7/1/25

cryptography — Type of security
— Need " "
— Algo (existing) " "

Algo

* Key → Based on key uses key cannot
* Key less → New algo proposed

1 Key for locking & unlocking

2 Key for locking using 1 and unlocking for an with other

locking → Encryption
unlocking → decryption

Total 10 to 15 Algo

* Straight forward Algo based Questions
Either with Algo or numerical based on Algo

Data Encryption Stand. DES

what are the security services

Atul Kahate book

. Security → Protection of Data
→ Types :-
* No security
* Password / Id
* Security through hiding / Obscurity
* Security through Encryption

. Principle of security :-

→ C I A → Availability
Confidentiality
Intigrity

→C → Private data
→I → ২য় ব্যক্তি or কোন প্রয়োজনীয় তথ্য প্রবেশ করে
Trustworthy
→Availability → Access of a thing when it's needed (cutting)
→Access control → Authorized user can access only

Role Management = user specific
Rule Management = more of resources.

→ Authentication → Verification of sender / receiver.
→ Non-repudiation → Denial / falsification of service.

Security Attacks

Passive Attack

- No modification done by the attacker to the message or data
- only sees the info and gain access
- Sol → Try & Error থেকে try করে detect করা

Active Attack

- Easy Detection
- modifies the original message

} solution

- Example → Man In the Middle Attack

* Cryptography :—

↓

study or science of

Def:-

The art / science of achieving security through encryption is called cryptography.

Encryption → converting Plain text into ciphur text

Plain text: text that is understandable or readable or meaningful

ciphur text: non understa... non meaningf... non intelligi... abl...

college (meaningful)

↓ using an algo

AbDLJX (non meaningful)

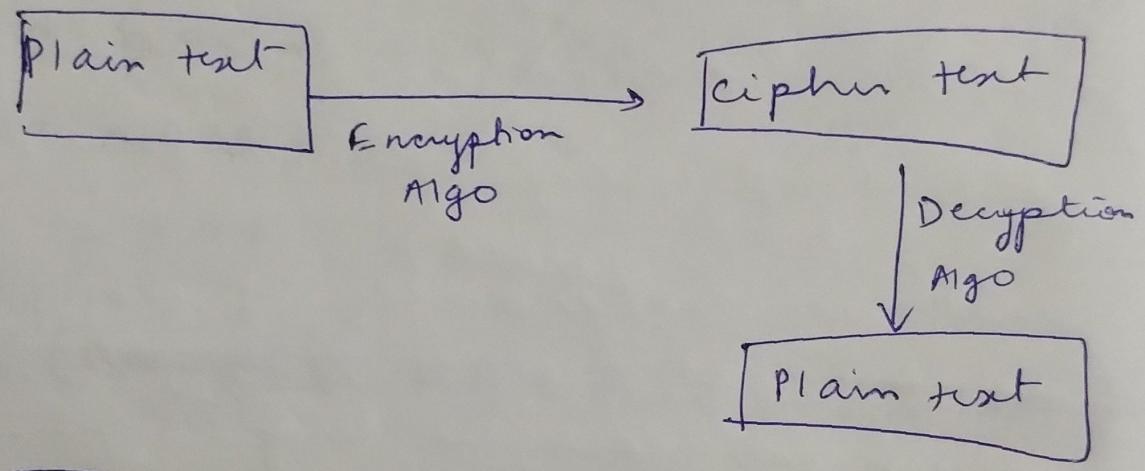
Cryptography

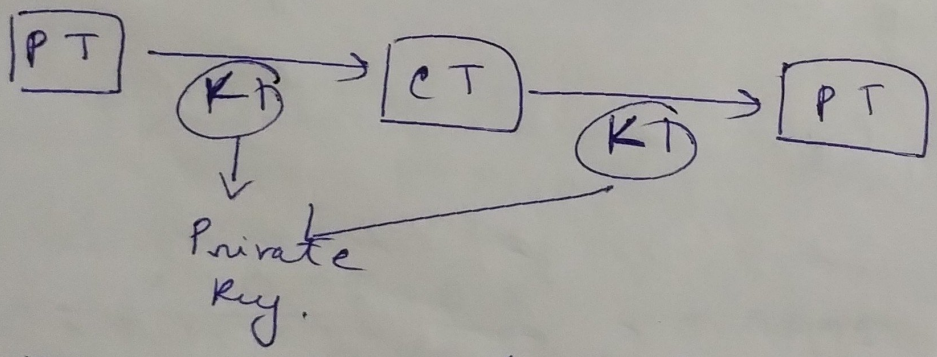
14/1/25

Key

- Symmetric Key Cryptography
  - Also known as private key cryptography
- Asymmetric Key Cryptography
  - Also known as Public key cryptography

It is also known as private key cryptography





KT is with sender and with some security channel it is assumed that KT is shared to the reciever. that would help reciever to decrypt the text.

Encryption & decryption done only using 1 Key is called Symmetric

* Assymetrical key Crypto

there consist of 2 Key

- Public key (Encryption is done using this key)
- Private key (Decryption is don using this key)

Plain text	→ Encryption K1 →	Cipher Text	→ Decryption K2 →	Plain text

K1 = Public Key (access to all)

K2 = Private Key (access to me or ~~specific~~ known to me).

- Encryption is don by the public key given by the receiver
- ~~those want to send them~~
- Receiver will use his/her private key to Decrypt the message.

Special case

Encryption → Public key

Decryption → Private key

Lis [illegible] [illegible] [illegible] $\frac{1}{2}$ case

* Hash code

No Keys are used of Encryption & decryption

Hash f^n is used converts var length Plain text into fixed length Ciphen text

This encrypted message or ciphen text is called message digest

big Plain length converted into consise ciphen text that's why ciphen text is known as message digest.

DES, MD5
Message digest-5

Techniques of- Cryptograph Algo

: Substitution Tech

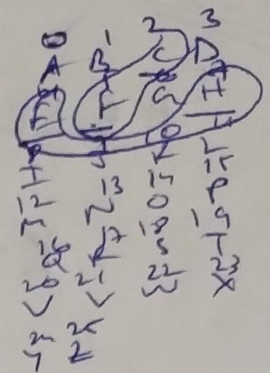
Transposition Tech → changing the pos of the actual text

HELLO → each input is substituted by another alphabet
↓ ↓ ↓ ↓ ↓
(J X Z Z A) ciphen text

HELLO → (E L H L O) ciphen text.

1st cryptography algo ever proposed is

* CEASER CIPHER *



C E A S E R

+3 +3 +3 +3 +3 +3

F H D V H U → [illegible]

Now this concept comes under the concept of 'Mono alphabetic ciphering'

There are 2 typs of ciphers

'Mono....

'Poly alphabetic ciphers'

Mono alphabetic

Meet me at two Pm

↓ ↓ ↓

X X X

ciphering is Encipher

Decipher is Decrypt

~~If~~ similar ~~alphabet~~ input produces similar o/p.

Poly alphabetic

Meet me at two Pm

↓ ↓ ↓

X Y Z

MCQ

'HELLO' encrypt the text using CEASER Alg

K = 4 (it means key is 4)

H E L L O
+4 | +4 | +4 | +4 | +4
L I P P S

} for 1 marks

But 3 marks ? Ashla we need to show the steps

step 1

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

C → ciphertext, E → Encryption, P → plaintext, K → key

26 → Total alphabet in a alphabetical order

$P = D(C, K) = (C - K) \bmod 26$

D → Decrypt.

(If '-ve' then add 26)

A B C D . . . Z
0

In cryptography A to Z 'A' numbering is starts with 0 and ends in 25.

$1 \leq K \leq 25$ (only applicable for CEASER CIPHER)

~~Hfct~~

HELLO , K=4

steps

$e(H) = (H + 4) \bmod 26$

$= (7 + 4) \bmod 26$

$= 11 \bmod 26$

$= 11$

$= L$

$e(E) = (E + 4) \bmod 26$

$= 4 + 4 \bmod 26$

$= 8 \bmod 26$

$= 8$

$= I$

$e(L) = (L + 4) \bmod 26$

$= (11 + 4) \bmod 26$

$= 15 \bmod 26$

$= 15$

$= P$

$e(O) = (O + 4) \bmod 26$

$= 14 + 4 \bmod 26$

$= 18 \bmod 26$

$= 18 \Rightarrow S$.

$\therefore$ KEY = LIPPS

... between 2/ words / more.
we would omit the space

```
HELLO   WORLD
|||||   |||||
LIPPS   XYZAB
```

Key = LIPPSXYZAB

We omit or preferably not use the space when converting into cipher text to make the text more confusing.

