CNS

26/8/22

Eg Cryptography –

(i) Plain text – It is denoted by (P)

(ii) Encription Algorithm –
(iii) Secret key
(iv) Cipher text
(v) Decryption algorithm

(1) plain text – This is the original interiegable messge of data that is fate into the algorithm as input.

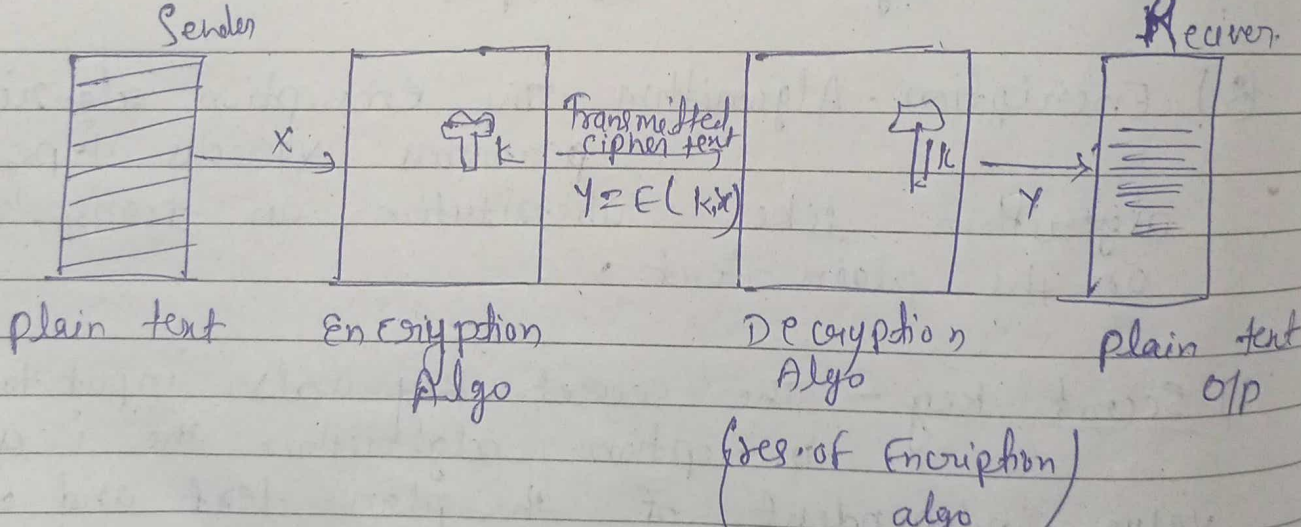
(2) Encription Algorithm – The encription algorithm performs various type of algorithm like substitution an transpotation on the plain text.

(3) Secret key – The secret key is also input to the increption algorithm the is a value independent of the plan text and of the algorithm the algorithm will produce a different output depending on the specific key be used at that time.

(4) Cipher text - This cipher text is the scrambled message produce as output. It depends on the plain text and secret key.

(5) Decryption Algorithm - This is essentially the inception algorithm run in reverse from it text the cyfer text and secret key and produce the original massage.

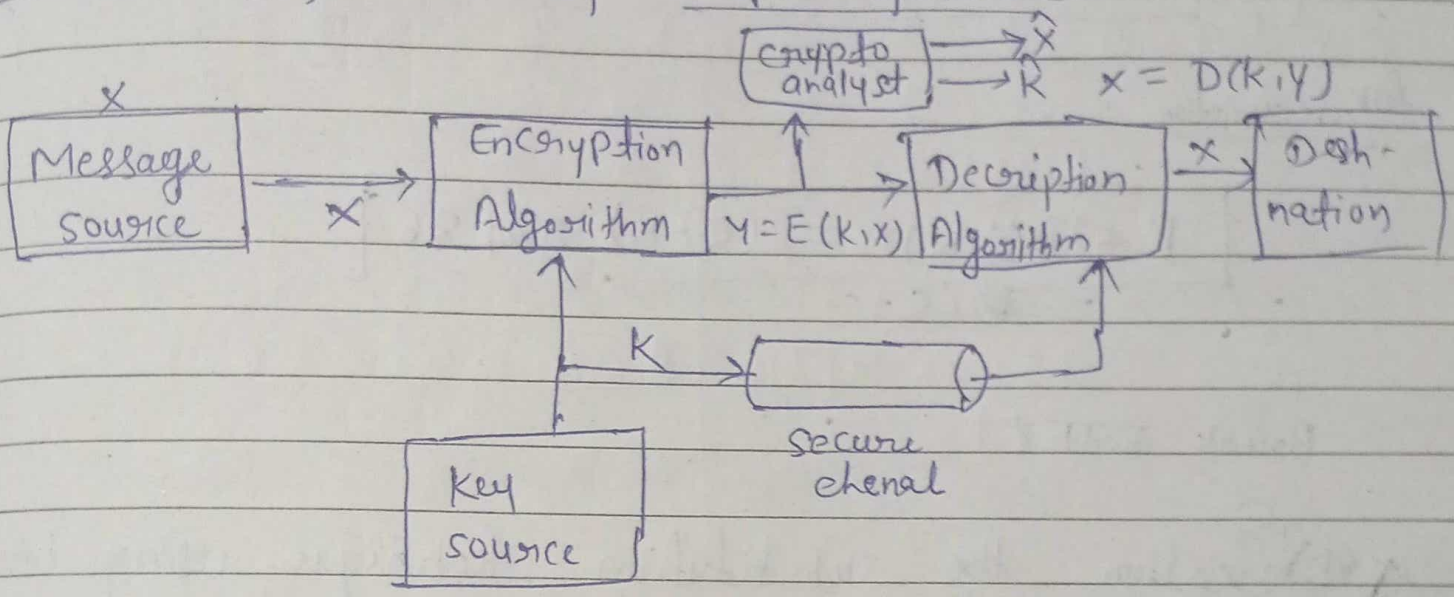
* Simplified model of Symmetric Encription



CNS

Date 27/8/22

Model of Symmetric ~~Key~~ Cripto-System :—



* Cripto analysis and ~~B~~rout-force attack

Date - 29/8/22

~~Substitution algorithm~~ - CNS

1) Substitution Techanique. —

(i) Ceaser Cipher

plain text : meet me after the toga party.

SDYWB

Cphar : PHHW PH DTWHU WKH WRJD

g_0, b_1, c_2 ---- z_{25}

$C = E(P, B_K)$ $C = E(P, K)$

$C = E(P, 3)$

$= (P + 3) \bmod 26$

encription

$$C = E(P,K) = (P+K) \text{ Mod } 26$$

for decription

$$P = D(C,K) = (C-K) \text{ mod } 26$$

$= D(C =$

Breaks करता है

Explain the substitution technique using inreption and decription method

Explain with suitable example

★ What are the three Important charchastic problem inable as to use a Brood force cripto analysis

(1) The inreiption and decription are knowe
(2) There are only 25 keys too thy
(3) The language of compt plain text is known and easily reconizable.

CNS

21/9/22

Mono alphabetic Cipher

Permutation

$n = n(n-1)$

$S(a,b,c) = 3(3-1)(3-2)$

$= 6$

$= (a,c,b)(b,a,c),(b,c,a),(c,a,b)$

(c,b,a)

4×10^{26} possible keys

* play for cipher

arrange it matrix from row and column

MONARCHY MCELUOH

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

* Transposition Technique.

* Meet me after toga Party

Me ma

et e

\\\\ original message

key: 2,3,4,5,6,7

28/4 = 7

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	D	A	Y	S	Z

railfence technique.

Cipher ttnD apta tsvo·aodw coiyknls petz

	1	2	3	4	5	6	7
	t	a	t	a	c	k	p
	t	p	s	o	o	n	e
	n	t	u	d	i	l	t
	D	A	o	w	y	s	z

cipher – a o dw

Q. Explain the transposition tech using suitable example.

tranposition techenique is a different kind of techenique by perform in sum short of permutation on the plain text cipher

This type of such cipher is known as rail fence Cipher and such technique is called as rail fence transposition techanique.

* Possible type of attack
~~1) cipher~~

Type of attack	Known to cryptoanalysis
1) cipher text only	* Encypher Algo * Cipher text

CNS

Date - 6/9/2022

* Type of attack -

type of attack	Known to crypto anyst
1) Cypher text only	- Encryption Algo - Cipher text
ii) known plan text	- Encryption Algo - Cipher text - one or more plain text - Cipher text pair formed with the secret key (
iii) choosen plain text	- plain text mesg choosen crypto anlysis together with ads . Carrorponden cipher text generated with

the secretely :

4) Choosen cipher text

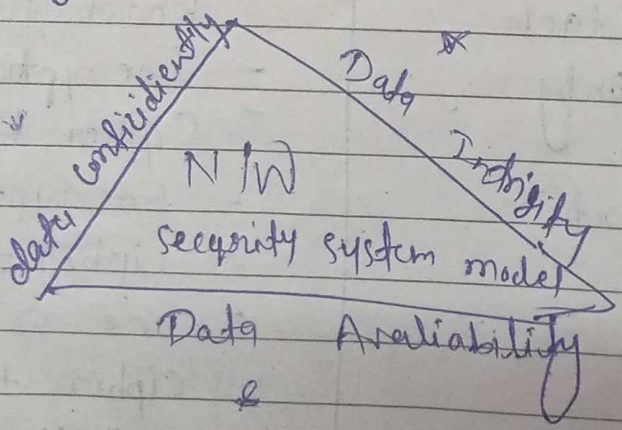
5) Choosen text

features N/w security — (i) Data Confidentiality

* 1) Confidentilely
  2) Privacy

(ii) Data Integrity

the security triode



Authonticity

Accountbelity.

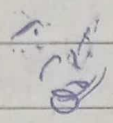
CNS

7/9/22

* The challenges of Computer Security

OSI Security

* Security attack –
(i) Passive attack
(ii) Active attack



CNS

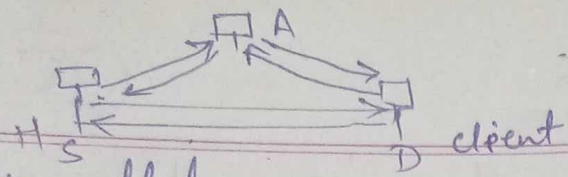
9/9/22

* OSI security Architecture –

This is
(i) Security attack – An action
(ii) Security Mechanism – A Process
(iii) Security service – Now process is implemented to enchanes the security of system.

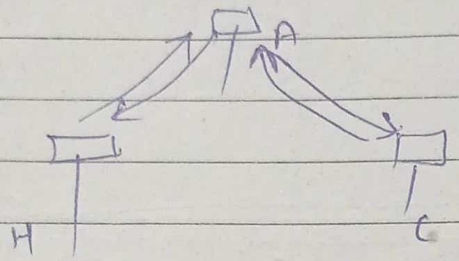
① Securidy attack –

Now there are two type of security Attack –
① Passive attack – नहीं करती है
② active attack. – directly stystem पे attack करती है

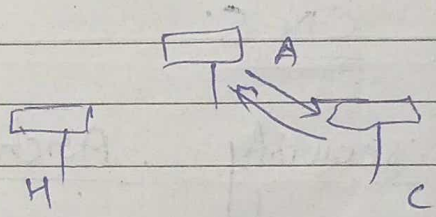


② Active attack –

1) Masquienade : –
2) Replay –
3) Modification of message.



4) Denial of Service
मना उड़ा



* Security Services –

There are 5 types of security ~~sun~~ services.

① autocation — ① Recr Reantity ② Data orgen autocat
② access control
③ Data confidencirity
④ data indigrity
⑤ ~~Reason~~ Non repediation

Authentication –

① Peer Entity Authendication

② Data origen authentication

③ Access control – the prievension of anautherise use of resource.

④ Data Confidencinity
(i) Corection conficidencinity
(ii) Conection less conficidencinity
(iii) selective field confiidencinity
(iv) traffic flow conficidencnity

⑤ data intigrity –
i) conection intigrity with recovery
ii) conection intigrity without recovery
iii) sectione field conection intigrity
iv) conection less intigrity
v) seclective field conection less intigrity

⑥
i) Non repeduction origen
ii) Non repeduction destination

13/9/22

CNS

* Security Mechanism -

specific Security Mechanism | Pervasive Security Mechanism

i) Enciphirment -

The use of mechanitical algorithm to transform data into a from that is not readily intelligable

ii) digitle signature - data upendent to are a cripto. grupy tranformation of data unit that allows a recipent of the data unit to prove the source and intigrity of the data unit.

