactions.

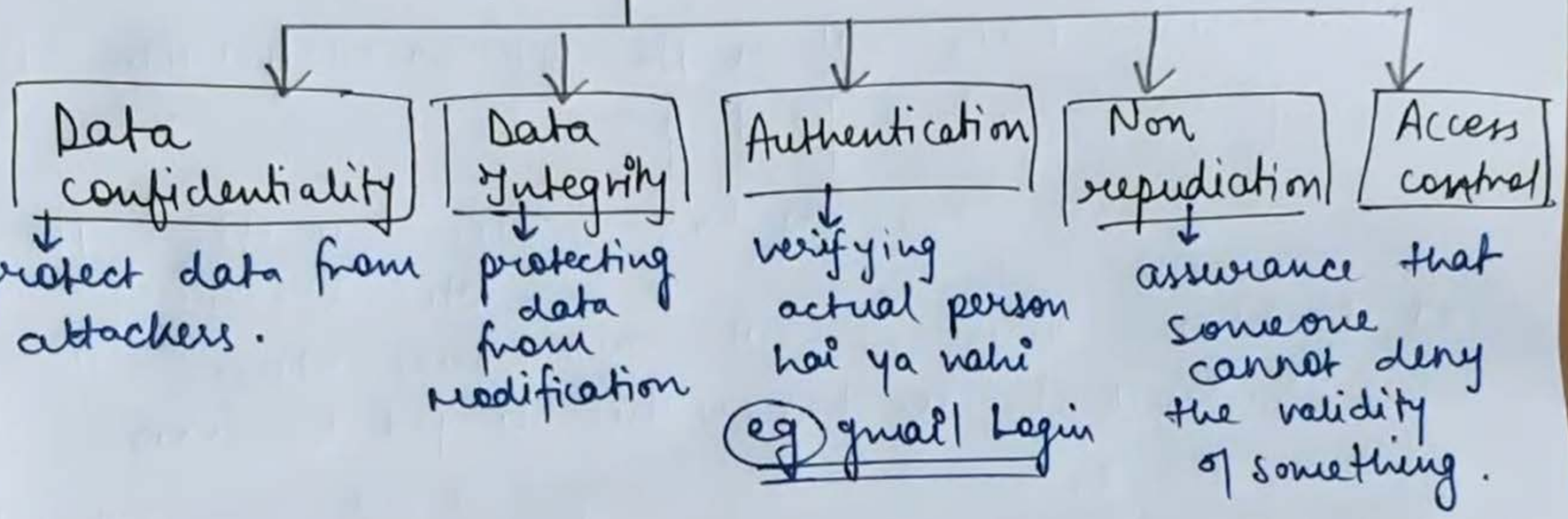
C I A triad in cryptography

↓

confidentiality, Integrity and availability



Security Services



Repudiation → denial of truth or validity of something
ie. act of claiming that something is invalid.

(H) **Non Repudiation** → is a service, which provides proof of the origin of data and the integrity of the data.

claiming that something is invalid.

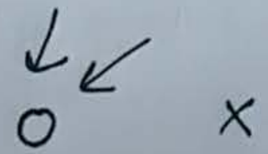
(4) Non Repudiation → is a service, which provides proof of the origin of data and the integrity of the data.

eg A give 1000 Rs check to B. and later B deny it.
It cannot happen b/c A will have its proof.

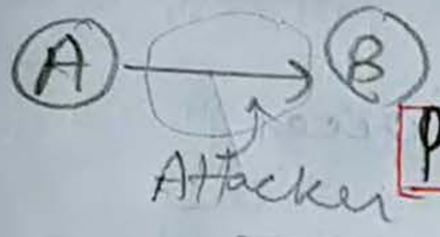
(5) Access control → to whom the access should be given can be decided.

or

The prevention of Unauthorized use of a resource (i.e, this service controls who can have access to our info, under what conditions).



Security Attacks



Passive Attack

Active attack

It attempts to learn or make use of the info from the system but doesnot affect the system resources.

i.e the attacker will only see the data he will not modify it.

We can prevent it using better encryption techniques.

Two types of passive attacks

1) Release of message content → attacker/hacker will easily be able to understand the data/inf

Two types of passive attacks

1) Release of message content → The attacker/hacker will easily be able to understand the data/info.

2) Traffic analysis → If we have encryption protection, an opponent/attacker might still be able to observe the pattern of these messages.

The attacker could determine the location and the identity of communication hosts and could observe the frequency and length of the message being exchanged.

This info might be helpful in guessing the nature of communication that was taking place.

Passive attacks are difficult to detect b/c they do-

Observe the pattern of

The attacker could determine the location and the identity of communication hosts and could observe the frequency and length of the message being exchanged.

This info might be helpful in guessing the nature of communication that was taking place.

Passive attacks are difficult to detect b/c they do not involve any alteration of data.

So, the sender & receiver will not be able to know whether a third person is reading their msg or NOT.