Cryptography

15/1/25

Transposition

Repositioning of the alphabets in a text

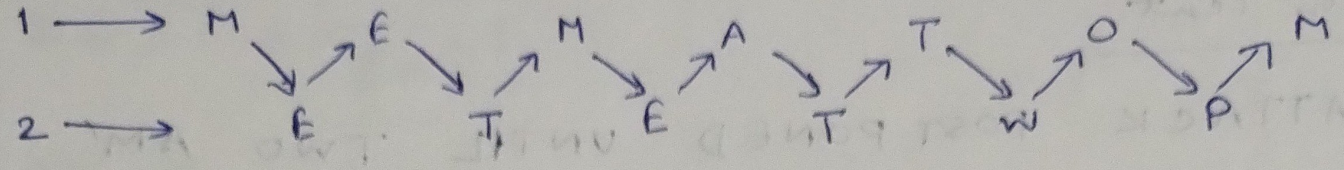
Transposition
- Keyed
- Keyless

1. Rail-Fence Algorithm :-

In this case no of rows is 2.

Plain text [illegible] convert it into cipher text using this algo.

Plain Text :- Meet Me At Two Pm



no. of colums are not divided because it depends on the input size. Only row is fixed.

∴ Ciphen Text → MEMATOMETETWP

We wrote the elements present in the 1st row followed by the elements present in the 2nd row.

2. Row/Transposition ciphen :—
Simple Columnar

Key will be given in this algo and Key will be an Integer value.

Key → Integer

Ex:- Key → 42135, 12435, 54132, . . . etc

In case Key is not Integer then,

Ex:- Key → CRYPTO
146352 → our Key

We would do the number in the order that which letters come 1st in the alphabetical order

→ Write the Key Row wise
Read the Key column wise.

Plain Text

'ATTACK POSTPONED UNTIL TWO AM'

Key → 146352

1	4	6	3	5	2
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	V	W	X	Y	Z

dummy / vulgous characters

Row and column no is fixed in this algo

যদি cell খালি থাকে then we need to add dummy characters in these cells.