(iii) Accessed control -

The varity of machanism that inforce exess right to resource.

(iv) data intrigity - The varity of mechanism is used for data intigrity.

(v) authetication exchange -
a mechanism a source the Identity of entity by means of information exchange.

(vi) Rounting Controll -

Traffice Padding
insert dummy

(vii) Notarigation - The uses of trusted third Party to ensure certain properties of data exchange.

*Pervasive security Machanism -

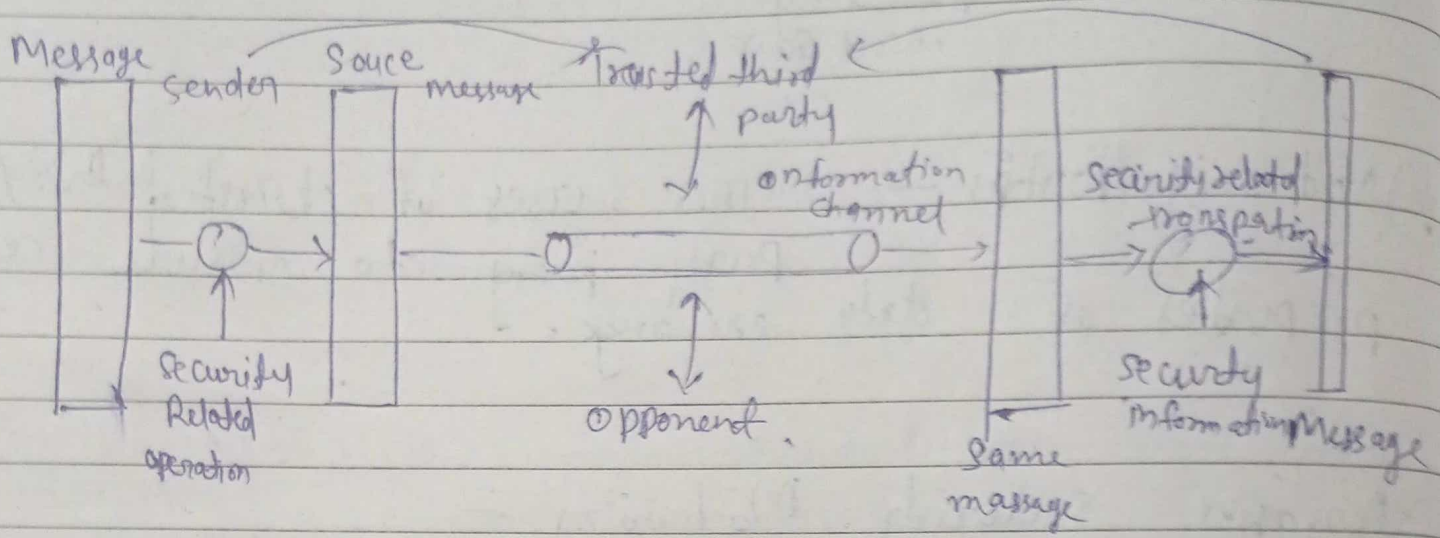
① Trusted functionality -
② Security level -
The marking bound a two resources that names of, desiged set of security attributes of dead resource.

③ Security audit -

④ Security recovery -

Imp Explain the OSI Security architecture.

* A model for N/W security.



CNS

Unit - 2

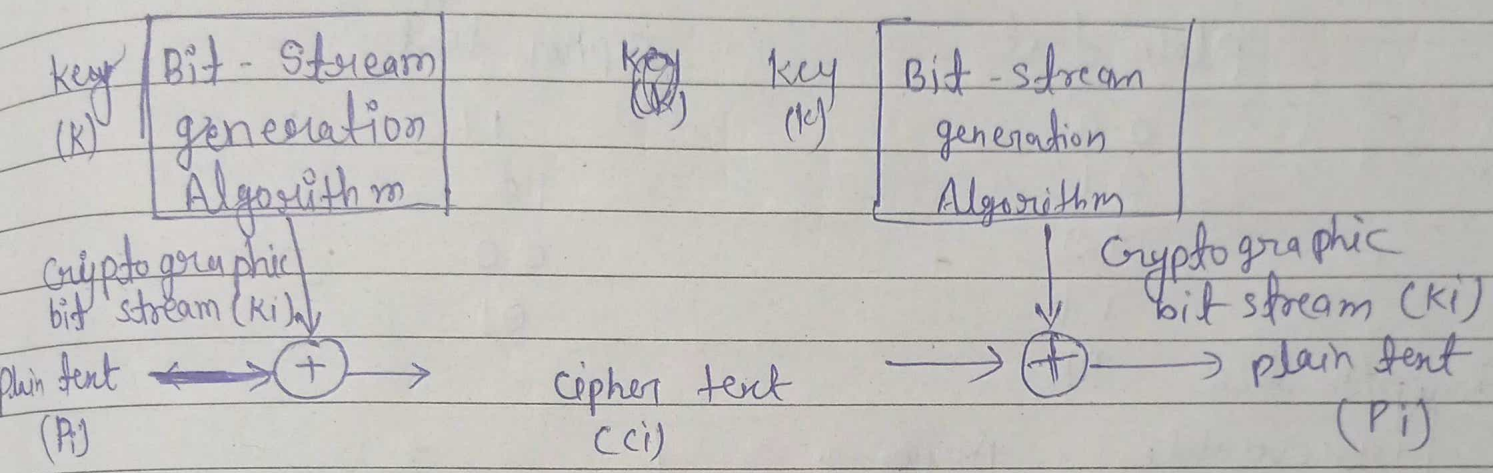
~~Date~~ - 14/9/22

~~Stream~~ Cipher

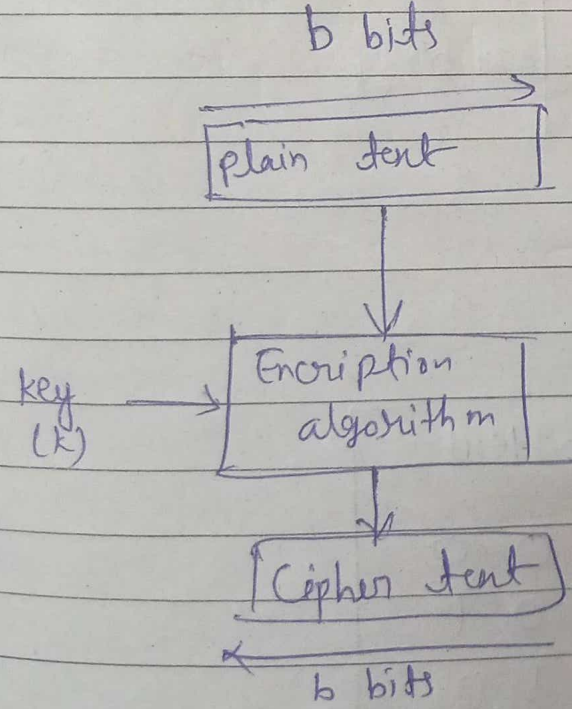
CNS Unit-2

14/9/22

Stream Cipher
Block Cipher



(a) Stream Cipher using algorithm bit - stream generator



(b) Block cipher

n bits no. of block

2^n

$n = 2 \quad 2^2 = 4$

reversable mapping

plain text	cipher text
0 0	1 1
0 1	1 0
1 0	0 0
1 1	0 1

2^n

$n!$

Encription table

irreversable mapping	
plain text	cipher text
0 0	1 1
0 1	1 0
1 0	0 1
1 1	0 1

$2^n - 1$

Decription table –

Cipher text	Plain text
1 1	0 0
1 0	0 1
0 1	1 0
0 1	1 1

CNS

2x2x2x2 Date 19/9/22 Page

4-bit block cipher :- (Encryption side)

plain text (I/P)	cipher text
0000	1010
0001	0110
⋮	⋮
1111	0000

Decryption table :-

Cipher text (I/P)	Plain text
1010	0000
0110	0001
⋮	⋮
0000	1111

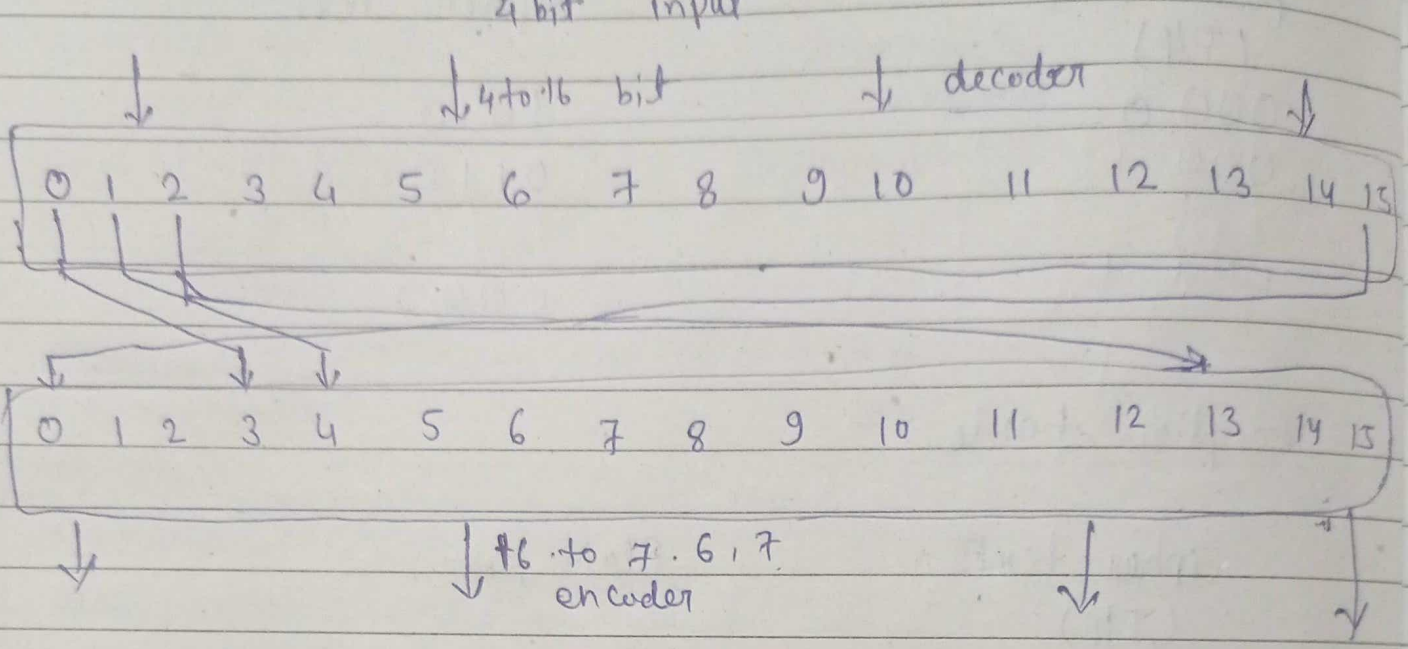
key = $n \times 2^n$

$= 4 \times 2^4 = 64$ bits

for n^{26}

$= 64 \times 2^{64} = 10^{21}$ bits.