→ he can [see + modify] msg

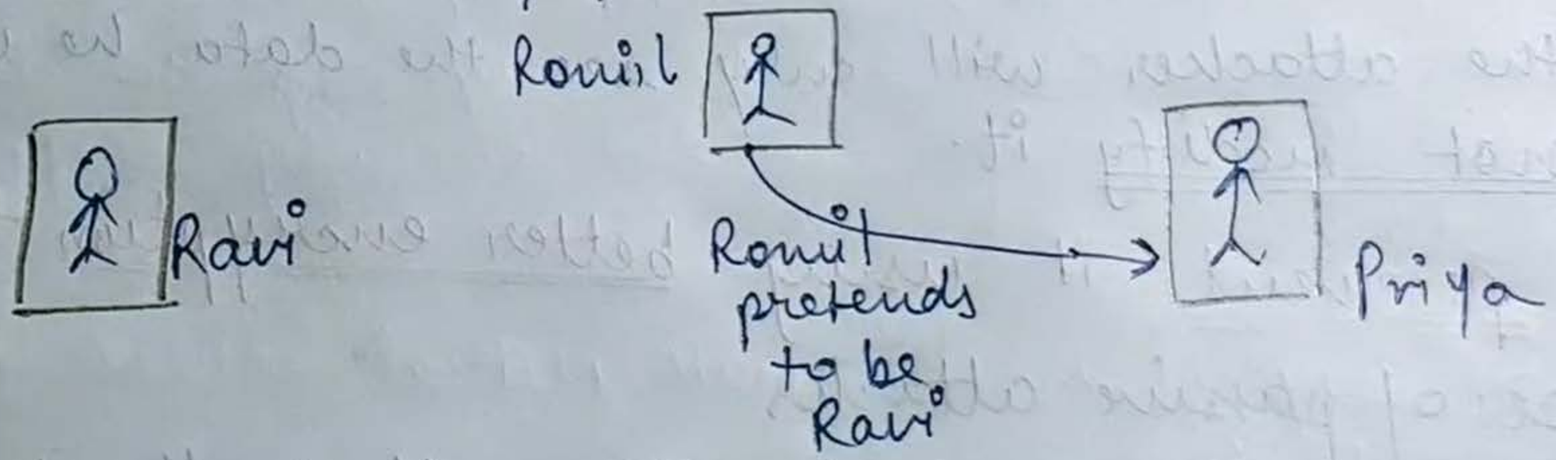
2) ACTIVE attacks

It attempts to alter system resources/ info [redacted].

(i) masquerade

→ when one entity pretends to be another entity.

eg

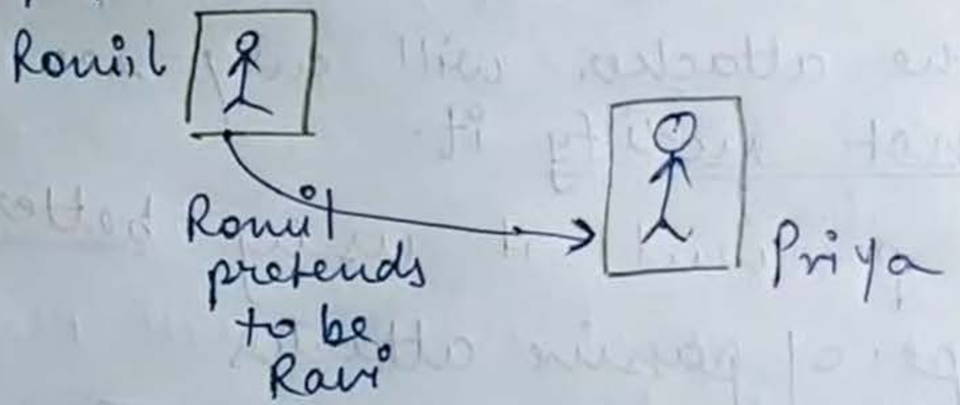


(ii) modification of messages

(iv)

(i) masquerade
→ when one entity pretends to be another entity.

eg



(ii) modification of messages
some portion of the message is altered or the message is delayed or reordered to produce an unauthorized effect.

eg) give 100 Rs to John

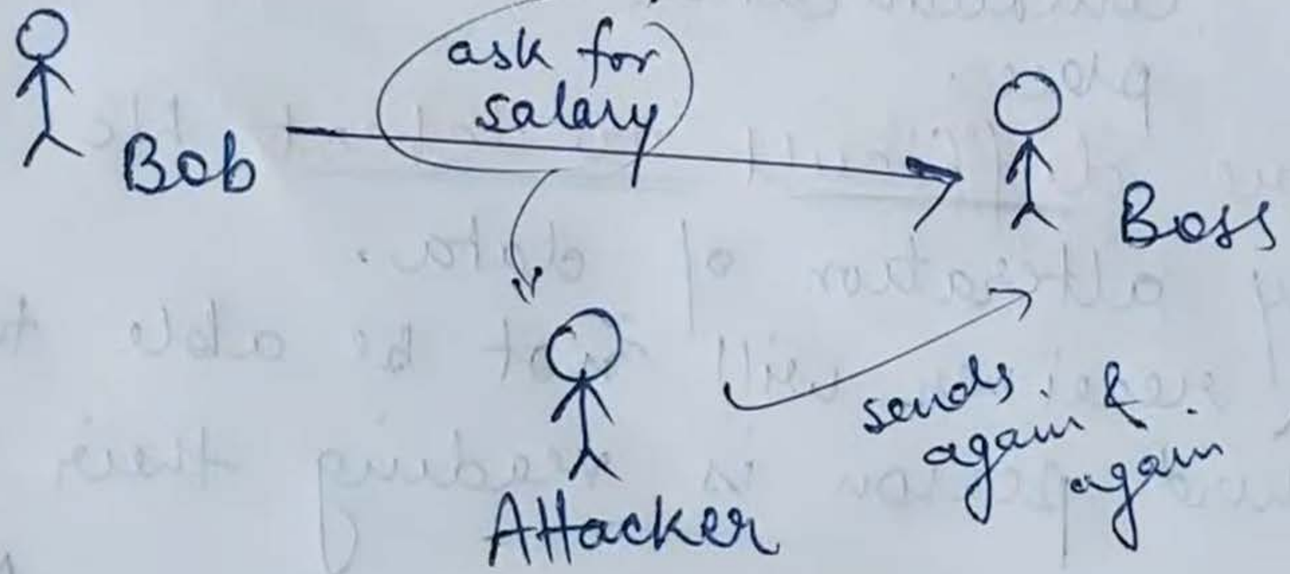
↓

give 500 Rs to Gaurav

give 500 Rs to Gaurav

(iii) ~~Replay~~ → Replay
involves passive capture of a message and its subsequent retransmission to produce an unauthorized effect.