=

cipher text → Write the text column wise

APNIM TOELV TSDTW ATUWX CPNOY KOTAZ

3. Double columnar method:—

Row transposition method 2 times

Key same থাকবে

and 2nd time we will take the cipher text as the Plain text then again generate

KEY = BATTLE
2 1 6 5 4 3

Plain Text :-

ENEMIES ARE READY TO ATT

2	1	6	5	4	3
E	N	E	M	I	E
S	A	R	E	R	E
A	D	Y	T	O	A
T	T	A	C	K	Z

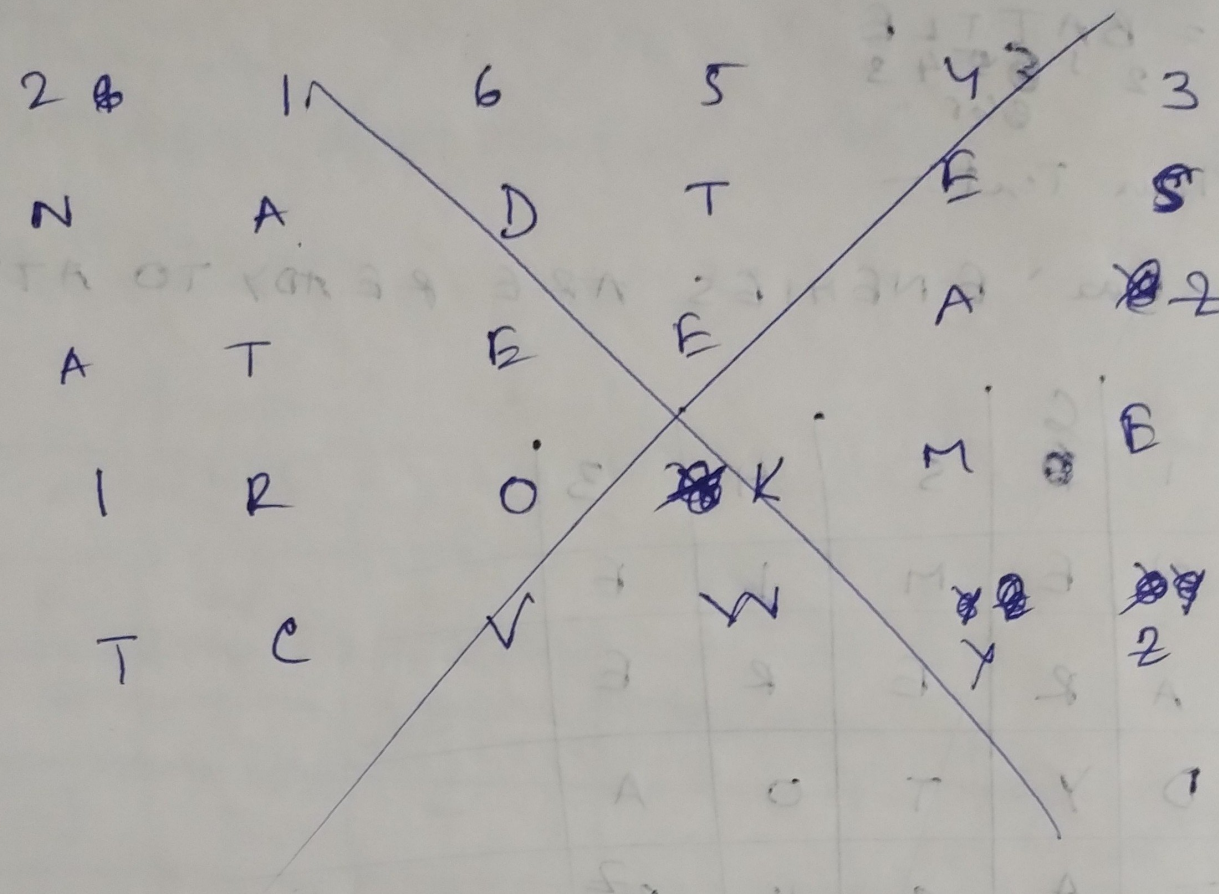
CIPHER text :- ESATNADTERYAMETCIROKEEAX

NADTESATEEAXIROXM
ETE

2	1	6	5	4	3
B	S	A	T	N	A
D	T	E	R	Y	A
M	E	T	C	I	R
O	K	E	E	A	X

CIPHER Text → EDMOSTEKAETETRCENYI
AAARX

2 1 6 5 4 3
N A D T E S
A T E E A X
I R O X M E
C T Y Y

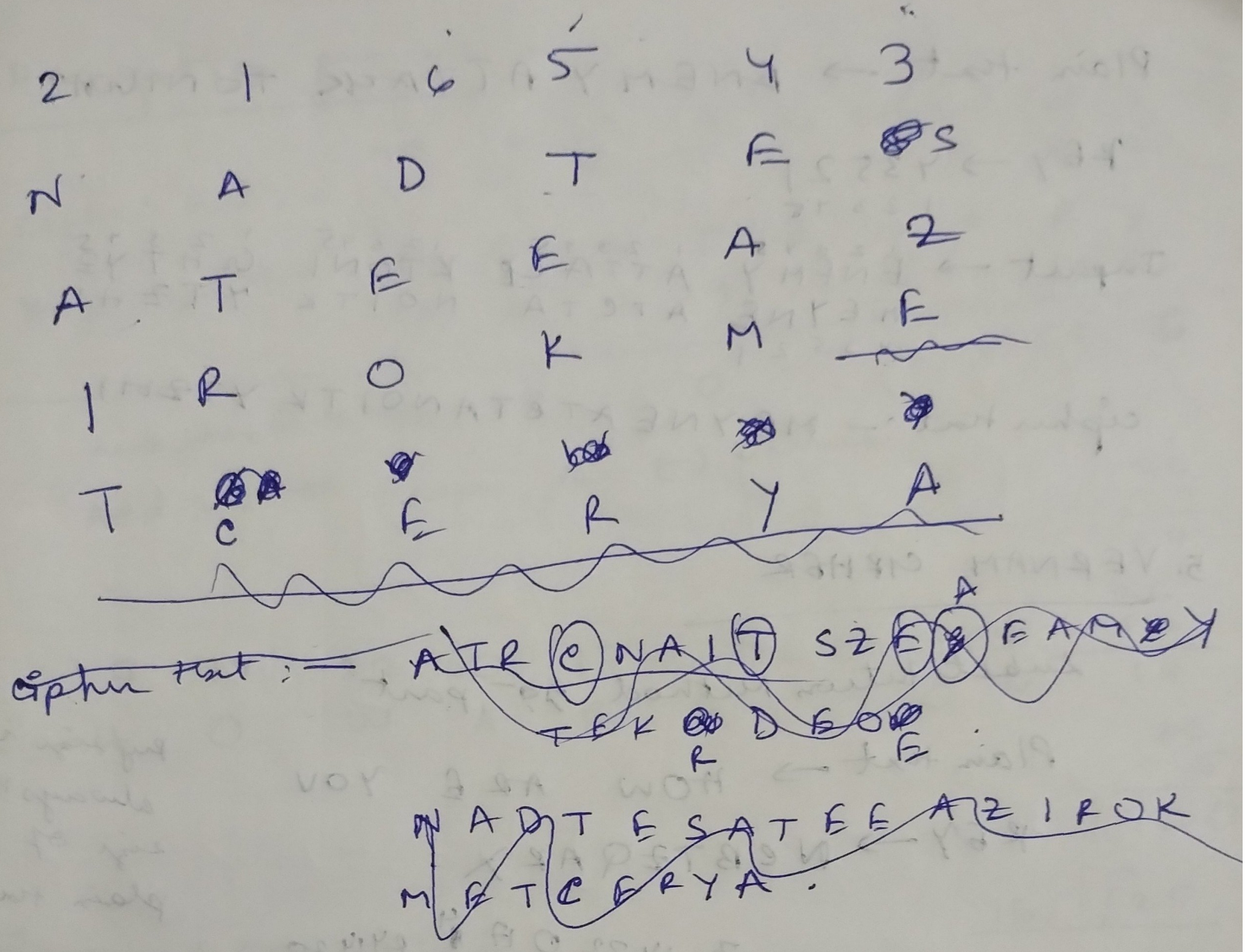


BATTLE = 21 65 43
21 65 43

2 1 6 5 4 3
E N E M I E
S A R E R E
A D Y T O A
T T A C K Z

* Always Place the ciphur key in continue numbering Ex:- 1 2 3 4 5 6

~~E S A T N A D T E R Y A M E T C I R O K~~
1 2 3 4 5 6
NADT ESAT EEAZ IROK METC BRYA



Ciphertext → ATRC NAITSZEA EAMY

TEKRDEOE

V.good

4. Key Transposition

Plain text will be given to you

Key will be given

Plain

Plain text → ENEMY ATTACK TONIGHT

KEY → 43521
1 2 3 4 5

Input → ENEMY ATTAC KTONI GHTYZ
MEYNE ATCTA NOITK YTZHI
4 3 5 2 1

cipher text :- MEYNEATCTANOITKYTZHI

5. VERNAM CIPHER

Substitution Method 9:- part

Plain text → HOW ARE YOU

KEY → NCBTZQARX

Key size always equal to size of plain text

Plain text → H O W A R E Y O U
7 14 22 0 17 4 24 14 20

Key text → N C B T Z Q A R X
13 2 1 19 25 16 0 17 23

Add → 20 16 23 19 42 20 24 31 43

Substract 26 From the values that are exceeding the value 25.

20 16 23 19 16 20 24 05 17

cipher text → U Q X T Q U Y F R

Decryption process

ciphertext :-		20	16	23	19	16	20	24	5
		U	Q	X	T	Q	U	Y	E	R
key text :-		N	C	B	T	Z	Q	A	R	Y
		13	2	1	19	25	16	0	17	23

Subtract = 7 14 22 0 -9 4 24 -12 -6

Add 26 from the (-) values

26 − 9 = 17

26 − 12 = 14

26 − 6 = 20

7 14 22 0 17 24 24 14 20

Plain text :- H O W A R E Y O U

Cryptography

22/1/25

6) Playfire Cipher

Plain text: SISTER NIVEDITA UNIVERSITY

In playfir
I/J are
considered
same

Key: CRYPTOGRAPHY

1	2	3	4	5
C	R	Y	P	T
O	G	A	H	B
D	E	F	I/J	K
L	M	N	Q	S
U	V	W	X	Z

INPUT:

SI ST ER
NI VE DI TA
UN IV ER SI TY

Rule:

1) If the alphabet in the pair is in the same Row then your input text all the characters will be substituted by the immediate right next neighbouring character in the row.

2) If they are in same column then next immediate character below will be substituted with the following character

3) If the characters are not in same R & C then diagonally we take the characters and we will write their corresponding alphabets.

cipher text: QK ZB MG QF RM EK YB WL EX

ER SI TY
MG QK CD

∴ QKZBMGQFRMEKYBWLEXMGQKCD

Plain text: NETWORK SECURITY

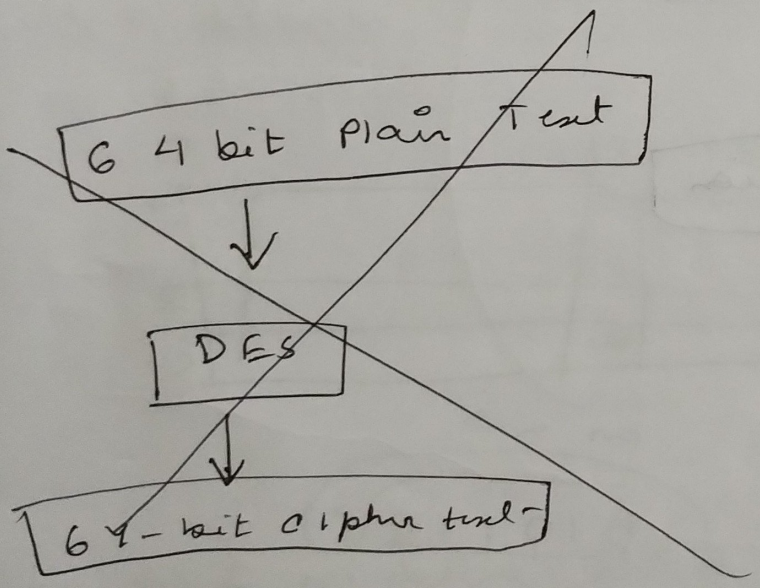
KEY: ATTACK

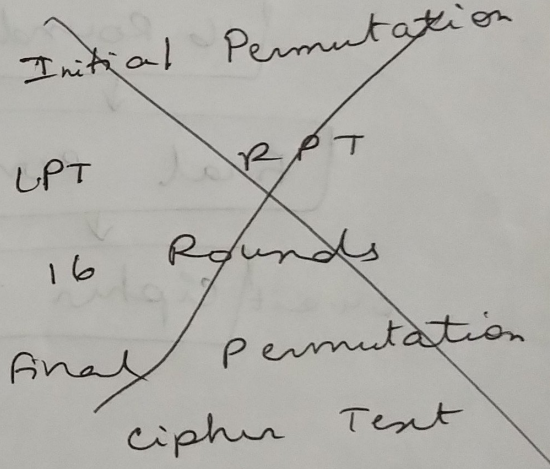
A	T	C	K	B
D	E	F	G	H
I/J	L	M	N	O
P	Q	R	S	U
V	W	X	Y	Z

NE TW OR KS EC UR IT YZ

→ LG ET ~~WO~~ MU GY FT PS LA ZV

Cipher Text: LGET MU GYFTPSLAZV





If there is similar letter then

TOMMY

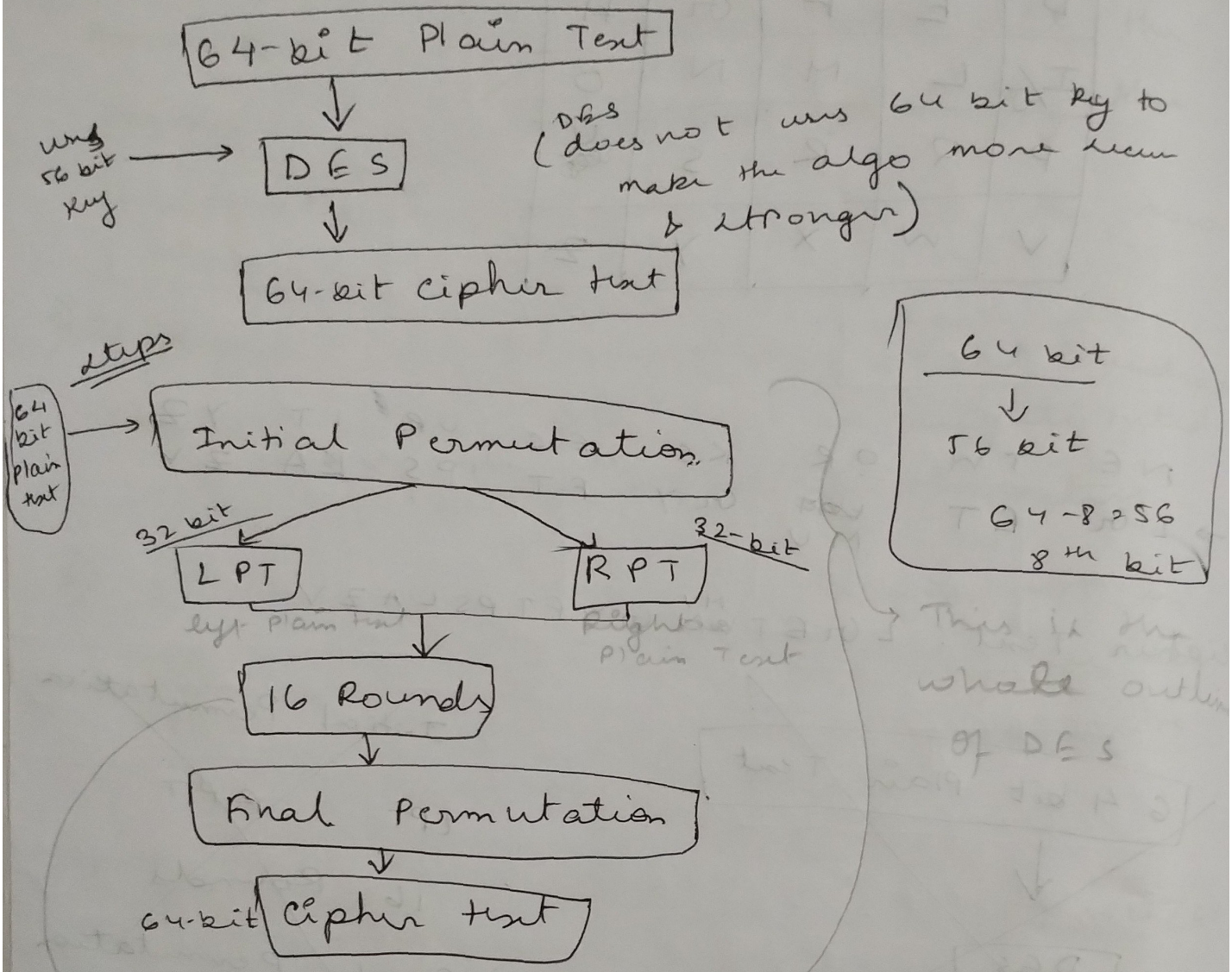
∴ TO MX XM YZ

TALL

TA LX XL

∴ TA LX XL

Data Encryption Algorithm (DES)