Hardware Model (ideal block cipher):—
for encryption –



mapping in linear equations –

$$y_1 = k_{11}x_1 + k_{12}x_2 + k_{13}x_3 + k_{14}x_4$$

$$y_2 = k_{21}x_1 + k_{22}x_2 + k_{23}x_3 + k_{24}x_4$$

$$y_3 = k_{31}x_1 + k_{32}x_2 + k_{33}x_3 + k_{34}x_4$$

$$y_4 = k_{41}x_1 + k_{42}x_2 + k_{43}x_3 + k_{44}x_4$$

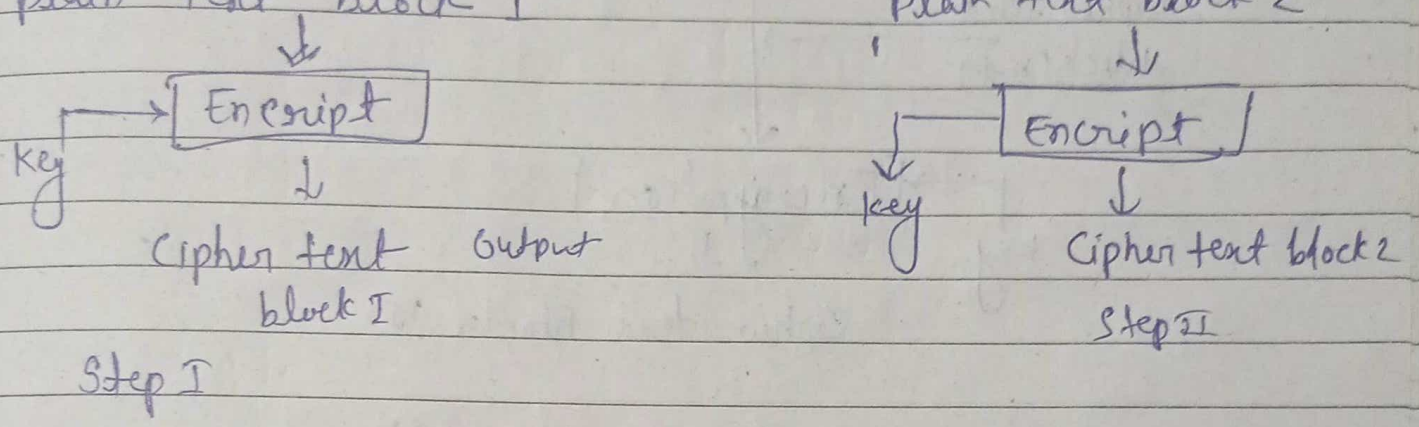
where x_i are the 4 binary digits of the plain text block while y_i are the 4 binary digits of the cipher text & k_{ij} are the binary coefficients

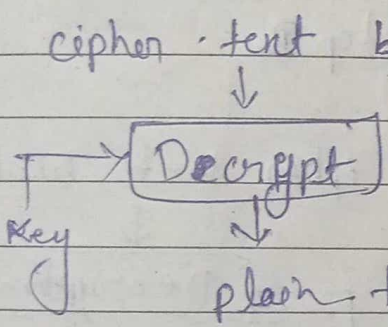
CNS

Date 20/9/22

* Algorithm Modes (Block Cipher)

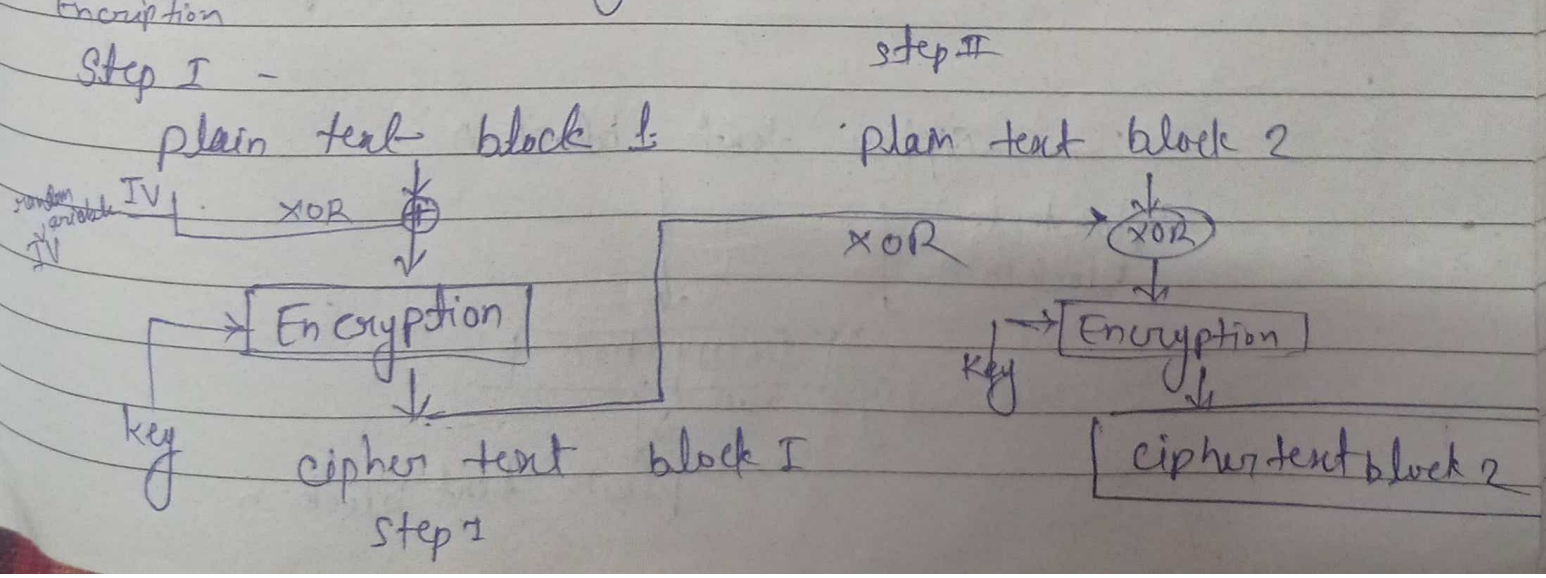
i) Electronic Code block (ECB)



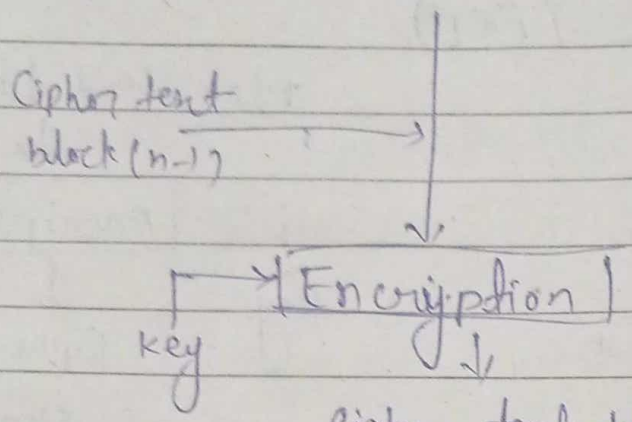


ii) Cipher block chaining Mode :-

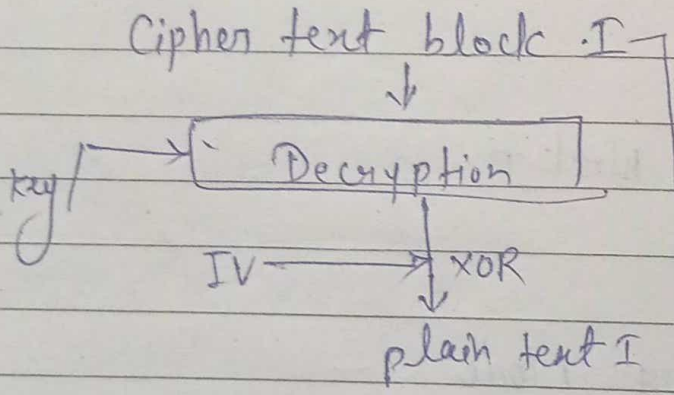
Encription



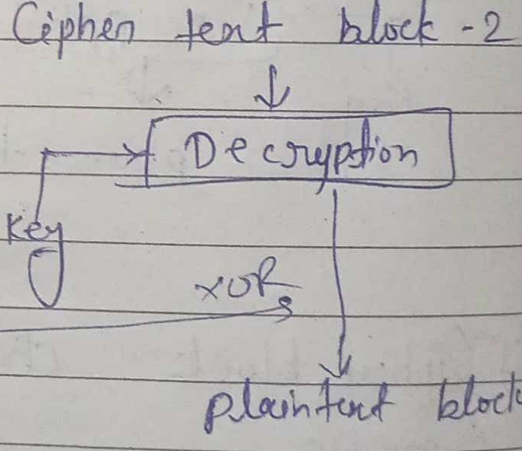
Step III -

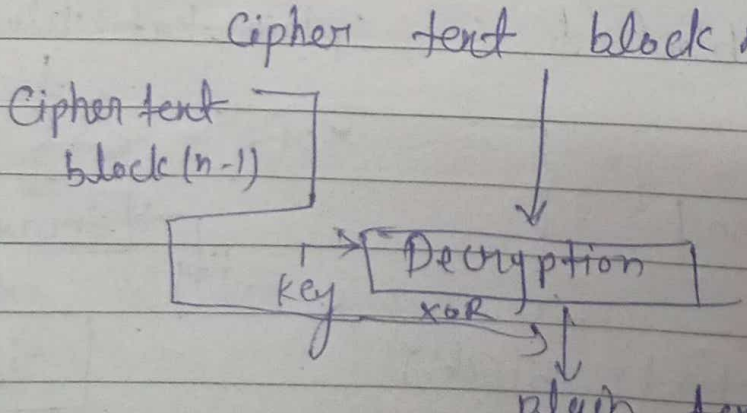


Decryption Step I

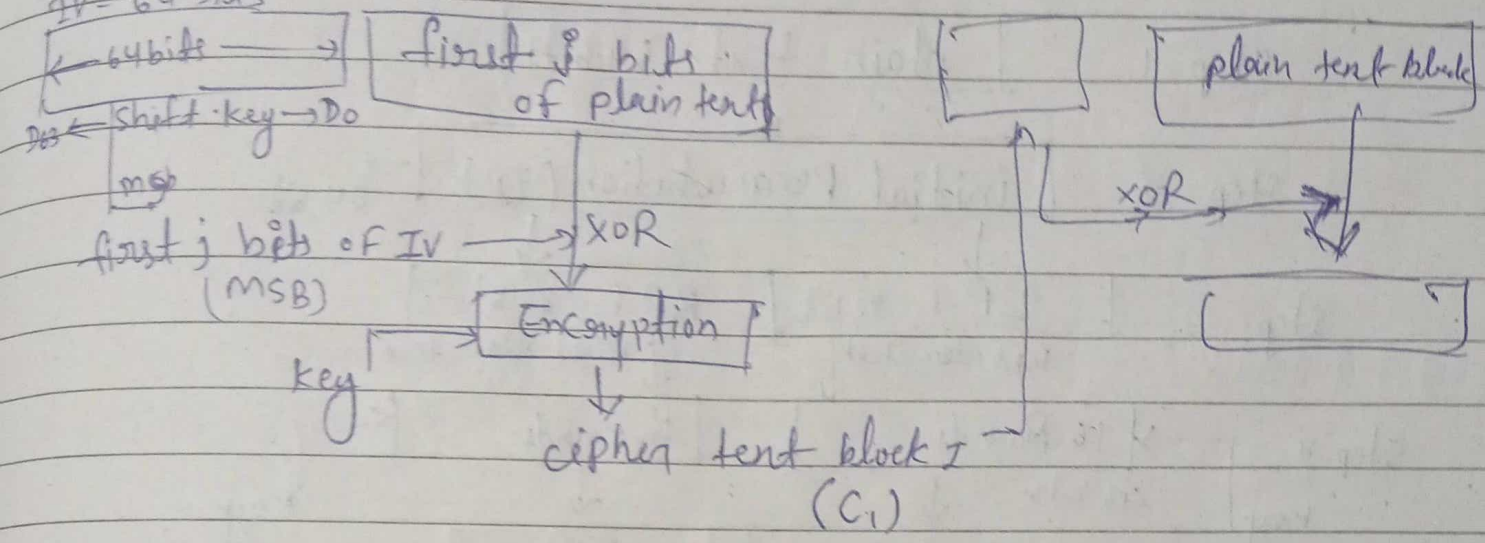


Step II





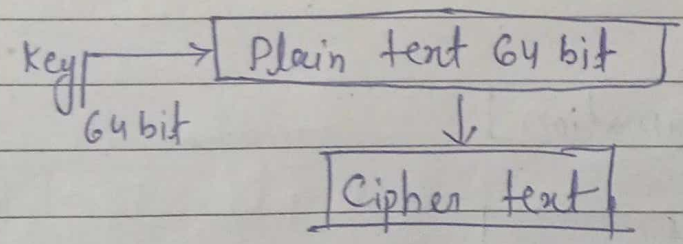
3) Cipher feed block mode (CFB)