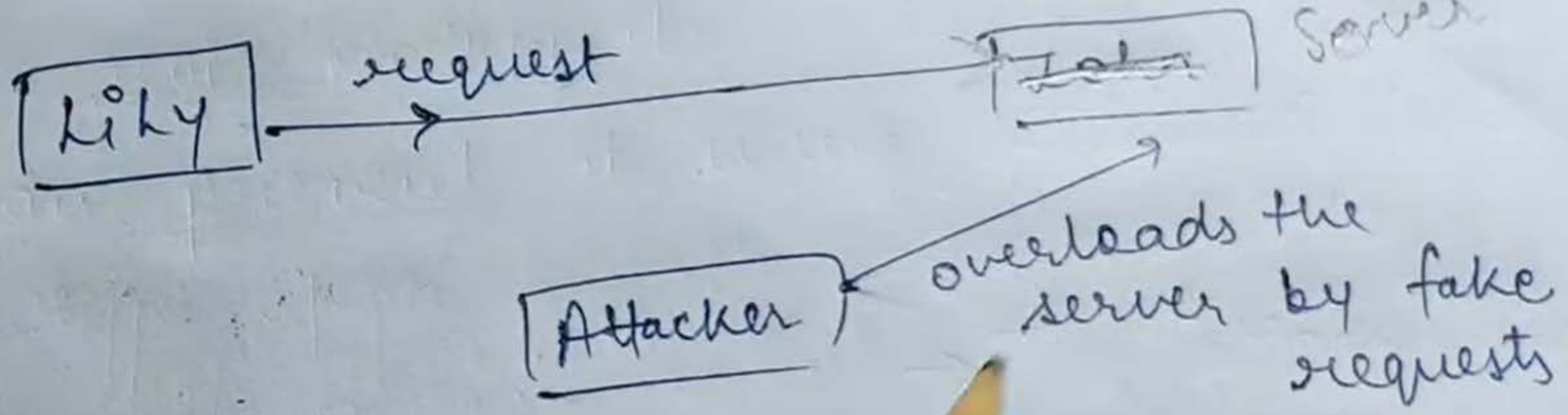
eg)



(iv) Denial of services

It prevents normal use of communication facilities.

eg) disruption of an entire network whether by disabling the network or by overloading it by messages so as to degrade performance.



5th video

Security Mechanisms

Security mechanisms are used to provide security.

1) Encipherment → The use of mathematical algo.s to transform data into a form that is not readily intelligible.

plain text to cipher text

2) Digital Signature → It is a means by which the sender can electronically sign the data and the receiver can electronically verify the

1) A ⟶ B

Plain → encrypt → ci

not readily intelligible.

plain text
to cipher text

2) Digital Signature → It is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

or we can say, it is a mathematical scheme for authentication.

3) Data Integrity →

1) A ⟶ B

Plain → encrypt → ciph

signature.

or we can say it is a mathematical scheme for authentication.

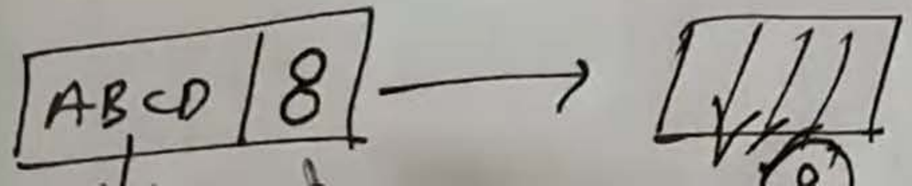
3) Data Integrity →

This mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver creates a new checkvalue from the received data and compares the newly created check-value with the one received.

If both the values are same, the integrity of

1) A ⟶ B

Plain → encrypt → cipher

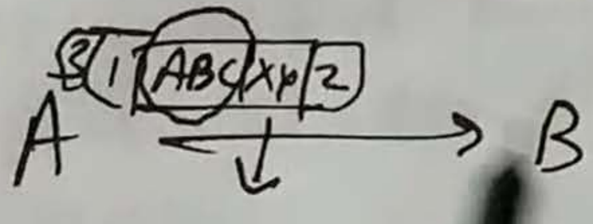


from the received data and compares the newly created check-value with the one received.

If both the values are same, the integrity of the data has been preserved.

4) Authentication exchange –
In this, two entities exchange some messages to prove their identity to each other.

5) Traffic Padding → In this technique, we add some extra/dummy bits with the data while encrypting



6) Routing control

means selecting and continuously changing different available routes b/w the sender & the receiver to prevent the attacker from eavesdropping on a particular route.