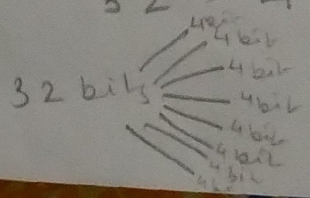


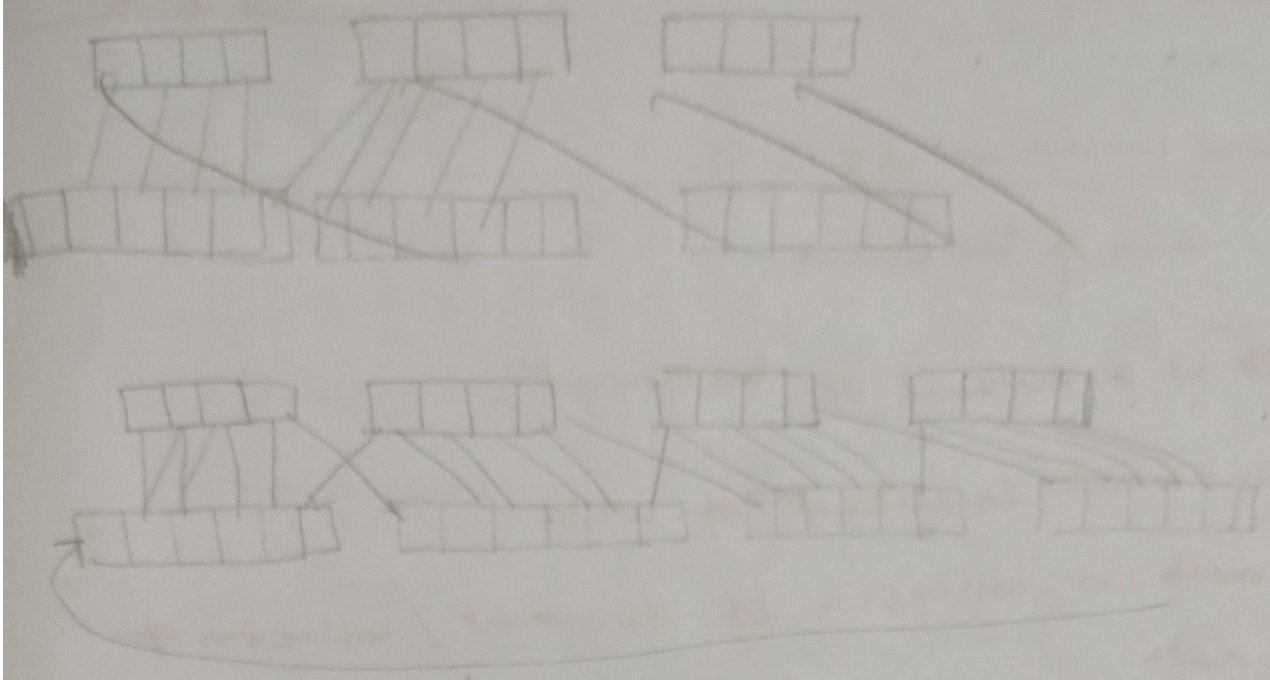
Rounds (out of 16 we will discuss on 1 round 32 bit 1 st Round & rest 16 rounds same)

1. Key Transformation from 1 forming to another form 56 bit → 48 bit Key

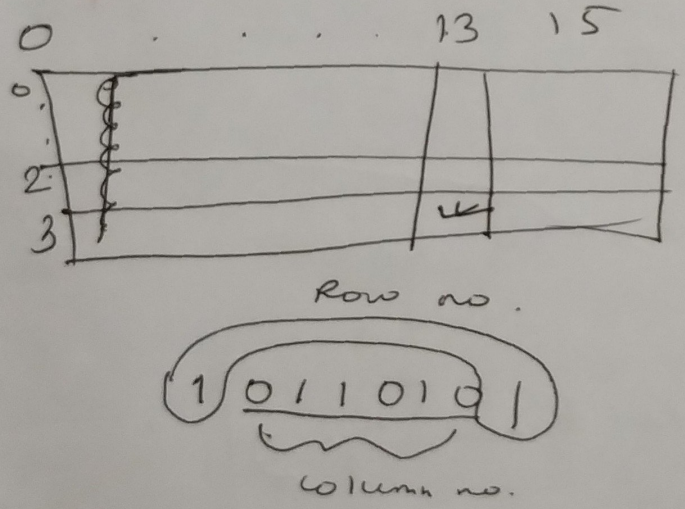
2. Expansion Permutation (all the steps would be applied to the RPT).

32 → 48 bit





3. X box substitution (XOR → 32-bit)



1,

↓

3 Row no.

0 1 1 0 1 0

↓

13 column no.

4. P-box substitution

Juggling up the data and making it 32 bit.

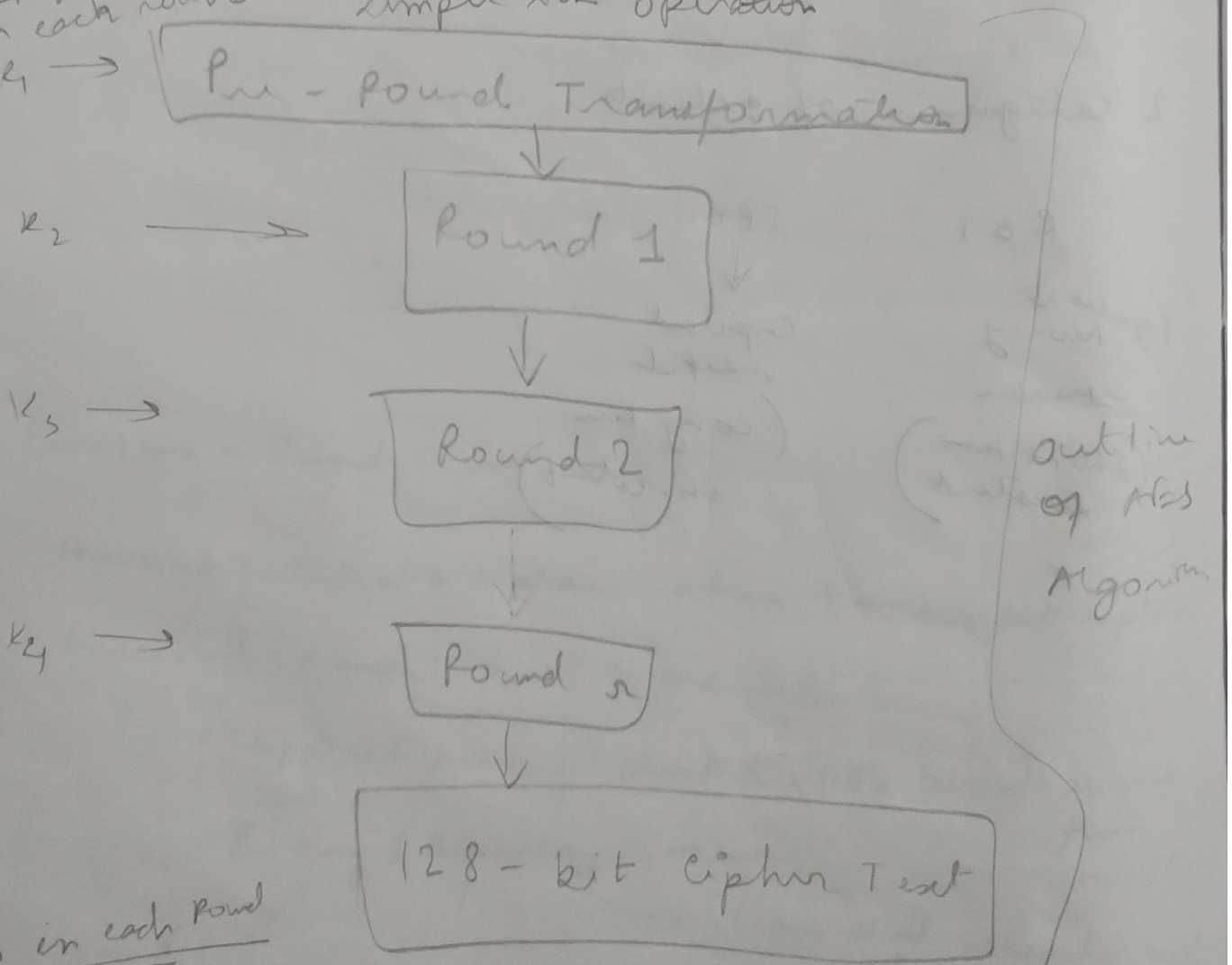
5. XOR and ~~substi~~ swap.

cryptography

∴ AES → advanced version of DES.