CNS

Date - 21/9/22

DES (Data Encryption standard)



key size 64 bit

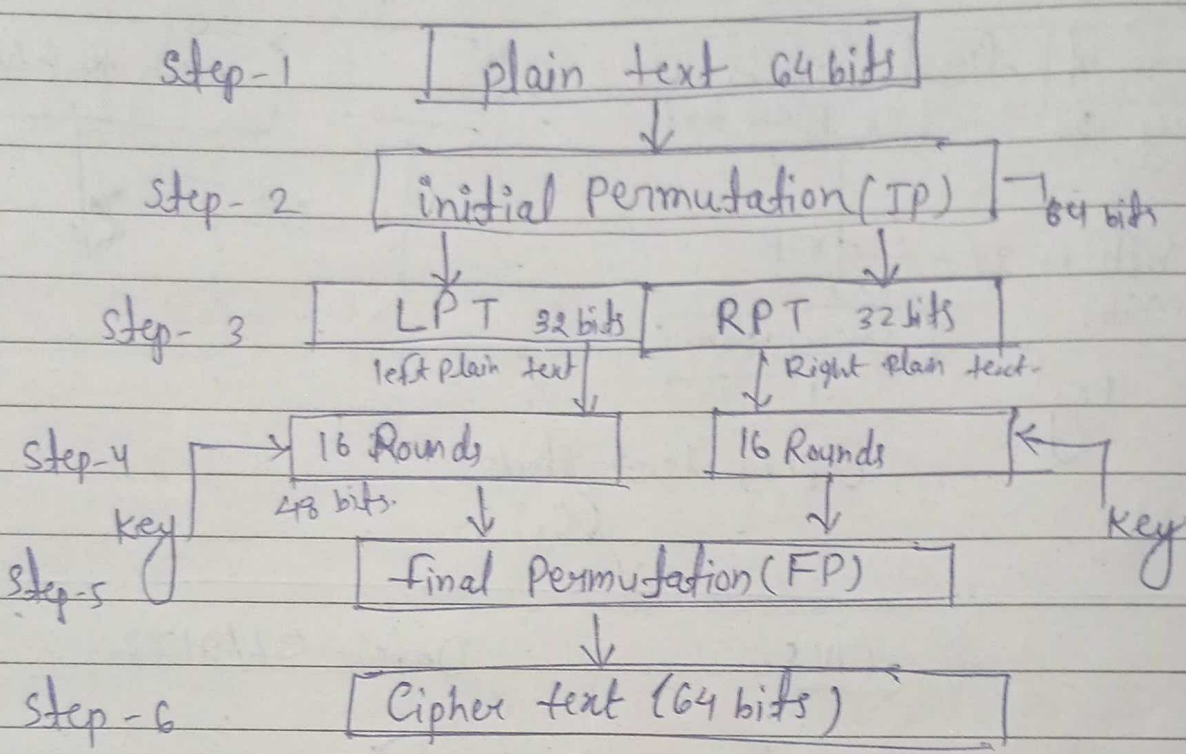
↓

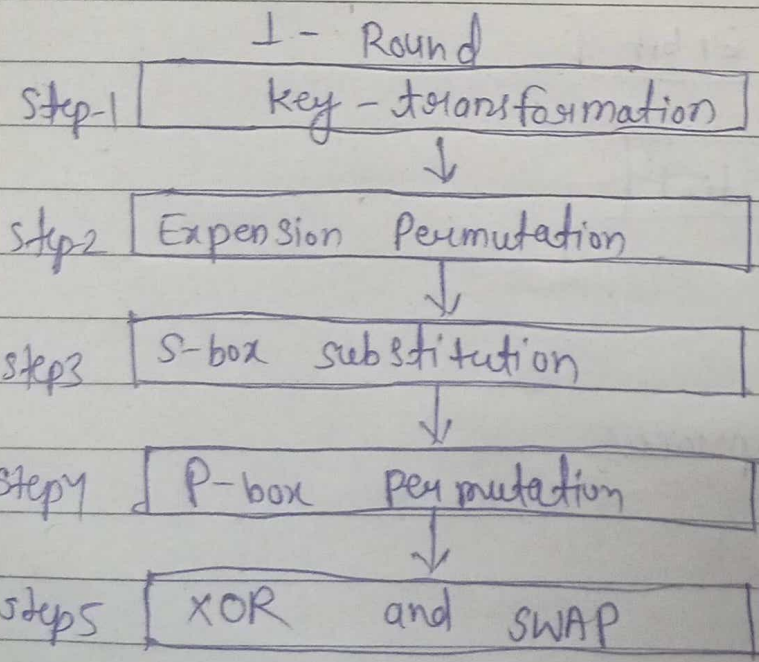
key discarding process

↓

key 56 bits

Algorithm of

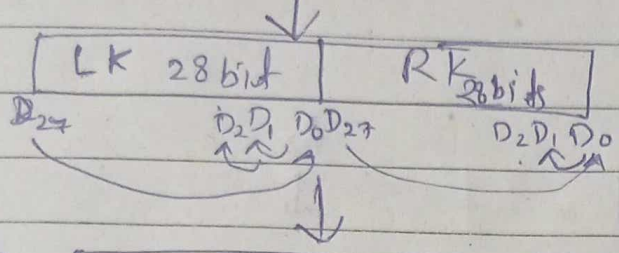




original - key (64 bits)

↓ Key discarding process

56 bit key



1-2-9-16

24

key - 56 bit

↓

48 bits key

↓

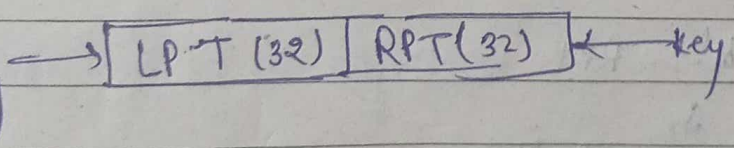
Compressed Permutation

CNS

22/09/22

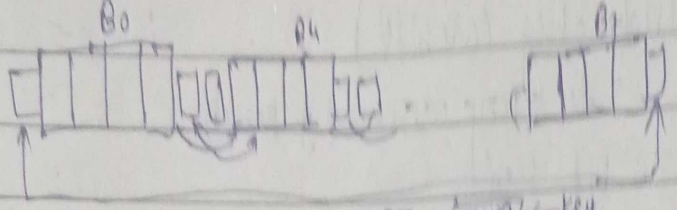
(2) Expression permutation

(plain text)



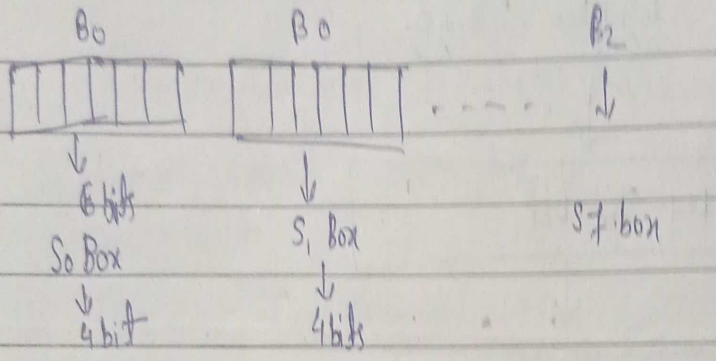
for RPT

divide it into 8 blocks of 4 bit each then convert it into 6 bits to convert RPT 32 bits → RPT 48 bits then XOR key and RPT



RPT → XOR/- key
48 bits RPT

(3) S-box Substitution



Si Box will convert 6 bits again into 4 bits.
i = 0, 1, 2, ... 7
again we will get RPT of 32 bits.

(4) P-bbs substitution -

simple permutation

32-bits RPT

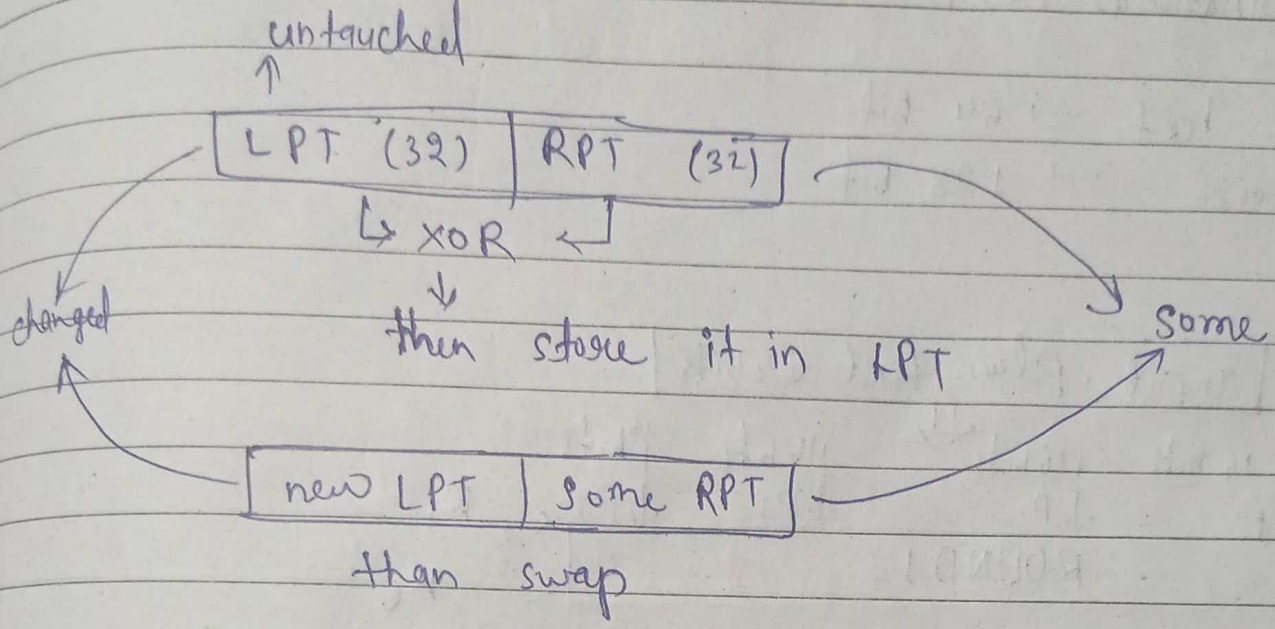
↓

permutation

↓

32-bit RPT

(5) XOR and swap (only change in LPT)



lpt	rpt	64 bits

lpt = RPT

rpt = LPT

final permutation

↓

Permutation

↓

Cipher text (64 bit)

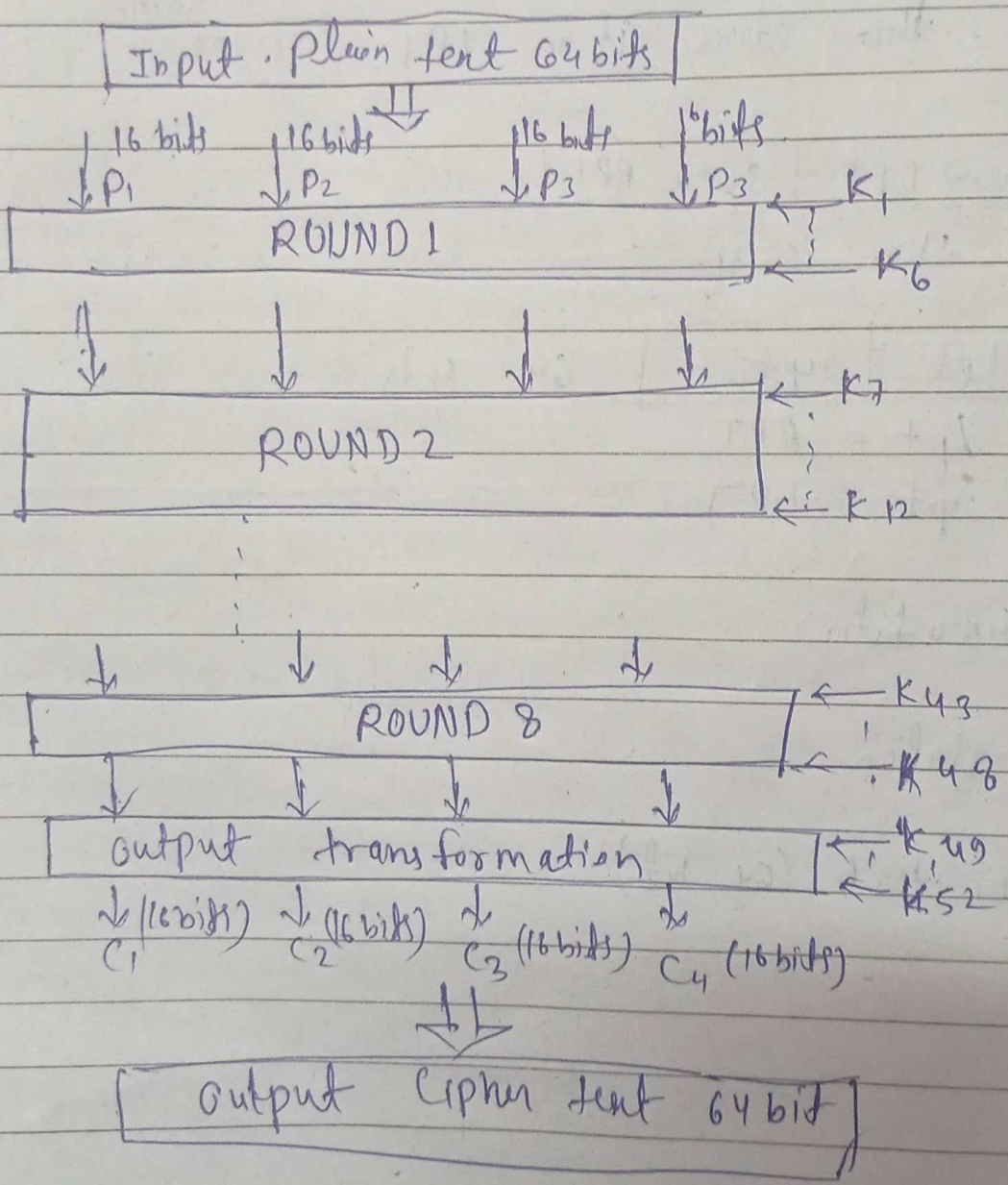
23/9/22

CNS

IDEA Algorithm :-

international Data

* plain text → 64 bit
* key size → 128 bit



step 1 - multiply P_1 and K_1

step 2 - add P_2 and K_2.