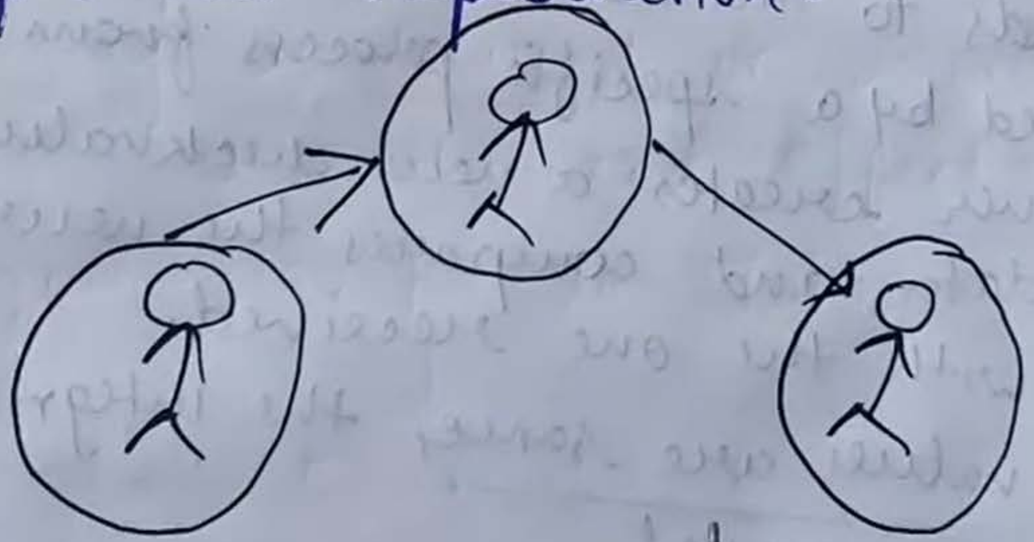
↓

पासू सी

ओएसपीएफ

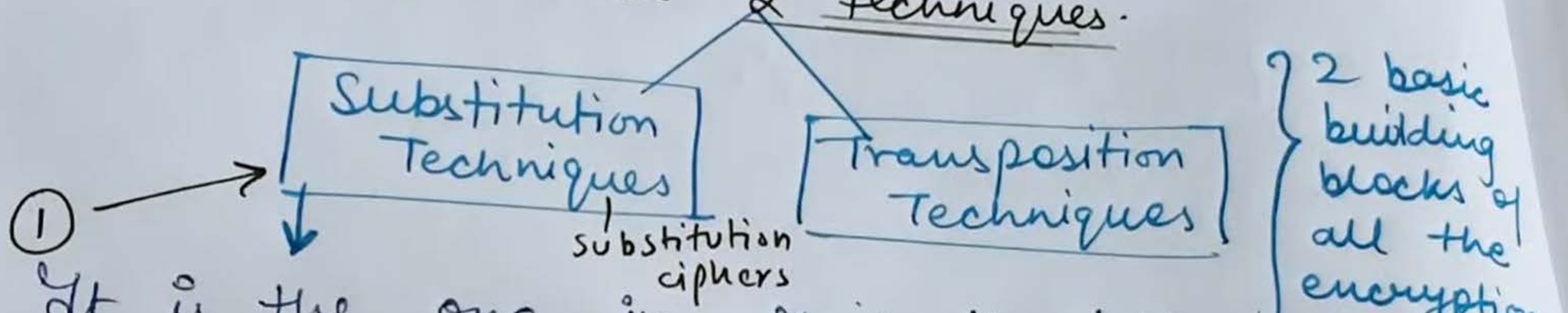
7) Access control -
These methods prove that a user has access right to the data.

8) Notarization → means selecting a trusted third party to control the communication between two entities. This can be done (for eg) to prevent repudiation.



CLASSICAL ENCRYPTION Techniques

Symmetric encryption also reffered to as conventional encryption is of 2 types or we can say it has 2 techniques.



It is the one in which the letters of the plain text are replaced by other letters or by numbers or symbols.

eg Name → I W P X

→ no replacement substitution

substitution ciphers

Techniques

blocks of all the encryption techniques

It is the one in which the letters of the plain text are replaced by other letters or by numbers or symbols.

eg Name → I W P X

↳ no replacement / substitution

(2) Transposition techniques / Transposition ciphers

performing some sort of permutations on the plaintext letters. ie it reorders the symbols.

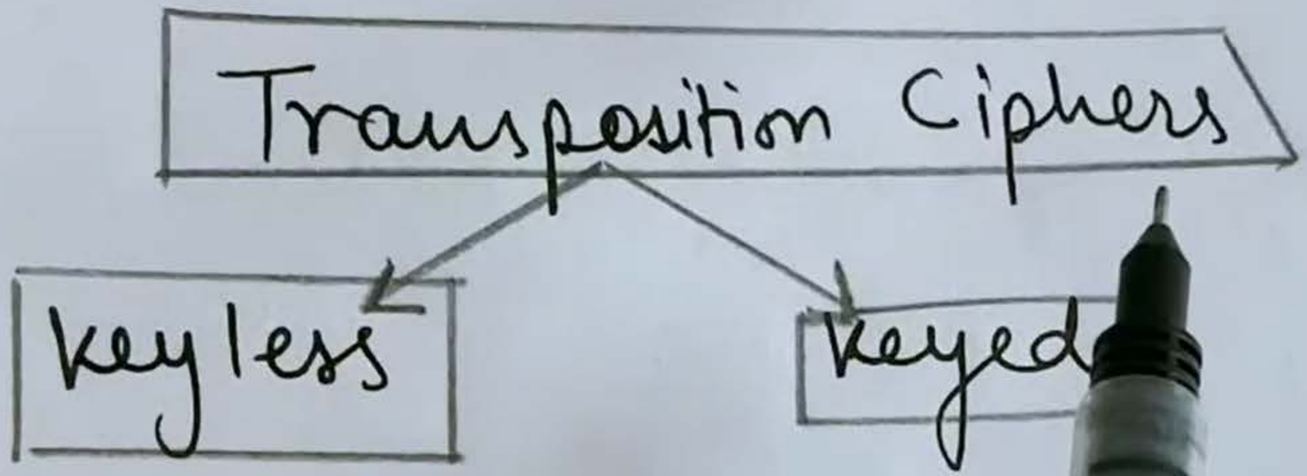
ie rearrangement of the letters of the plain text