Rounds	No. of Keys	Version
10	128 bit	AES 128
12	192 bit	AES 192
14	256 bit	AES 256

Subkeys is getting used in each round. Simple XOR operation



outline of AES Algorithm

Steps in each Round

1. Substitution Bytes
2. Shift Rows or Permutation (Repositioning)
3. Mix Columns

Round 1 → Round 2

4. Add Round Keys

—: AES :—

was proposed in early 2000's

and in was proposed by Rijndael and accepted by US military by 2001.

It is same as DES only with some changes.

In DES the size of i/nput text is 64bit
in AES " " " " is 128 bit
In DES there was 16 rounds and 4 steps in each round and 1 key was used that is 56 bit key

In AES, the key size } are variable.
no. of Rounds }
no. of Rounds dinpends on no. of keys

If no. of Round is = 10,
key = 128 bit

Key expansion (চাবি সম্প্রসারণ)
From Original Key we need to find sub keys

Original key (K) → Sub key (K_1, K_2, K_3, ...)

~~No of Key bits~~

In each round we will use the ~~key~~ subkey

no. of subkeys = no. of round + 1

Ques,

Round = 10

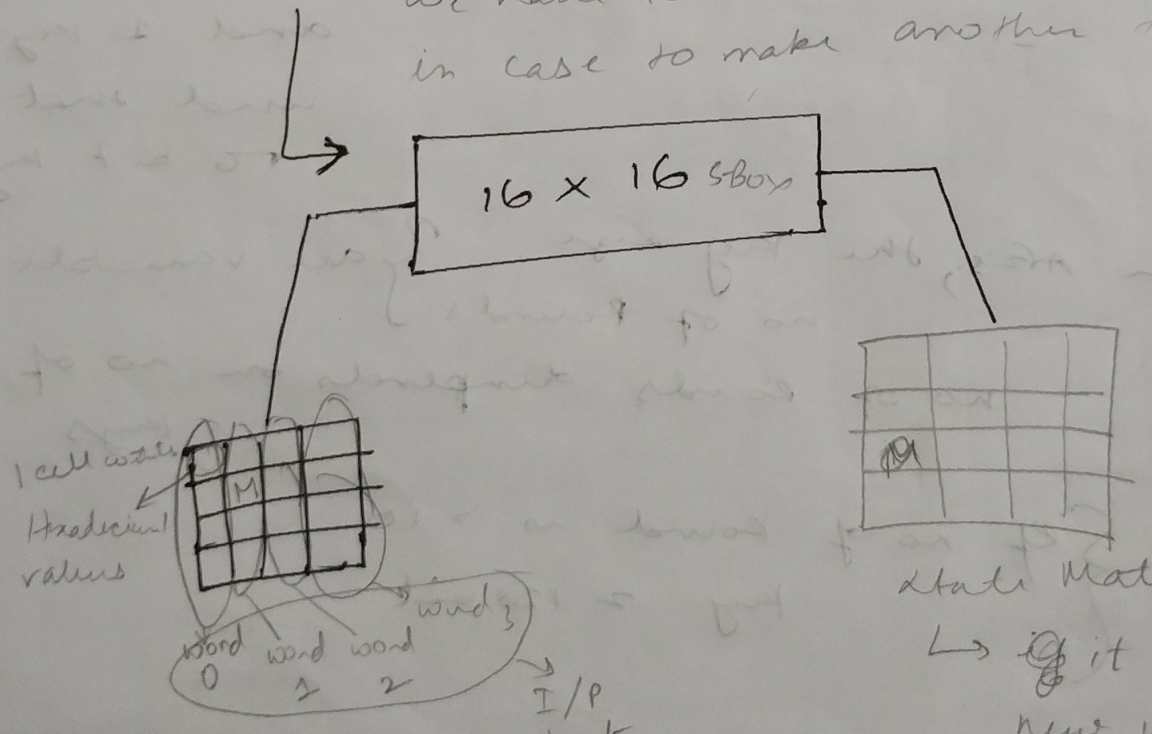
Key size = 128

no. of subkey = 10 + 1 = 11

Steps

1. Substitution Bytes :—

We have to substitute some bytes in case to make another text.



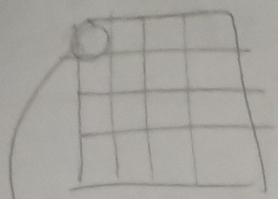
Each word Hexadecimal values

State Matrix
↳ it saves the new values of the input

128 bit

$\frac{128}{8}$ byte = 16 byte

[1 word = 1 column. = 4 byte = 32 bit] standard

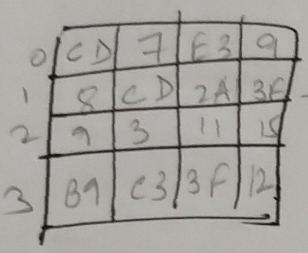


I/P

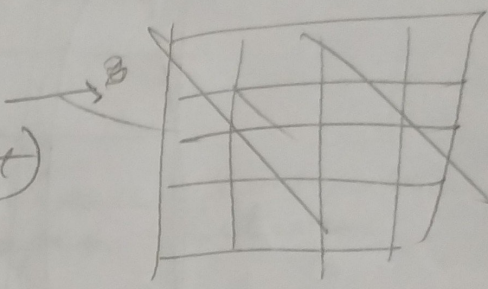
0101 — Row

1010 — Column

Shift Rows :

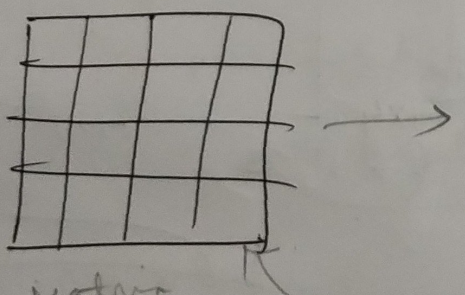


→ Shift Row (only using Left shift)