step 3 - add P_3 and K_3

step 4 - multiply P_4 and K_4

step 5 - XOR the result of step 1 and step 3

step 6 - XOR the result of step 2 and step 4.

step 7 - multiply the result of step 5 with K_5

step 8 - add the result of step 6 and step 7.

step 9 - multiply the result of step 8 with K_6.

step 10 - add the result of step 7 and step 9.

step 11 - XOR the result of step 1 and step 9.

step 12 - XOR the result of step 3 and step 9.

step 13 - XOR the result of step 2 and step 10

step 14 - XOR the result of step 4 and step 10

for Output transformation -

step 1 - multiply R_1 & K_1.

step 2 - add R_2 & K_2.

step 3 - add R_3 & K_3.

step 4 - multiply R_4 & K_4.

Q: what is the strength of IDEA ?

what is the strength of IDEA -
→ Size of key (i.e. 128 bits difficult to break so it is more powerful compare to DES)

Date - 24/9/22

RC4 (Rivest Cipher 4)

RC4 generates a pseudorandom stream of bits called keystream. This is combined with the plain text using XOR for encryption. Even decryption is performed in a similar manner.

There is a variable length key consisting of 1 to ~~12~~ ~~15~~ 256 bytes (or 8 to 2048 bits). This key is used to initialize a 256-byte state vector with elements identified as S[0], S[1], ---, S[255]. To perform an encryption or decryption operation one of these 256 bytes of S is selected, and processed. We will call the resulting output as k. After this, the entries in S are permuted once again.

overall, there are two processes involved:
(a) initialization of S, and
(b) stream generation.

CNS

26/9/22

RC5 -

basic principle -

1. The plain text box size can be of 32 bit, 64 bit or 128 bit (since 2-word block is used)

2. The key length can be of 0 to 2040 bits.

3. No. of Rounds (0-255)

RC5 = w/r/b

where w = word size
r = no. of rounds
b = no. of (8-bits) in the key.

RC5 = 32/12/16
= Block size 64 bits
no. of Rounds = 12

= key size = 128

RC6 = 32/12/16

~~Divide~~

RC5 Imp

S_0, S_1, S_2 = sub zero

Divide the plain text into two equal block A & B

Add A & S[0] = C

B & S[0] = D

Start in i = 1

1. XOR C & D = E

2. Circular left sift E by D bits

3. Add E & S[2] = F

4. XOR D & E = G

5. Circular left G by f bits

6. Add G & S[2i+1] to produce H

Increment i by 1

check if i > r

yes

call fun C

Call Fun D

Stop

D = 16 circular right shift

E = D1 ... D16

Left significant bit

Most significant bit

CNS

28/9/22

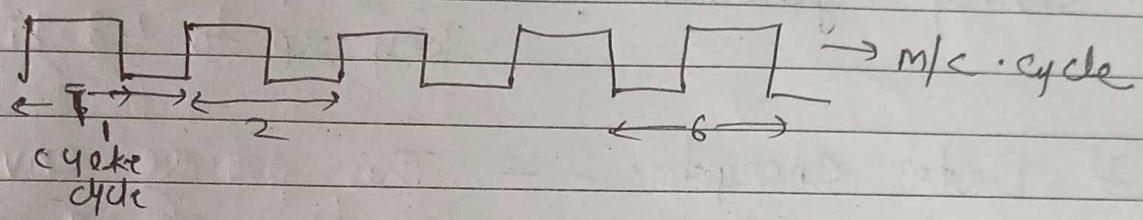
✱ Blowfish Encryption Algorithm

Developed by Bruce Schnier

Encription feature of low fish algorithm

① fast

Blowfish encryption rate on 32 bits microprocs is 26 clock cycle per bit.



② Compact - blowfish can exicute in less then 5 kb of memory.

③ Simple - blowfish uses only primitive operation such as addition, XOR and table lookup, making its design and implimentation simple

④ ~~imp~~ Secure - blowfish has a variable key length up to an maximum of 448 bits long, making it both flexible and secure.

Working Operations –

Blowfish incripte 64 bit block with a variable length key. It consiste of two parts as follows –

① subkey generation
② data Encryption

① subkey generation – This process convert the key up to 48 bits

② Data encription – – This process envoles the iteration of a simple functi 16 times - each round contains a key depepdent permution on key and data depepdent sabustitution.

* Subkey Generation –

(i) Key size – 32 bits to 448 bits
1 word – 2 bytes
16 bits – 2 word

$K_1, K_2 - , K_3 - - K_4$

where $n = \leq 14$

448/32 =

(ii) Concept of P-array which consists of 18, 32 bit subkey $P_1, P_2 \ldots P_{18}$