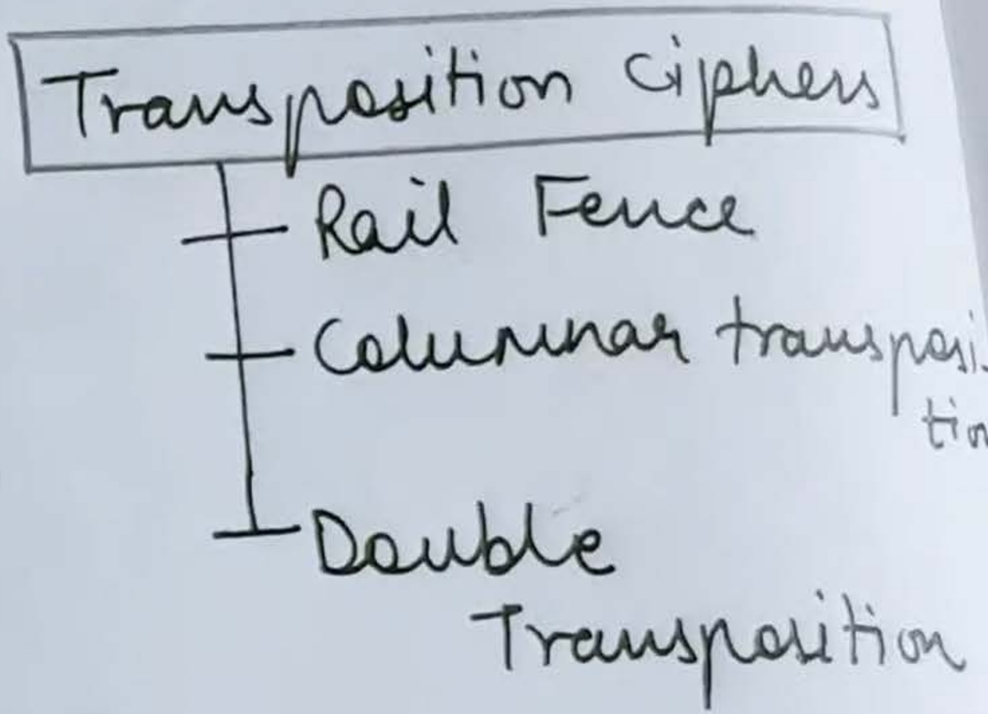
eg NAME → EAMN or AENM or MNEA, etc

These are of 2 Types

(1) Rail Fence Cipher or keyless transposition cipher

(2) [redacted]





Substitution Techniques

- Caesar cipher
- monoalphabetic ciphers
- polyalphabetic ciphers
  - Vigenere cipher
  - Vernam cipher
- Playfair cipher
- Hill cipher
- One time Pad

1) monoalphabetic substitution ciphers

A single cipher alphabet for each plain text alphabet is used throughout the process.

i.e fixed substitution always.

if 'N' then always 'J' in place of 'N'.

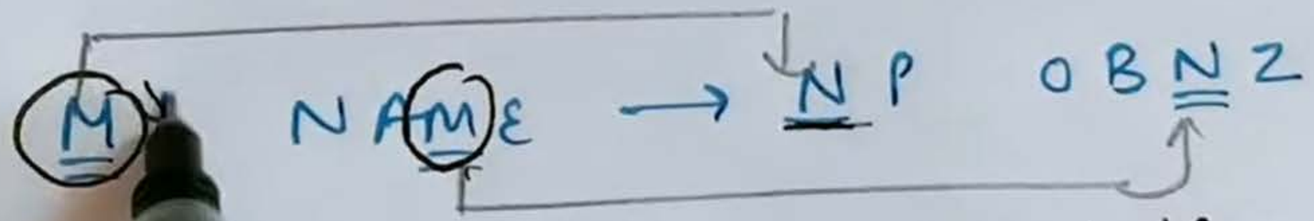
- polyalphabetic ciphers
  - Vigenere cipher
  - Vernam cipher
- Playfair cipher
- Hill cipher
- One Time Pad

1) Monoalphabetic substitution ciphers

A single cipher alphabet for each plain text alphabet is used throughout the process.

i.e fixed substitution thaga.

if 'N' → I use 'x' then always I will use 'x' only in place of 'N'.

eg. 

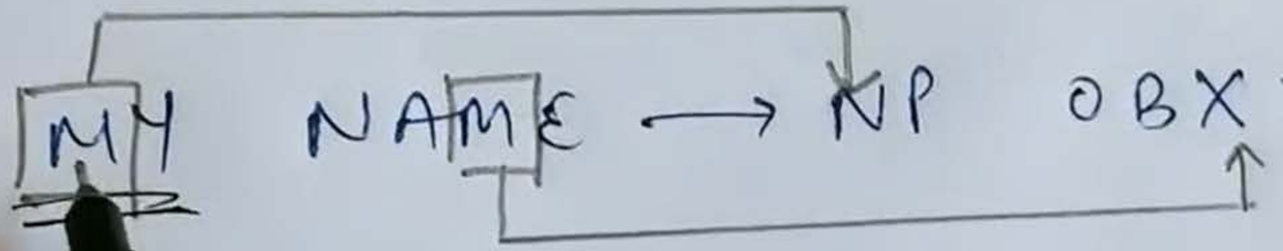
eg. in book

In monoalphabetic cipher, relation blw a character in the plaintext to a symbol in cipher text is always one to one

a character in the plaintext to a symbol in cipher text is always one to one.

2) Poly alphabetic substitution cipher.

* There is no fixed substitutions.
* Each occurence of a character may have a different substitute i.e. we can use more than 1 substitution for the same letter.



The relationship b/w a character in the plain text to a character in the ciphertext is one to many.

a → d and later a is replaced with m.

TRANSPOSITION Techniques

(i) no replacement of character.
(ii) we will rearrange the character's position ie we will apply some sort of permutation on the plaintext letters.