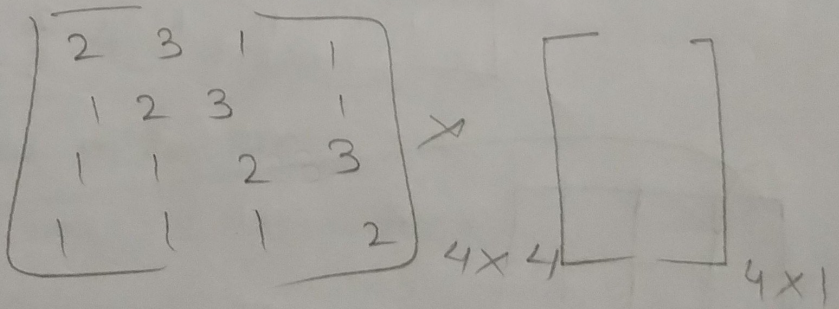


CD	7	E3	9	0 shift
CD	2A	3F	8	1 shift
11	15	9	3	2 shift
12	B7	C3	3F	3 shift

Mix Columns :-

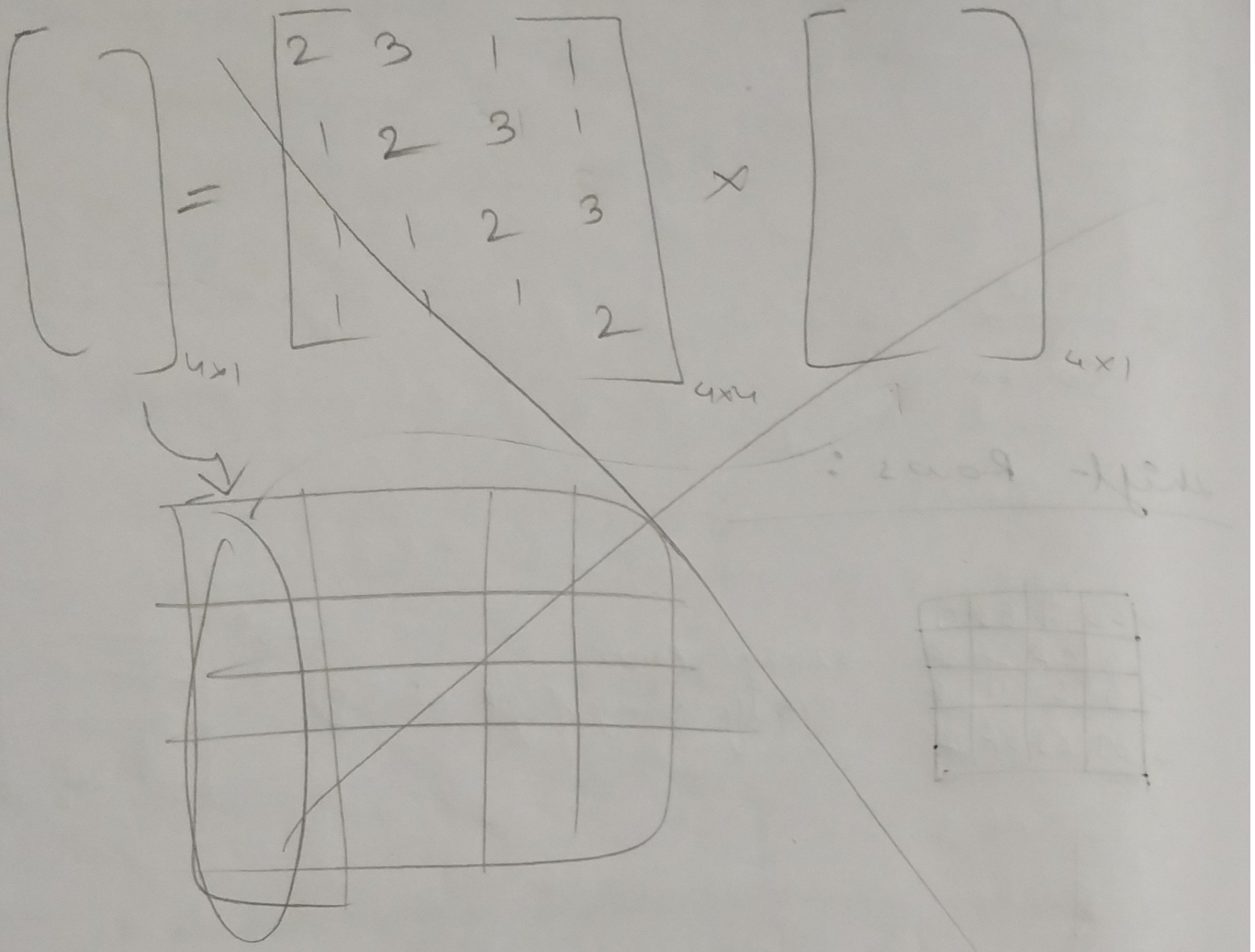


matrix

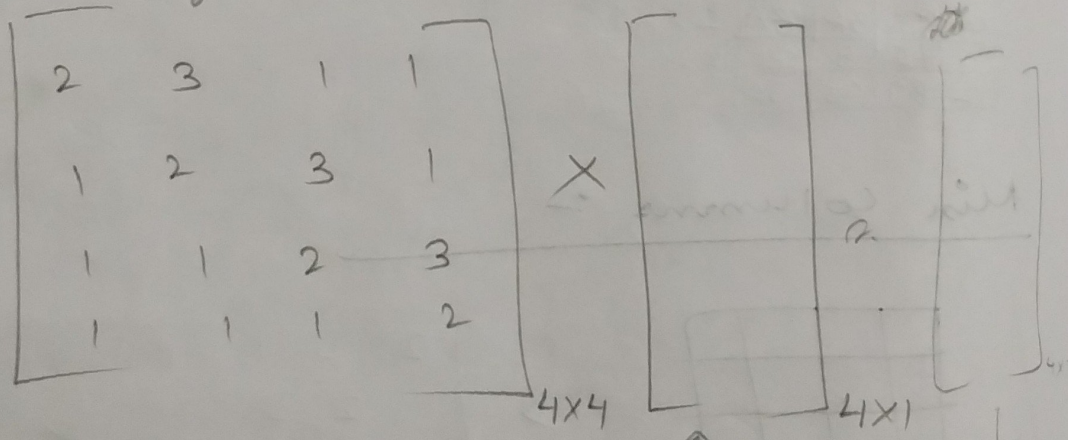


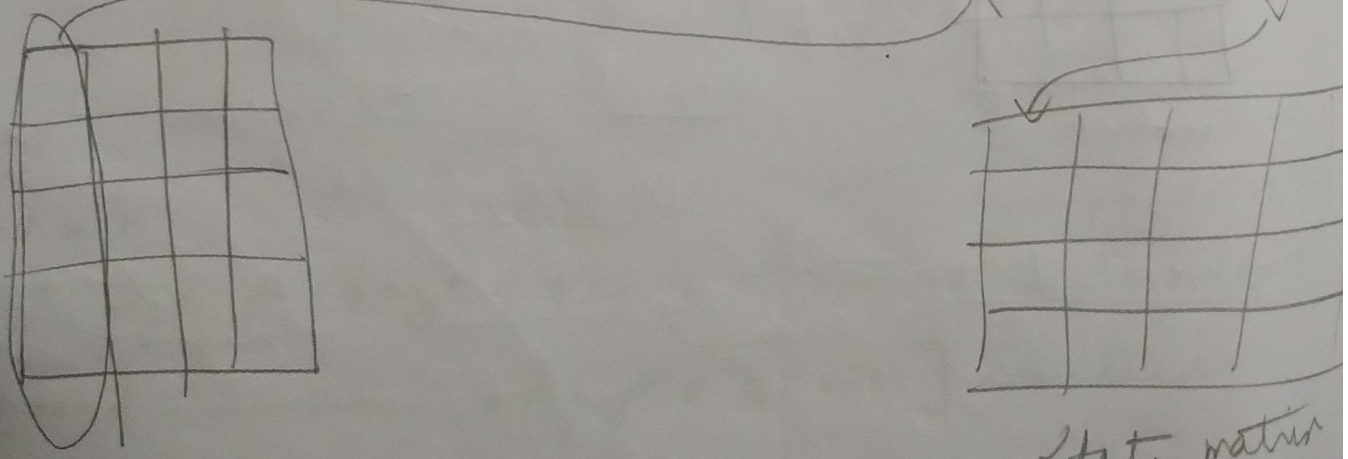
Predefined matrix

we need to mix this matrix with predefined matrix



Predefined matrix

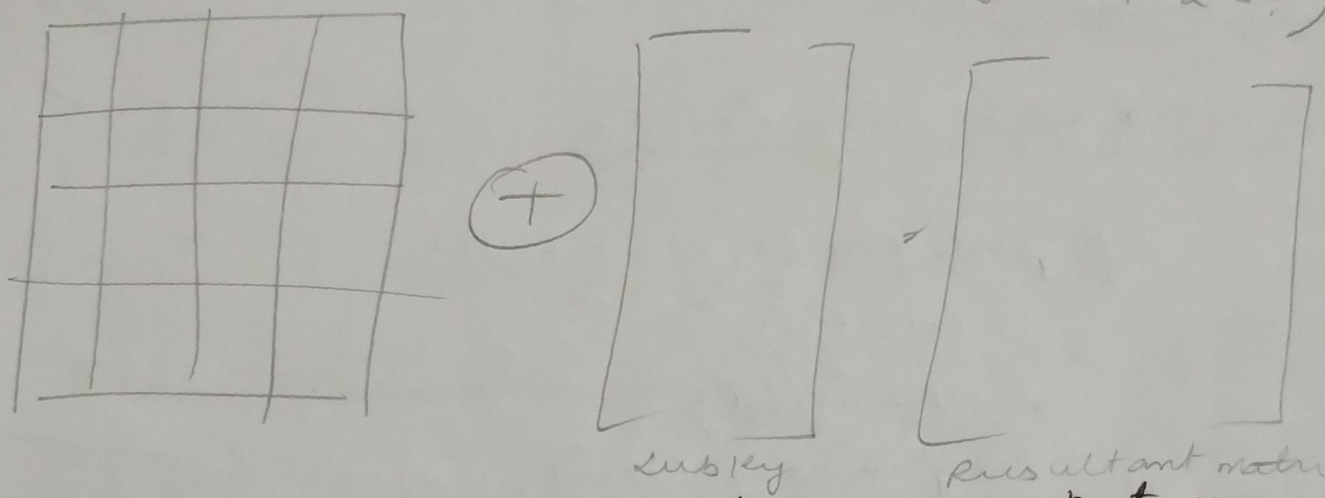




State matrix

Last step

Add Round Key :— (Pre Round Transformation)



Simple XOR operation would happen between

1 round and 1 sub key.

No. of sub ky = Round + 1

10 + 1

11 subkey

1 Key = sub ky = 4 bytes

∴ 11 subkeys = 44 bytes

∴ 44 bytes are required

In Last Round to all the steps will be there except 3rd step or Mix Column step.