(iii) four S-boxes, each containing 256, 32 bit entries

$S_{1,0}, S_{1,1} \ldots S_{1,255}$

$S_{4,0}, S_{4,1} \ldots S_{4,255}$

CNS

Date - 29/9/22

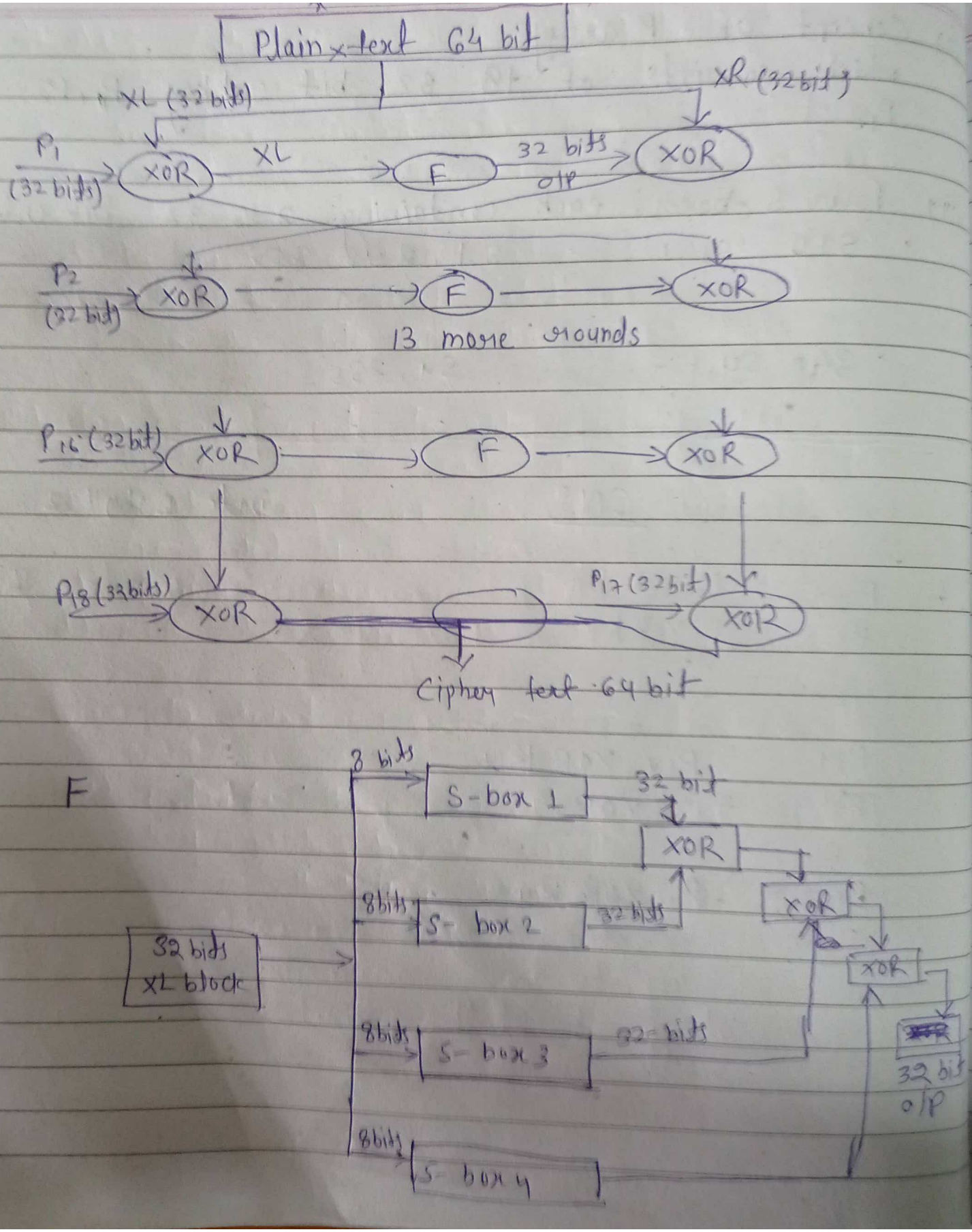
(iv) $P_1 = P \text{ XOR } K_1$

$P_2 = P \text{ XOR } K_2$

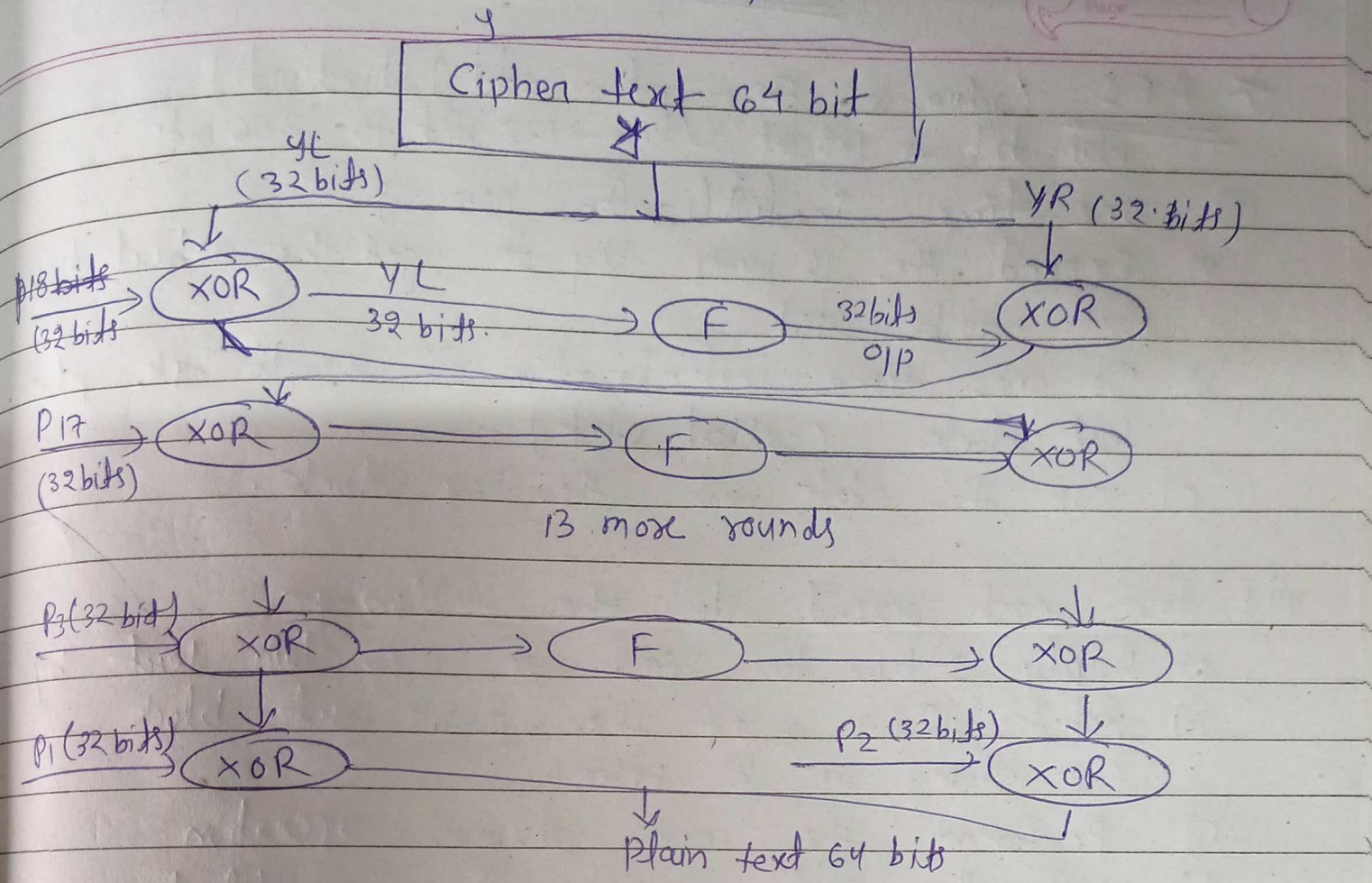
$P_{14} = P_{14} \text{ XOR } K_{14}$

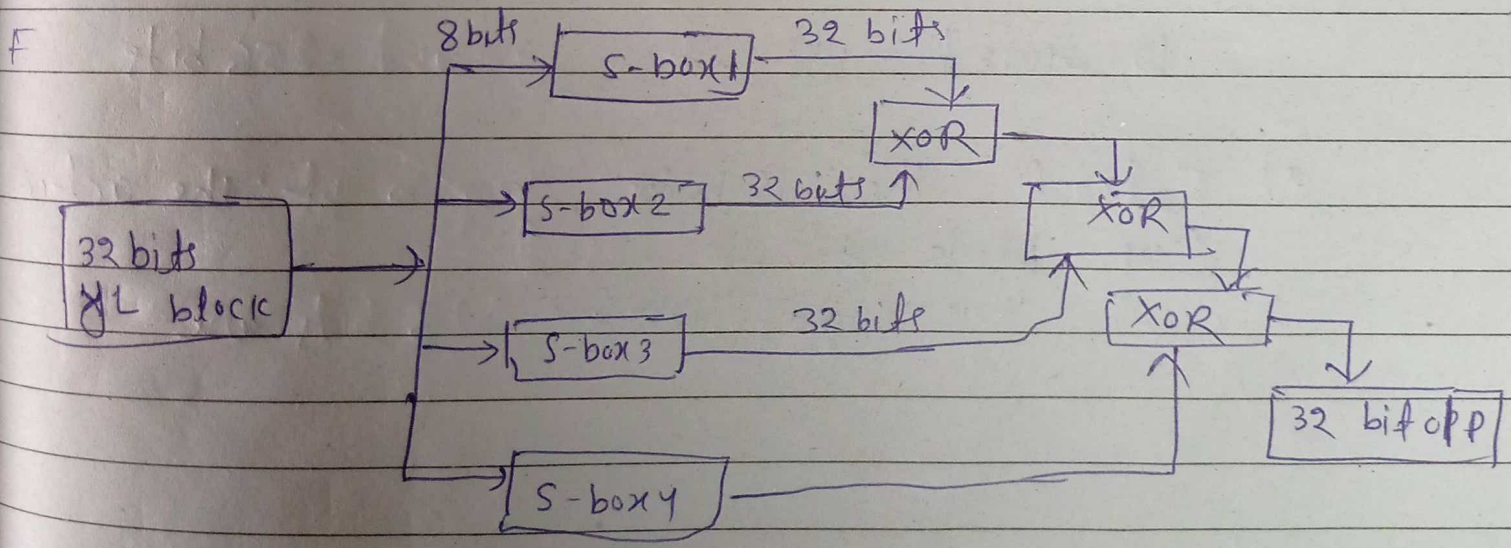
$P_{15} = P_{15} \text{ XOR } P_1$

$P_{18} = P_{18} \text{ XOR } R_4$


Plain text 64 bit
XL (32 bits)
XR (32 bit)
P1 (32 bits)
XOR
XL
F
32 bits o/p
XOR
P2 (32 bit)
XOR
F
XOR
13 more rounds
P16 (32 bit)
XOR
F
XOR
P18 (32 bits)
XOR
P17 (32 bit)
XOR
Cipher text 64 bit
F
32 bits XL block
8 bits
S-box 1
32 bit
XOR
8bits
S- box 2
32 bits
XOR
XOR
8bits
S- box 3
32 bits
32 bit o/p
8bits
S- box 4

Blowfish ~~Encription~~ Decryption Algorithm





CNS

20/9/22

* AES (Advance Encryption ~~std~~ standard)
Plain text → 128 bit, key → 128 bit to 256 bits

(i) one time initialization process
a) Expand the 16 bytes key to get the actual key block to be used
b) Do one time initialization of the 16 byte plain text block (called state)
c) XOR the state with the key block.

(ii) for each round do the following
a) Apply S-box to each of the plain text bytes.
b) Rotate Row k of the plain text block (i.e. state) by k bytes.
c) Perform the mix column operation
d) XOR the state with the key block.

10 round - 128 bit 14 Round - 256 bits

a) Extract the 16 bytes key to get the actual key block to be used
↳ 11 array 4×4 = 128 bits are

CNS

11/10/22

Comparision b/w

Characteristic	Symmetric	Asymmetric
key used for encry & decry	Same key is used for ecry & decry	A one key used for encry & another different key is used for decry
Speed of encryp & decryption	very fast	slower
Size of resulting encrypted text	Usually same as or less than original text	more than the original text
Key agreement / Exchange	A big problem	No problem at all
No. of keys required as compare to the no. participants in the message exchange	Equals about the square of the number of participants so scalability is an issue	Same as the no of participants so scalability is not issue
uses	mainly used for encry & decry. cannot used for digital signature and	Can be used for encry & decry as well as for dig signatn

Symmetric key

CNS

8/10/22

P=47 , Q=17

* RSA Algorithm -

1. choose two large Prime nos - P & Q.
2. calcute $N = P \times Q$
3. select the public key जो सबको पता होगा Encryption E, such that it is not a factor of (P-1) & (Q-1)
4. select the prite key D such that the following eqn is true.

$$(D \times E) \bmod (P-1) \times (Q-1) = 1$$

5. for encreption calculate the cipher Text from the plain text as follows $CT = PT^E \bmod N$

6. for decription calcute the plain text (PT) from assume the cipher text (CT) as follows :

$$PT = CT^D \bmod N$$

P=47, Q=17

47-1 47-1

47×17 46×16 = 736

E=3

E=3

$$(D \times 3) \bmod 736 = 1$$

P=7, Q=17

$$(D \times 5) \bmod 96 = 1$$

D=77

$385 \bmod 96 = 1$

modulus

x mod y

x

y

$CT = PT^E \text{ MOD } N$

$= 10^5 \text{ MOD } 119$

$= 100000 \text{ MOD } 119$

$\boxed{CT = 40}$

$PT = CT^D \text{ mod } N$

$\boxed{PT = 10}$

CNS

Date - 10/10/22

* Diffie - Hellman key exchange Algorithm -

Alice Bob

discription of the algorithm

(1) Firstly Alice and Bob agree on two large prime number ~~and~~ n and g. this to integers need not to cape secrate.

(2) Alice choose another large random no. x and calculate A $\boxed{A = g^x \text{ mod } n}$

(3) Alice send this A to Bob

$A \rightarrow$ Bob

(4) Bob ~~or~~ Indipendently choose another large random no. y $B \rightarrow y$

(5) and calculate B in such away.

$\boxed{B = g^y \text{ mod } n}$

5) Bob send this B to Alice. (B no.)

B → Alice

6) Alice now compute the secrete key K_1. (Private key)

$$K1 = B^x \bmod n$$

7) Bob computed

$$K2 = A^x \bmod n$$

Eg: $n = 11$, $g = 7$, we have calculat K_1 and K_2

$x = 3$, $y = 6$

B = ## 1 Lakh 70 thousds

R = 2

Soln

① $n = 11$, $g = 7$

② $A = 7^3 \bmod 11$

$343 \bmod 11 = 2$

③ A → R

④ $B = 7^6 \bmod 11$

$= 117649 \bmod 11$

$B = 4$

$K1 = g$

$K2 = 8 \bmod 11$

★ KNAPSACK Algo —

Pink कलर हुये 1 value
Pick नही किया है तो 0 value देना
last मे cipher text.

S1 Plain text	0	1	1	0	1	1		1	0	0	1	0	1		1	1	0	0	1	1				
S2 knapsack	1	7	8	12	14	20		17	8	12	14	20			17	8	12	14	20					

S3 CT = 7 + 8 + 14 + 20 = 49

1 + 8 + 12 + 20 = 41

1 + 7 + 14 + 20 = 42

Algorithm

$S = b_1 M_1 + b_2 M_2 + b_3 M_3 + \cdots b_n M_n$

$b_4 M_4 + b_5 M_5 + b_6 M_6 + \cdots$

$S_1 = 0 + 1 \times 7 + 1 \times 8 \cdots +$

CNS

Date 4/11/22

Unit - 3

Digital Signature.

Message digest

* It is used to identify the authentiuity of sender. that prove the source of msg in authentic.

Two types of Hash function or Message Digest

① LRC method [Longitudinal Redundancy check]

ex. suppose original message is

1st row 01101101 2nd row 11110000 3rd row 01101100 4th row 11001100

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
0	1	1	0	1	1	0	1
1	1	1	1	0	0	0	0
0	1	1	0	1	1	0	0
1	1	0	0	1	1	0	0

1 का even parity

even parity - 0

odd parity - 1

parity ⇒ 1 1 0 0 0 0 0 0 (5th row) ⇒ LRC code / Hash

* ② Multiplication Method - (Idea of a Message Digest)

suppose original data (PT)

plain text ⇒ 7391743

multiply operation	Result
mul 7 X 3	21
Discard first digit	1
mul 1 x 9	9
mul 1 x 9	9
mul 9 X 7	63
Discard first digit	3
mul 4 X 3	12
Discard first digit	2
mul 2 X 3	(6)

{Possibility of same Hash code (depends on msg length = 2^{128}}

(6) → Hash function

Page No.