(i) Rail Fence technique

In this, the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

eg. "all the best for exams" → Plaintext

To encrypt this with a rail fence of depth 2, we write the following

a l t r x m

(1) Rail Fence technique

In this, the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

eg. "all the best for exams" → Plaintext

To encrypt this with a rail fence of depth 2, we write the following

```
a l l h b s f r x m
 l t e e t o e a s
```

encrypted msg is :-

A L H B S F R X M L T E E T O E A S

Note → used for short messages

→ easy to break by the attacker.

Note → used for short messages
→ easy to break by the attacker.

(ii) Row Transposition cipher

We write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of column.

key → integer value (unique digits from 0 to 9)

eg 45312

eg 4321 etc.

eg Plain → attack postponed until two am

key → 4 3 1 2 5 6 7

Plain text: → a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

~~4 3 4 1 2 5~~

a/c to Wikipedia ← sometimes left blank (IRRegular case)

extra/dummy bits

Ciphertext: TTNA APTM TSUO AODW COIX KNLY PETZ

explaination → (i) To encrypt, start with the column labelled as 1, i.e, in our example, column 3.

Write down all the letters of the column.

(ii) Now, proceed to column no. 4 which is labelled as column 2., then 2, 5, 6, and 7th column.

Double Transpo

* column or tran
applied twice
* The key in
* This techniq
German

Note → eg K
It

eg

Refer

Problem → can easily be understood by the attacker / 3rd party.

→ used for short msgs. only.

It can be made more secure by performing more than 1 stage of transposition. So, the result will be a more complex permutation.

Key →	4	3	2	5	6	7
PlainText →	t	n	a	a	p	t
	m	s	u	o	a	o
		c	o	i	x	k
		y	p	e	t	z

AUOP TTWL TMDN AOIE PAXT TOKZ

no space in between

Double Transposition

* Columnar transposition | Row transposition cipher applied twice
* The key in case 2 can be same/different also.
* This technique was used in world war I by German military and also in world war II

Note → eg keyword | key → STRIPE
It will be used as → 564231 } decided by the alphabetical order of letters in the key. (IMP)

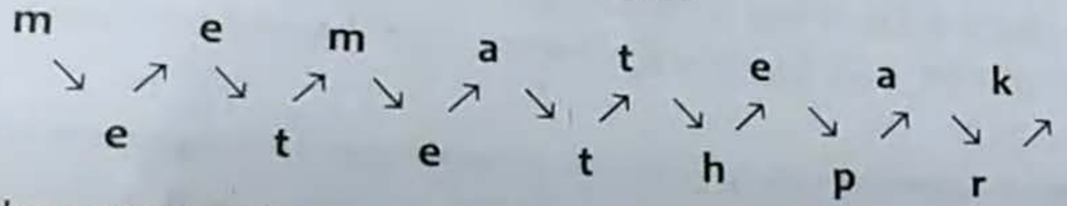
eg key → Z E B R A
→ 5 3 2 4 1

...position of the plaintext may appear in the tenth position of the ciphertext. A ...ciphertext may appear in the first position of the ciphertext. In other words, ...cipher reorders (transposes) the symbols.

A transposition cipher reorders symbols.

❑ **Keyless Transposition Ciphers** Simple transposition ciphers, which were used in the past, are keyless. There are two methods for permutation of characters. In the first method, the text is written into a table column by column and then transmitted row by row. In the second method, the text is written into the table row by row and then transmitted column by column.

EXAMPLE 3.22 A good example of a keyless cipher using the first method is the rail fence cipher. In this cipher, the plaintext is arranged in two lines as a zigzag pattern (which means column by column); the ciphertext is created reading the pattern row by row. For example, to send the message "Meet me at the park" to Bob, Alice writes



She then creates the ciphertext "MEMATEAKETETHPR" by sending the first row followed by the second row. Bob receives the ciphertext and divides it in half (in this case the second half has one less character). The first half forms the first row; the second half, the second row. Bob reads the result in zigzag. Because there is no key and the number of rows is fixed (2), the cryptanalysis of the ciphertext would be very easy for Eve. All she needs to know is that the rail fence cipher is used.

EXAMPLE 3.23 Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

```
m  e  e  t
m  e  a  t
t  h  e  p
a  r  k
```

She then creates the ciphertext "MMTAEEHREAEKTTP" by transmitting the characters column by column. Bob receives the ciphertext and follo[illegible] the reverse process. He writes the received message, column by column, and reads it row by row as [illegible] plaintext. Eve can easily decipher the message if she knows the number of columns.

EXAMPLE 3.24 The cipher in [illegible]ple 3.23 is actually a transposition cipher. The following shows the permutation [illegible]ch character in the plaintext into the ciphertext based on th positions.

01	02	03	04	[illegible]06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓										

the permutation: (01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15), and (00, 12, 24, 36), the difference between the two adjacent numbers is 4.

❑ ***Keyed Transposition Ciphers*** The keyless ciphers permute the characters by using writing plaintext in one way (row by row, for example) and reading it in another way (column by column, for example). The permutation is done on the whole plaintext to create the whole ciphertext. Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

EXAMPLE 3.25 Alice needs to send the message "Enemy attacks tonight" to Bob. Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group. The following shows the grouping after adding a bogus character at the end to make the last group the same size as the others.

e n e m y a t t a c k s t o n i g h t z

The key used for encryption and decryption is a permutation key, which shows how the characters are permuted. For this message, assume that Alice and Bob used the following key:

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

The first character in the plaintext block becomes the first character in the ciphertext block; the

encrypt

Keyless Transposition ciphers

enemy attac kston ightz

ciphertext →	3	1	4	5	2
Main →	1	2	3	4	5

1	2	3	4	5
e	n	e	m	y

cipher → e e y n

2nd 1:4
↳ (spa
n

(*) Now,
in
se
+
p

Caesar Cipher

- It is also called shift cipher / additive cipher.
- Each letter in the plaintext is replaced by a letter corresponding to a no. of shifts in the alphabet.
- It is a Monoalphabetic caesar cipher.
  It is one of the earliest and simplest method of encryption technique.