Cryptography

International Data Encryption Algo (IDEA)

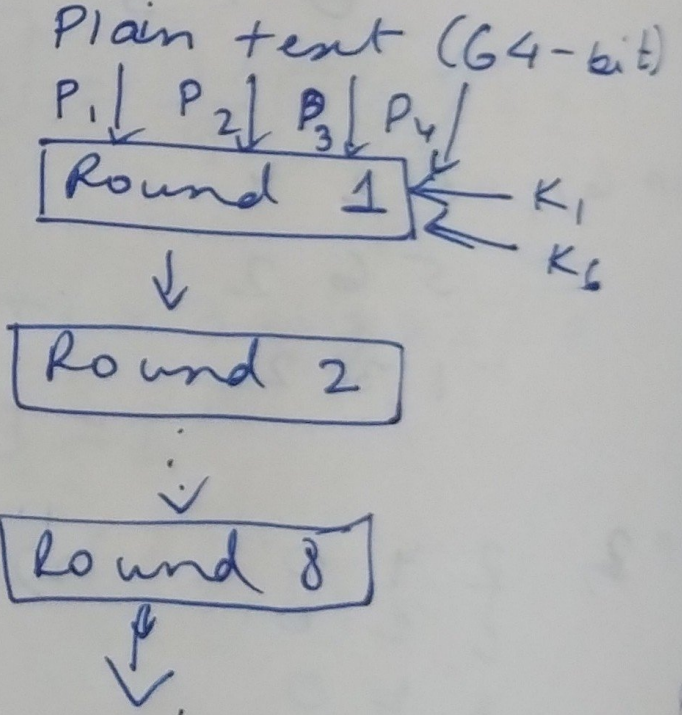
Plain Text : 64 - bit

Key : 128 - bit

Round : 8

Plain text is divided into 4 parts

Total 6 Keys required in each round.



4 Keys Required in last round.

O/P Tranformation → 64-bit ciphen text

No. of steps in each round : 14

STEPS

1. Multiply P1 & K1
2. Add P2 & K2
3. Add P3 & K3
4. Multiply P4 & K4
5. XOR Step 1 & Step 3
6. XOR Step 2 & step 4
7. Multiply step 5 & ~~step~~ K5
8. Add step 6 & step 7
9. Multiply step 8 & K6
10. Add step 7 & step 9
11. XOR step 1 & step 9
12. XOR step 3 & step 9
13. XOR step 2 & step 10
14. XOR step 4 & step 10

Rivizat ciphen-5 (RC5)

Plain Text → 16, 32, 64

Keys → 0-225 } (8 bit)
Rounds → 0-255 } var to make connection secure

Plain text has 2 bit data
suppose → if 16 → then 8b + 8b (2 bit)
if 32 → then 16 + 16

PTO

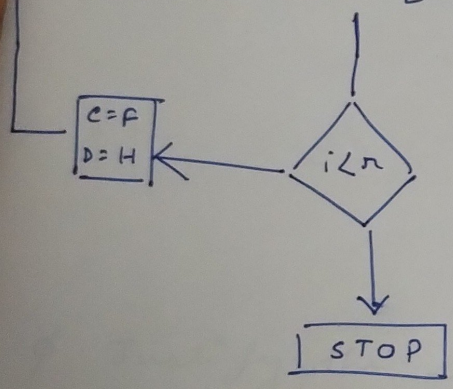
1. Plain text is divided into 2 similar parts → A & B

2. Add A and s[0] (subKey) → C

   Add B and s[1] (subKey) → D

   let counter = i;

3. XOR C and D → E
4. Circular left shift E by D bit
5. Add E and s[2i] → F
6. XOR E and F → G
7. Circular left shift G by F bits
8. Add G and s[2i+1] → H



Blowfish

Plain Text → 64-bit

Key → 32 bit – 448 bit

4 – Sboxes → 256 bit

No. of subkeys → 14

↳ eg: s[0]
s[1]
⋮
s[13]

P[ ] ⇒ Parray (consists of Hexadecimal values)

P[0] = P[0] XOR s[0]

P[1] = P[1] XOR s[1]

P[2] = P[2] XOR s[2]

⋮

P[13] = P[13] XOR s[13]

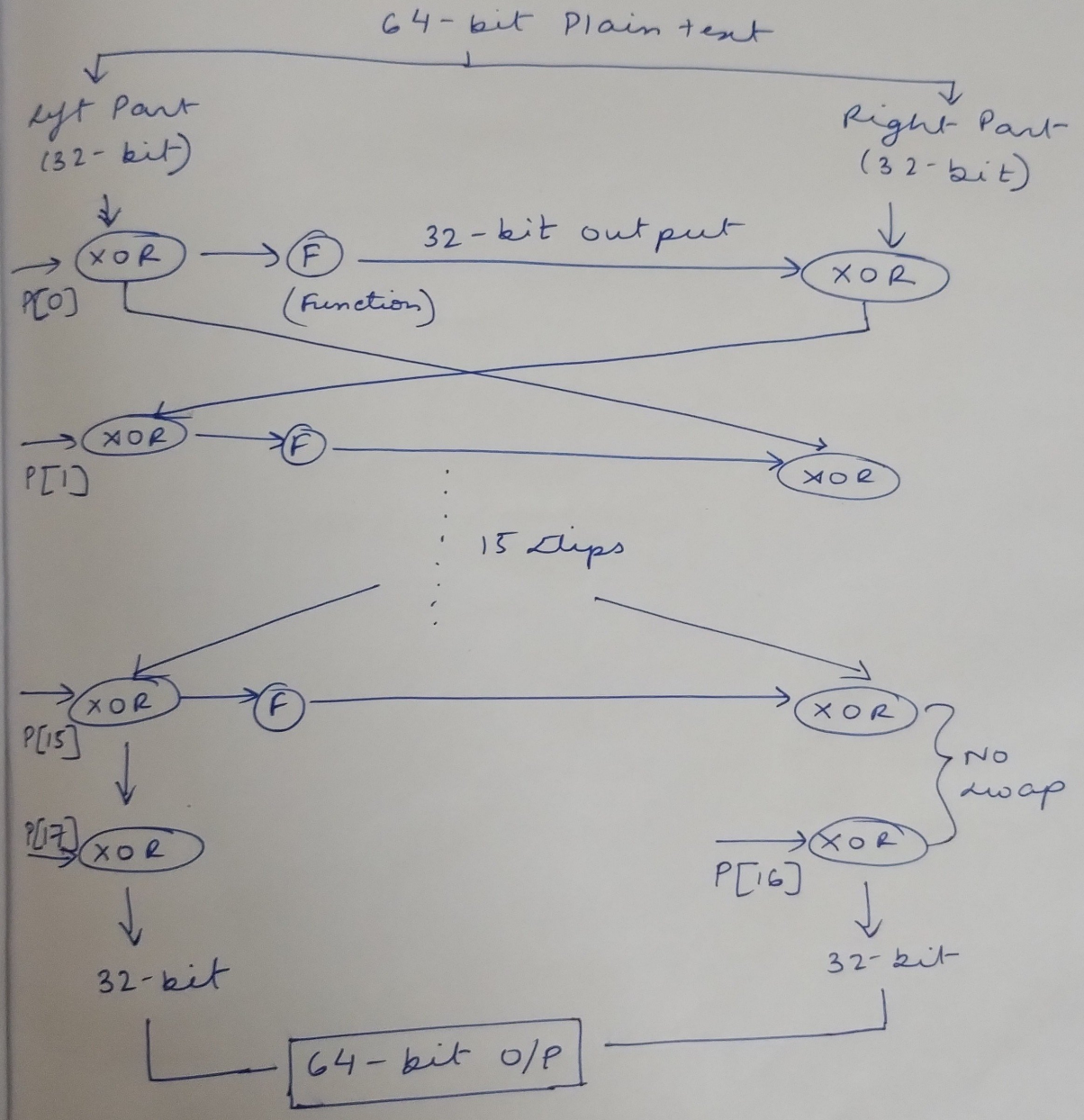
P[14] = P[14] XOR s[14]

P[15] = P[15] XOR s[1]

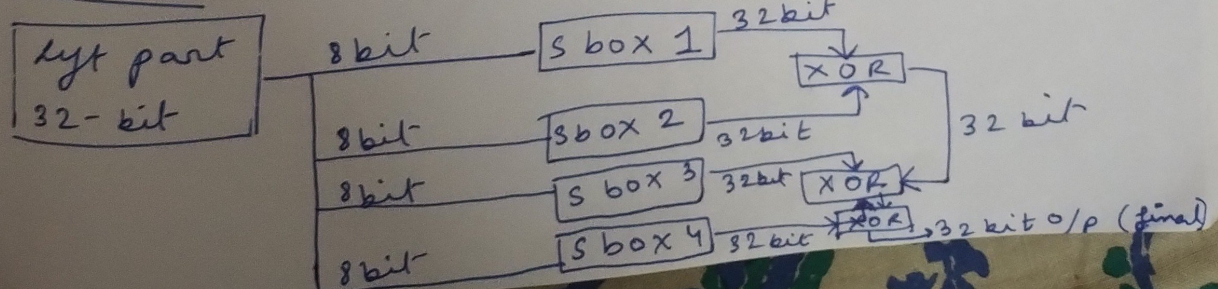
P[16] = P[16] XOR s[2]

P[17] = P[17] XOR s[3]

The sub keys cannot be used directly in the algo. They need to be modified with the help of ~~Poor~~ P array.