CNS

7/11/22

* (SHA) Secure Hash algorithm

i) Padding →

400 bits → original Information
148
448 → 448 bits

1000 bits
+1
1001
+24
1025

1024
+1
1025

400
+ 48
448 bits

112
-64
48

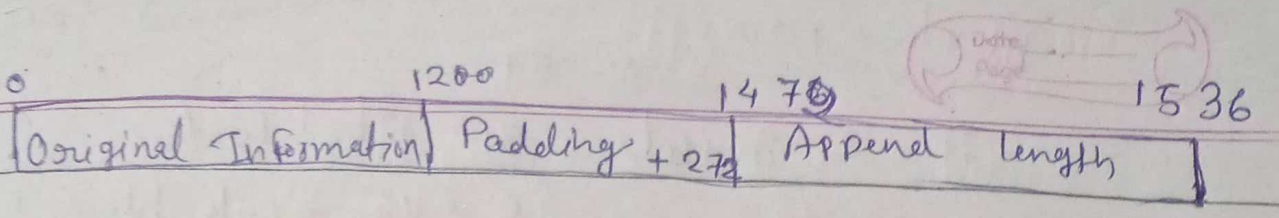
Append length
48
+64
512 bits

512
+3
1536

1200

1001
+23
1024

1536
-64
1472



Step 1)

1200
272
1472

Steps ⇒

(i) Padding
(ii) Append length
(iii) Convert the input into 512 bit block
(iv) initializing chaining variable.
5 variable (32 bits)

		value				
A	Hex	01	23	45	67	H
B	Hex	89	AB	CD	EF	H
C	Hex	FE	DC	BA	98	H
D	Hex	76	54	32	10	H
E	Hex	C3	D2	E1	F0	H

steps 5
(v) Process block
Step-5.1 - copy the variable A to E in to a to e. value same.
5.2 - now divide the 512 - blocks in to 16 sub block i.e. 32 bits.
5.3 - SHA has 4 rounds & each round has 20 steps. so total 80 eteration steps.

block process –

(i) – input 512 bit block
i.e 16 - sub block (32 bits)
w(t)

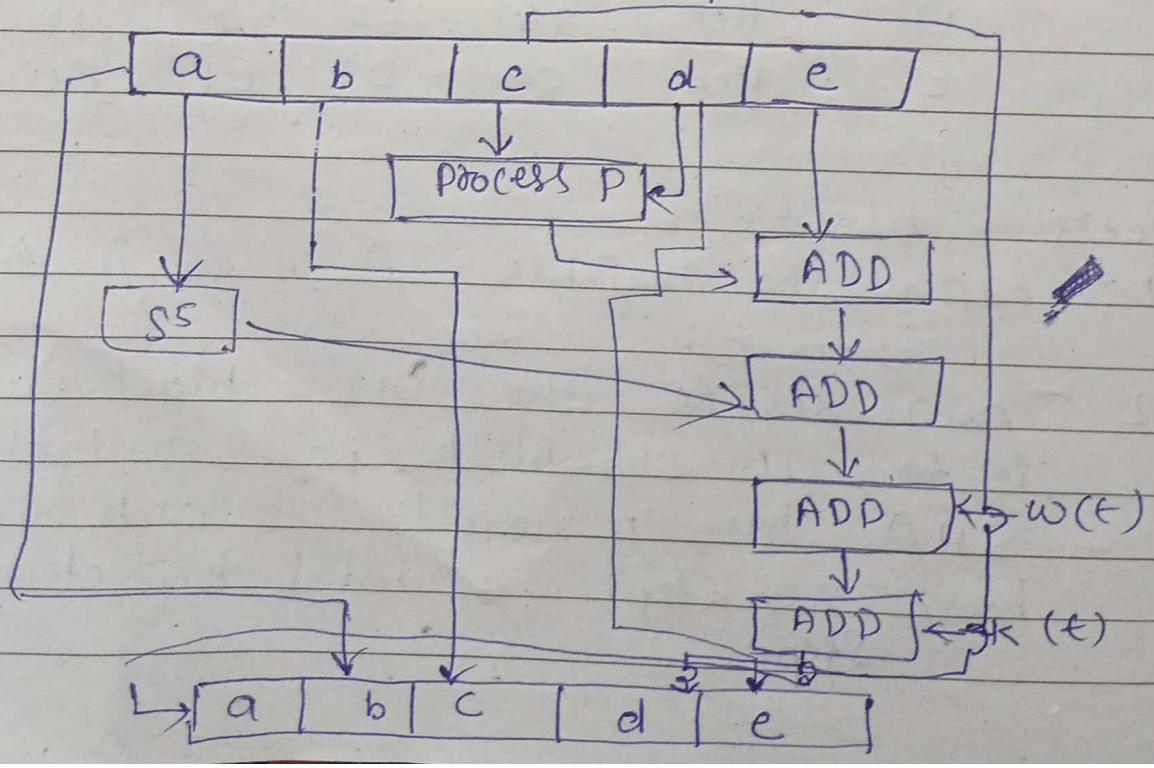
(ii) Chaining variable a, b, C, d, e,

(iii) four constant K(t) – 32 bits

Round	value of (t)	
	between	value lena hai
1	1 to 19	t = 1 to 79
2	20 to 39	
3	40 to 59	
4	60 to 79	

* SHA CNS Date - 9/11/22

Step 5.4 – operation of process Block



Explain the SHA algorithm ?

Mathematical operation of process block

- abcde = (e + Process P + $S^5(a)$ + w(t) + K(t))
  $a, S^{30}(b), c, d$
  where a, b, c, d, e = 5 variables
  process P = logical operation
  S^t = Circular left shift of process block by t bit
  w(t) = 32 bit output process block.
  K(t) = constant.

* Process P

Round		Process P
1	⟶	(b AND C) OR ((NoT b) AND (d))
2	⟶	B XOR C XOR d
3	⟶	(b AND C) OR (b AND D) OR (C AND d)
4	⟶	B XOR C XOR d

Explain the SHA with functional block and mathematical operation.

- SHA - 512 (a, b, c, d, e, f, g, h) (A to h)

CNS

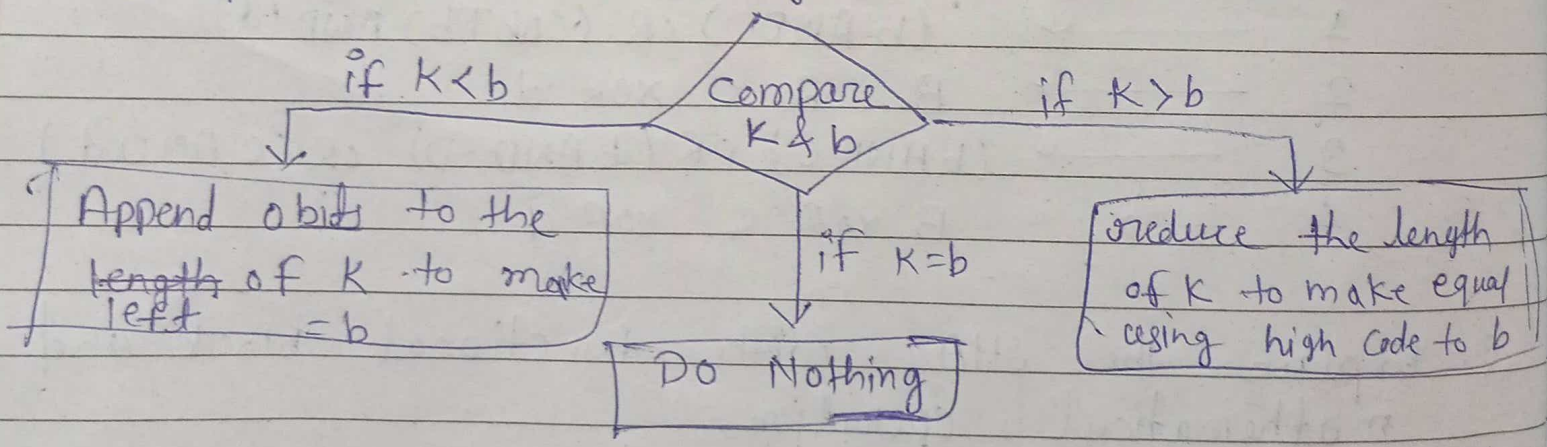
10/11/22

* MAC (message Authentication Code)
* HMAC (Hash Based Message althentic code)

Working Principle of HMAC -

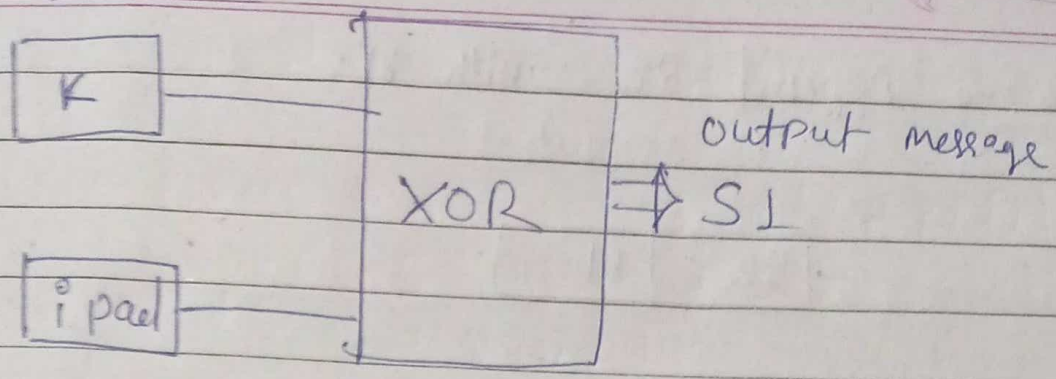
MD = Message Digest
M = Input Message
L = The no. of blocks in the M
b = no. of bits in each block
K = The shared symmetric K
input i pad = A string 00110110 repeated b/8 bits
output o pad = A string 01011010 repeated b/8 bits.

Step 1: Make the length of K equal to b

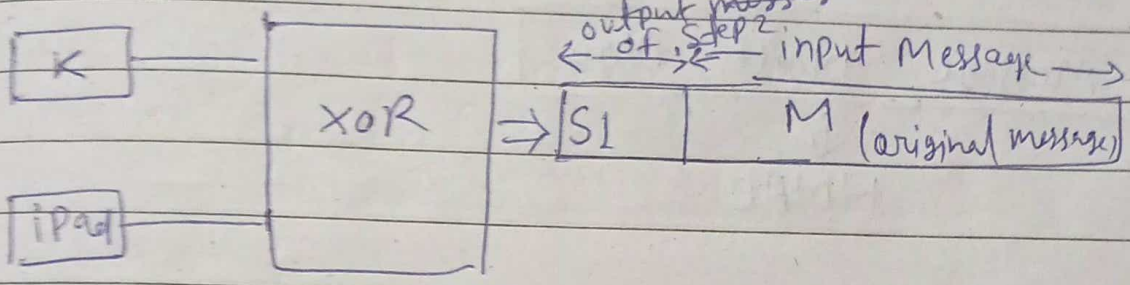


Step 2: - XOR K with ipad to produce S1

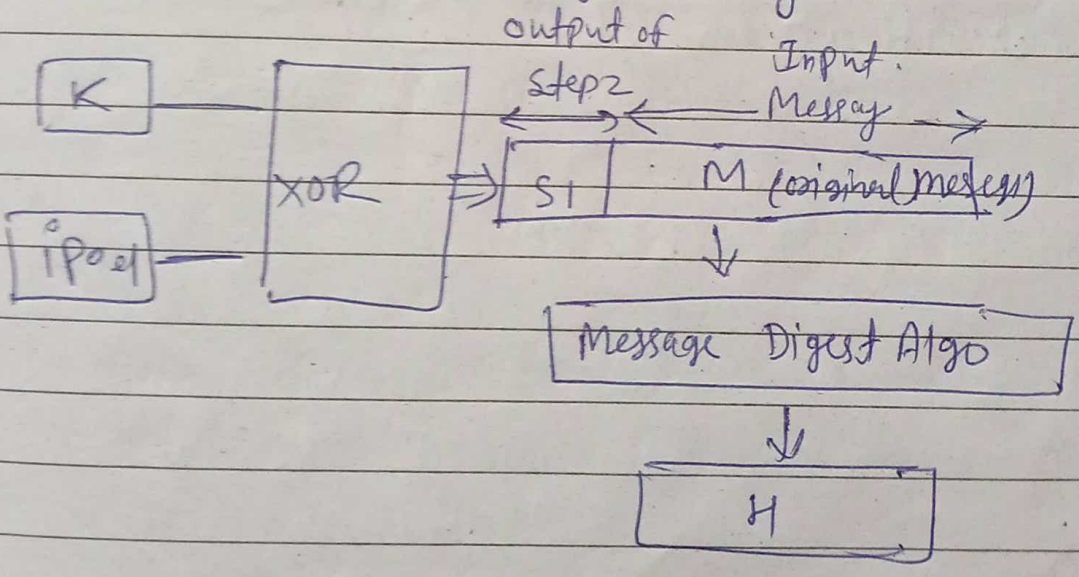
assume K = 50



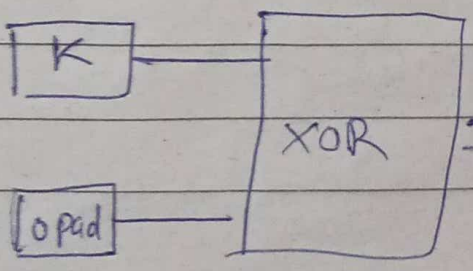
Step 3 :- Append M to S1



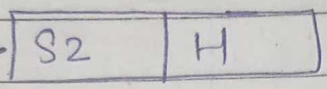
Step 4 :- Message Digest Algorithm



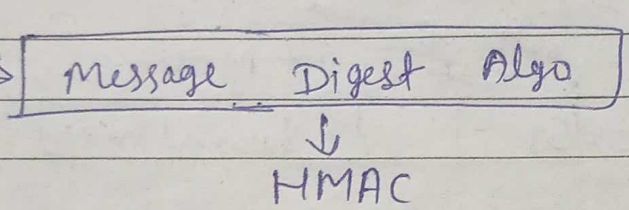
Step 5 :- XOR K with opad to produce S2.