Note → Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes called Caesar ciphers.
He used a key of 3 for communications.

eg plain → Meet me
cipher → PHHW PH

Z	e	b	r	a
C	H	E	U	D

message

// Encryption

Ciphertext

$$C = E(k, p) = (p + k) \bmod 26$$

(message, key, plain)

// Encryption

For decryption,

$$p = D(k, C) = (C - k) \bmod 26$$

(ciphertext)

// if $(C-K)$ is -ve then add 26 to it

Numerical value is assigned to each letter

a	b	c	d	e	f	...	x	y	z
0	1	2	3	4	5		23	24	25

* If the cryptanalist/attacker knows a ciphertext, then he can apply brute-force technique to find the plain text by using all the possible 25 keys.

eg in book pg 64

Since it is a part of symmetric encrypt. Same key is used for encryption and decryption.

$$1 \leq K \leq 25$$

eg | pg-49 book

eg message → "HELLO"

let key = 4

$C(H) = (p+k) \bmod 26$

$= (7+4) \bmod 26 = 11 = L$

$C(E) = (p+k) \bmod 26 = (4+4) \bmod 26 = 8 = I$

$C(L) = (p+k) \bmod 26 = (11+4) \bmod 26 = 15 = P$

$C(O) = (P+K) \bmod 26 = (14+4) \bmod 26 = 18 = S$

(i) desig

(*) It i

The

Playfair Cipher Algorithm

It was invented in 1854 by Charles Wheatstone. but was named after Lord playfair, who promoted the use of cipher.

Cipher → Algo for encrypting and decrypting

ciphertext → process which applies different types of algos. to convert plaintext → coded text is called ciphertext.

ALGORITHM

1) Create 5 X 5 matrix that is called grid of letters.

Cipher → Algo for encrypting and decrypting

ciphertext → process which applies different types of algos to convert plaintext → coded text is called ciphertext.

ALGORITHM

1) Create 5 x 5 matrix that is called grid of letters.
2) The matrix is made by inserting the values of key and remaining alphabets into the matrix (row wise from left to right) where, letter I and J will be combined together.
3) Convert the text into pairs of alphabet

eg Heya → He ya

(a) pair cannot be made with same letters. Break the letters into single and add 'x' to the previous letter

eg Hello → He lx

made by inserting the values of key and remaining alphabets into the matrix (row wise from left to right) where, letter I and J will be combined together.

3) Convert the text into pairs of alphabet

eg Heyar → He ya r

(a) pair cannot be made with same letters. Break the letters into single and add 'x' to the previous letter

eg Hello → He lx lo

Helloe → He lx lo e

alone problem

(b)
If the letter is standing alone in the process of pairing, then add 'z' with the letter.

eg Helloe → He lx lo e(z)

e was alone so we added z Here.

Hexxoe → He xz xo ez

x was already there so, we took 'z'

(4.) Code be formed using 3 rules:

are in the same row,

He xxoe → He xz xo ez

Here.

x was already there so, we took 'z'

(4.) Code will be formed using 3 rules:

(i) If both the alphabets are in the same row, replace them with alphabets to their immediate right.

(ii) If both the alphabets are in the same column, replace them with alphabets immediately below them.

(iii) If not in same row/column, replace them with alphabets in the same row respectively, but at other pair of corners.

aabhjiii

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

KS → FU

Plain Text

B M →
R W →

Same row

F G →
U Q →
Q W

added Here.

so, we took

same row,
their immediate

column,
below

with

1) Create
2) The ma
and
(row
I a
3) Convert
eg
(a) pa
eg

encryption,
nd

49
book

Vigenere cipher

(i) designed by Blaise de Vigenere (16th century French mathematician).