Function F



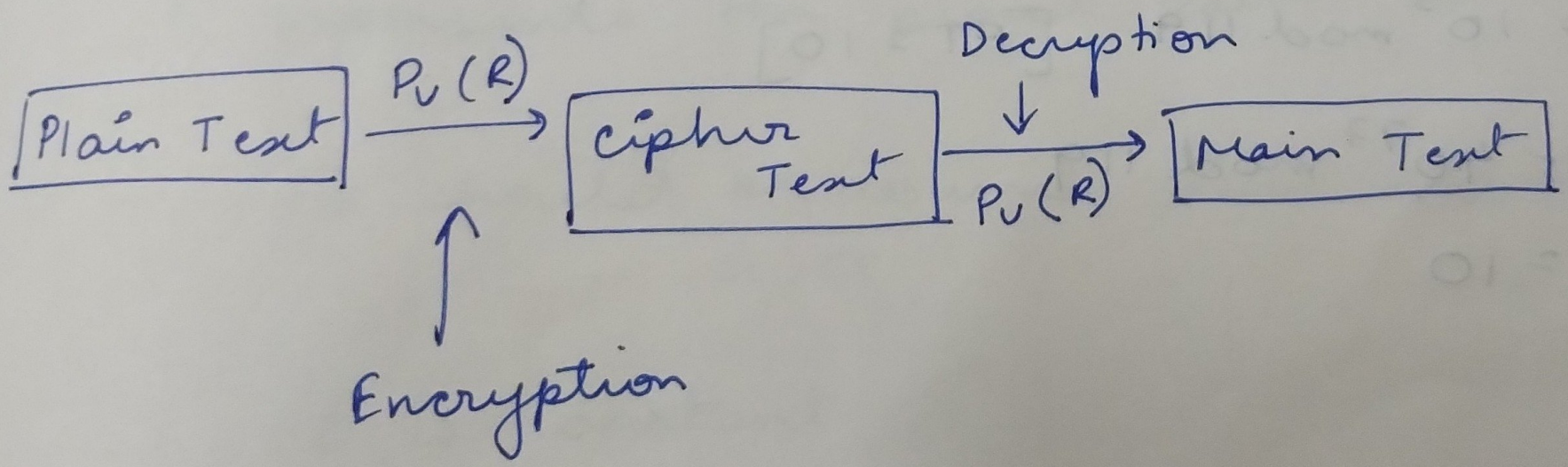
Cryptography

18/2/5

Public Key Cryptography

Private Key → Decryption Key

Public Key → Encryption Key



RSA Algorithm :— [Rivest Shamir Algo]

1. choose 2 prime no. p, q
2. Calculate, $N = p \times q$
3. Calculate public key (Encryption key), E in such a way that the key is not any factors of $\boxed{(p-1) * (q-1)}$
4. Calculate private key (Decryption key), D is which satisfies the following condn.

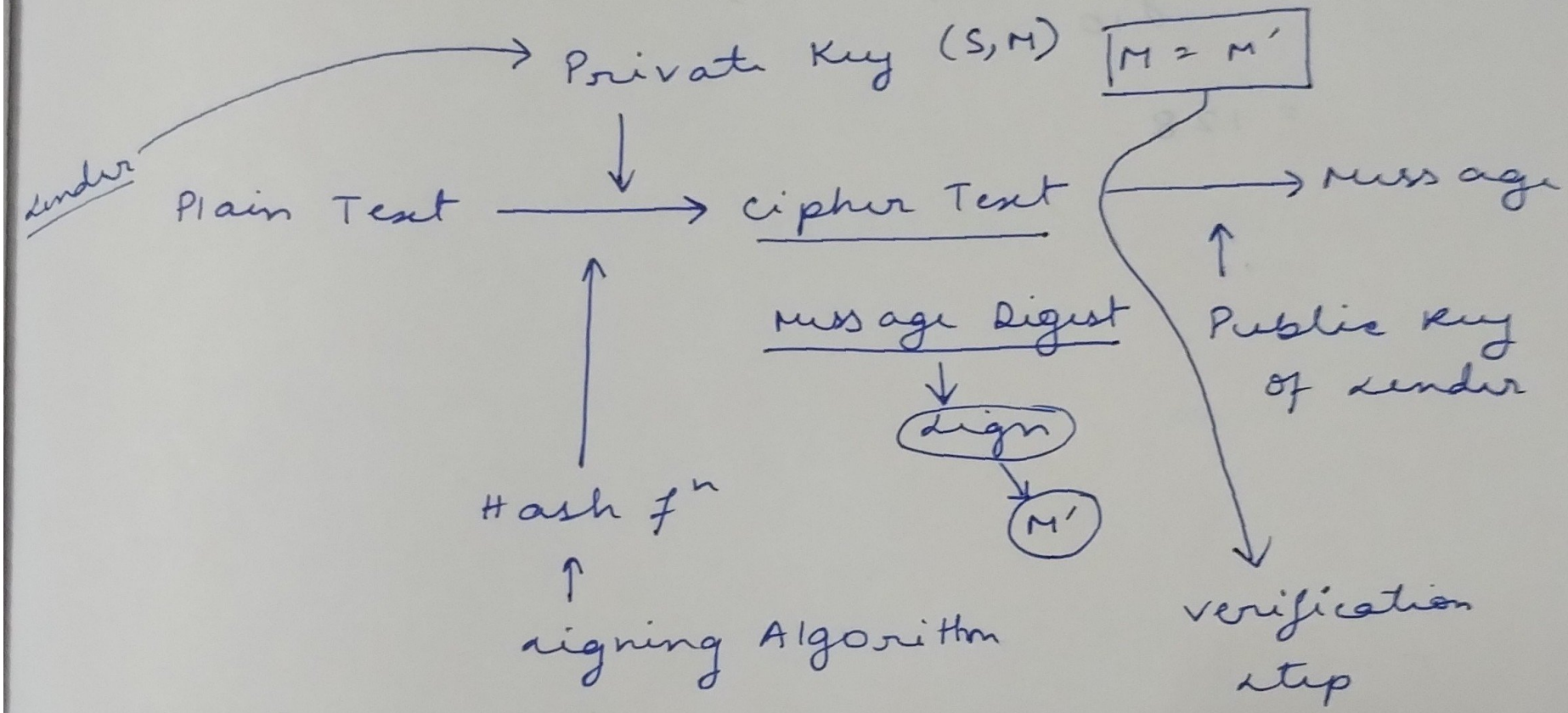
   $(D * E) \bmod (p-1) * (q-1) = 1$
5. For encryption, $CT = PT^E \bmod [N]$
6. For decryption, $PT = CT^D \bmod n$

Eg:-

1. $P = 7 \qquad q = 17$
2. $N = 7 \times 17 = 119$
3. E, $6 \times 16 = 96 \longrightarrow (2, 3)$
   ↳ 5 (suppose)
4. $(D * 5) \bmod 96 = 1$
   ↓
   77
5. $CT = 10^5 \bmod 119 \quad [PT = 10]$
6. $PT = 40^{77} \bmod 119$
   $= 10$

Imp

Digital Signature :-



1, 2, 3, 4 → same as R E A Algorithm

5. Encryption, $S = M^D \bmod n$

6. Decryption, $M = S^E \bmod n$.

Cryptography 19/2/2

1. Convert the following Plain text into Cipher Text using ceasar cipher where Key = 4,

   Plain text = STUDENTS DULP. PROG

2. Encrypte the following text using double columnar transpodition method.

   Plain text : ARTIFICIAL INTELLIGENCE WORKSHOP.

   Key : 42513

3. Encrypt the below mentioned plain text using Play fair cipher.

   Plain text : STUDENTS ARE PLAYING FOOTB

   Key : LEAGUE

1. Plain Text = STUDENT DVLP PROGR

W X Y H I R X I H Z P T S V S K

Key = 4

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

$e(s) = (19 + 4) \bmod 26 = W(23)$

3. Plain Text: STUDENTS ARE PLAYING FOOTBALL

Key: LEAGUE

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

STUD ENTS ARE PLAY ING FOOT BALL

TPAH GKPT DXLQ EGVN SFHN

OT BA LX XL

TZ DL AV VA

Cipher Text: TPAHGKPTDXLQ ~~EGVN~~ EØ VNSFHN

TZ DL ~~A~~V VA

2. Plain text: ARTIFICIAL INTELLIGENCE WORKSHOP

Key: 42513

4	2	5	1	3
A	R	T	I	F
I	C	I	A	L
I	N	T	E	L
L	I	G	E	N
C	E	W	O	R
K	S	H	O	P

ciphur Text :- IAEEOORCNIESFLLNRP

AIILCKTITGWH

4	2	5	1	3
I	A	E	E	O
O	R	C	N	I
E	S	F	L	L
N	R	P	A	I
L	C	K	T	I
T	G	W	H	

ENLAKWA RSLTOILITHIOENII ECFP
G