Step 6:- Append S2 with H.
II output



Step 7:- Message digest Algorithm apply



* format of Digital certificate -

(2)

Version
certificate serial No.
Signature Algo. identifier
ISSUER Name
validity (not before / not after)
Subject Name
Subject public key Information
issuer unique Identifier

(1)

Subject unique Identifier
Extensions
certification Authority & Digital Signature

CMS

Date - 11/11/22

based

CMAC (cipher Message Authentication code)

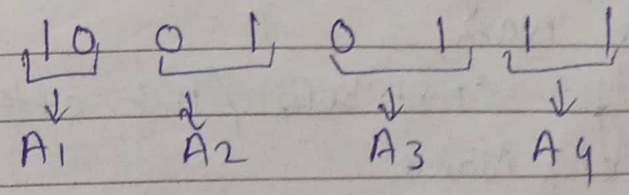
feature ⇒

↳ It has a size limit.

↳ It is a block cipher.

↳ given message is divided into equal blocks & each & every block is encrypted separately or endividually.

for Eg.



$C_1 = E[K, A_1]$

$C_2 = E[K, A_2 \oplus C_1]$

$C_3 = E[K, A_3 \oplus C_2]$

$C_4 = E[K, A_4 \oplus C_3]$ — $C_4 = CMAC$

$C_n = E[K, A_n \oplus C_{n-1}]$

↓

CMAC

Imp HMAC = Original message [H]

★ Disadvantage of HMAC or CMAC —

★ key Management

.cer

CNS

Date - 12/11/22

★ PKI (Public key Infrastructure)

Digital certificate generated ASN.1

feild

i) Certificate Serial No. - Provide unique identification No. of the particular Cert

ii) Signature Algo identifier.

iii) Issuer Name

iv) validity (not befor / not after)

v) subject Name

vi) subject public key Information

vii) Issuer unique Identifier
viii) subject unique Identifier
ix) Extension
x) certification & Authenxity & Digital signature.

* Distribution public & private key :=>

CNS Date - 14/11/22

* KERBEROS —
↳ user authentication Protocal
Set of Rules - Protocal

* the working of kerberos -
So, There are four parties involved in the network protocal.

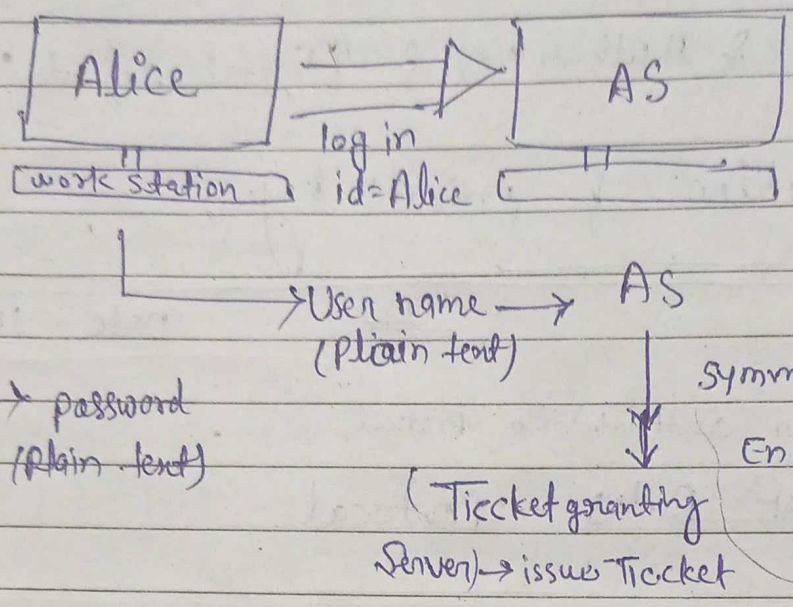
① Alice - The client work station.
user

② Authentication server - varifies the user during login
(AS) valid user

③ Tirckket granting server - The ISS. This server issues Tickets
(TGS) to certify proof of identify.

④ Bob - ~~The server~~ The Server offering ~~Server~~
Service ~~can~~ ~~services~~ such as N/W sharing
Resource Sharings printing etc.

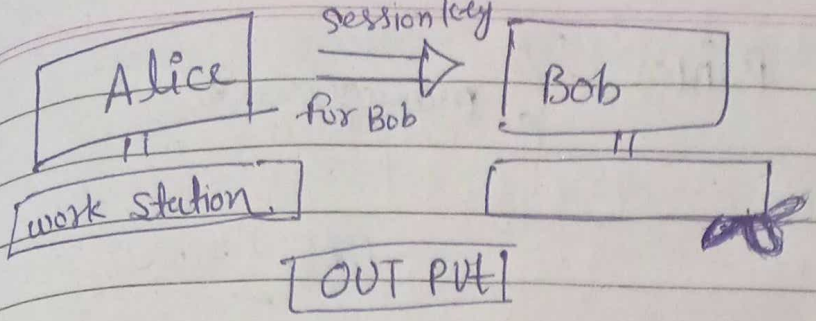
Step I - ~~log in~~ login (AS)



Step 2 - obtaining a service granting Ticket (SGT)

(i) The TGT as step 1
(ii) The id of server (Bob) whose ~~sver~~ services Alice interested in
(iii) The current time stampup, encrypted with same session key (KS)

Step 3 - user contacts Bob for Accesing the server
(Alice + Bob



⇒ information
(plain text)

⇒ KS + Symmetric key
(time stamup) + cipher text

* Biomatric Authentication

CNS Date - 15/11/22

* Private key Management -
* Machanisum for Protecting Private key -
(i) Password Protection.
(ii) PCMCIA CARD - ATM
personal Computer Memory Card ~~international~~
international Association.

(iii) Tokens - one tim possword (OTP)
(iv) Biometrics - also OTP, finger print
(v) Smart Card.

mechanism

Smart card or PCMCIA CARD
difference

Unit - 4

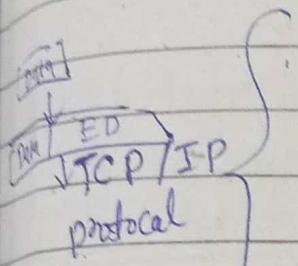
16/11/22

(i) SSL (Secure Socket layer) — This is available in TCP protocol

↳ it is a protocal & used for exchanging secure information bet^n the web browser & web server.

* web browser is a is a application software

start → add → google chrome



Application layer
secure Socket layer
Transport layer
Internet layer.
Data link layer
Physical layer — (destination का address बताते)

Add Application layer
PT ↑ plain text
Dicryption.
↑ C.T.

The working of SSL -

SSL has three sub-protocal -

(i) The handshake Protocal, — type of acknowledgement
(ii) The Record Protocal
(iii) The Alert protocal

(i) The handshake protocal

(1) The handshake Protocal -

parameter - → message

Type	Length	Content → what ever ?
1 byte	3 bytes	1 or more byte

fig: format of the handshake protocal

Message Type

1st
- Hello - request
- client Hello
- Server Hello

2nd
- Certificates
- Server key exchange
- Certificate - request
- Server Hello done
- Certificate verify

client key exchange

~~fin~~ shed finished → dead

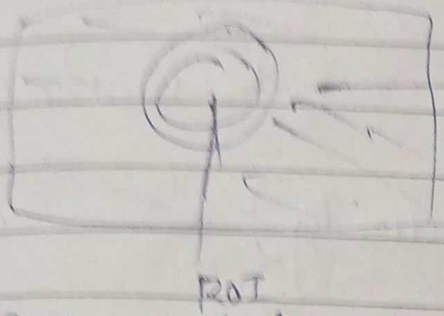
* Handshake protocal 4 Phases in Handshake protocal -

(i) 8. Establish Security Capabalition
(ii) Server authentication & key exchange
(iii) client authentication & key exchange
(iv) finished

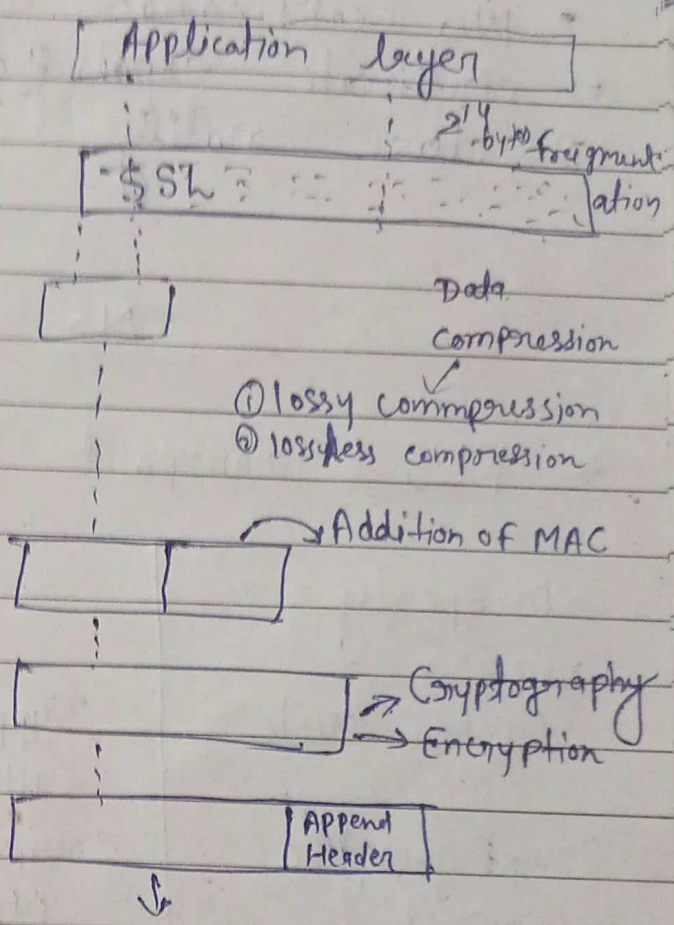
CNS

(Fragmentation) 17/11/22

The Record protocal -
(a) Confidentiality
(b) Data Integrity



(3) fragmentation
(4) Compani Compression
(5) Addition of MAC
(6) Encryption
(7) Append Header



(b) The Alert protocal

Alert Imp 1 topic

1) Unexpected Message
2) Bad Record MAC
3) Decompression Failure
4) Hand Shake failure
5) illegal parameters.
6) illegal parameters,
7) No certification.
8) Bad certification

fatal alerts.

* No certification
(8) certificate expiring d
(9) close notify

IETF

CNS Date - 18/11/22

* TLS (Transport layer Security) difference

Property	SSL	TLS
version	3.0	1.0
Cipher Suite	Supports an algo called Fortezza	Does not support the algo Fortezza
Cryptographic secret	computed as random No.	uses psends random No. for master secret
Alert protocal	As explained in SSL	No. cert. is deleted few newly added i) Decryption failure ii) Record overflow iii) Unknown Certificate iv) Access demind v) Decode error vi) internal error

property	SSL	TLS
Handshake protocal	Same as explained	Some details are changed
Record Protocal	use MAC	use HMAC

Like

Type	length	content
2 byte	5 byte	20 or more byte

* HTTPS (before sending request data)
  ↳ Server access limit.
* SHTTP — secure HTTP

The secure highper tent protocal is a set of security machanisum defined for protecting the Internet traffic. this include the data entry froms and internet based transcations.

No dead HTPP request send by using SSL is indenty HTTPS.

the key difference betn SSL and SHTTP is that SHTTP work on indusival message were as SSL does not differensiate between different message.

CNS

Date - 19/11/22

* SSH (Secure Shell) Protocal -

↳ Secure communication, remote login, Encrypted Message & athentic user (client & server)

Remote login = one-to-one communication.

* Working of SSH -