(ii) It is a polyalphabetic substitution cipher

The encryption is done using a (26 x 26) matrix or
↓
ie a Table

Method (1) → Vigenere Table → used to find cipher-text

eg. Plain Text = GIVE MONEY

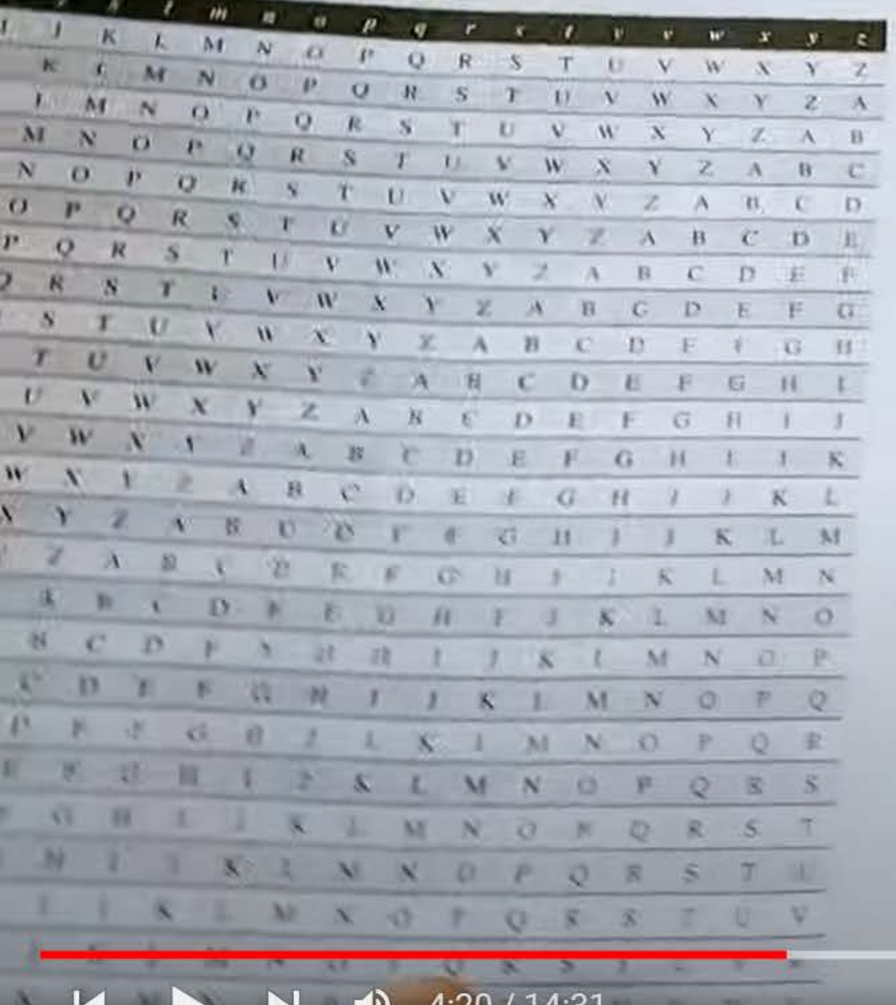
Key = LACK

soln →

G	I	V	E	M	O	N	E	Y
L	O	C	K	L	O	C	K	L

VIGENERE CIPHER in Cryptography Method-1

Vigenere cipher as a combination of m additive ciphers



(16th century French mathematician).

② It is a poly alphabetic substitution cipher

The encryption is done using a (26×26) matrix or ie a Table

Method (1) → Vigenere Table → used to find cipher-text

eg Plain Text = GIVE MONEY

Key = LOCK

soln →

P →	G	I	V	E	M	O	N	E	Y
K →	L	O	C	K	L	O	C	K	L

Repeat the letters of the key so that the no. of letters in P and K ie Plaintext and becomes equal.

cipher → R W X O X C P O J

For Decryption,

cipher → R W X O X C P O J

Key → L O C K L O C K

H

Method-2 When the table is not given

1) Encryption

$C_i = E_i = (P_i + K_i) \bmod 26$ // $E_i \rightarrow$ encryption

(Ci → ciphertext)

2) Decryption

$D_i = (E_i - K_i) \bmod 26$ // $D_i \rightarrow$ decryption

(Ei → Ci)

eg Plaintext → "she is listening"

Key → "PASCAL"

∴ key stream → (15, 0, 18, 2, 0, 11). The key stream is the repitition of this initial key stream (as many times needed).

Plain	s	h	e	i	s	l	i	s	t	e	n	i	n	g	
P's value															

$C_i = (E_i - K_i) \bmod 26$ // E_i → encryption // D_i → decryption

[eg] Plaintext → "she is listening"

key → "PASCAL"

∴ key stream → (15, 0, 18, 2, 0, 11). The key stream is the repitition of this initial key stream (as many times needed).

Plain	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
key stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Cipher Text	H	H	W	K	S	W	X	S	L	G	N	T	C	G

VERNAM CIPHER

(i) used for encrypting alphabetic text.
(ii) simply a type of substitution cipher.

In this, we assign a number to each character of plain-text like (a=0, b=1, c=2, ... z=25).

Length of key used for encryption = length of plaintext.

eg Plain Text → RAMSWARUPK
Key → RANCHOBABA

Soln → Plain text →

17	0	12	18	22	0	17	20	15	10

Key →

key → RAMSWARUPK

key → RANCHOBABA

Soln → Plain text →

17	0	12	18	22	0	17	20	15	10
→ 17	0	13	2	7	14	1	0	1	0
(PT+key) after adding → 34	0	25	20	29	14	18	20	16	10
subt → 8	0	25	20	3	14	18	20	16	10

Cipher → I A Z U D O S U Q K

Now, for Decryption,

Cipher →	8	0	25	20	3	14	18	20	16	10
key →										
CT- 1 →										

Shannon's Theory of confusion and Diffusion

1) The terms confusion and diffusion were introduced by Claude Shannon.

2) Shannon's concern was to prevent cryptanalysis, based on statistical analysis. The reason is as follows:

Assume attacker has some knowledge of the statistical characteristics of the plaintext (eg in a msg, the frequency distribution of the various letters may be known.
If these statistics are in any way reflected in the ciphertext, the cryptanalyst i.e attacker may be able to deduce the encryption key.

reflected in the ciphertext, the cryptanalyst
i.e attacker may be able to deduce the
encryption key.

Thus Shannon suggested 2 methods for frustating the attackers:

1) confusion } properties for creating
2) Diffusion } a secure cipher.

DIFFUSION → In simple words, if a symbol in the plaintext is changed, several or all symbols in the ciphertext will also change.

BOOK

→ The idea of diffusion is to hide the relationship between the ciphertext and plaintext.

the symbols in the plaintext.

2) CONFUSION → is maintained as complex as possible.

→ It hides the relationship b/w ciphertext and the key.

→ If a single bit in the key is changed then most/all bits of the ciphertext will also be changed.

A/c To wikipedia,

Confusion means that each bit of the ciphertext should depend on several parts of the key, obscuring the connection b/w the two.

obscuring: make unclear or difficult to understand.

In short,

diffusion → make statistical relation blw plaintext and ciphertext as complex as possible

if change 1 bit of plain then half or more bits of cipher should change.

confusion → makes relation blw key & ~~plain~~ cipher text as complex as possible.

each bit of ciphertext should depend on key.