Cryptography

7/01/2025

Cryptography and Network Security

- Key Based
- Key less

- **Security**
- **Types of Security**
  1) No Security
  2) ID & Password
  3) Obscurity
  4) Security through encryption

Security Services / Principle of Security

i) Non-Repudiation
(False Identification or you can't denied anything)

ii) Authentication

iii) Access Control → Role Management (User Specific)
→ Rule Management (Resources)

CIA → Confidentiality Integrity Availability

Various types of security :-

Attack

Two Types :-

1) Passive Attacks (Doesn't do any modification of actual msg)
   - Detection Difficult
2) Active Attacks (modification of actual msg)
   - Detection easier compare than passive attacks

(Detection → Solution)

Man in the middle Attacks

Cryptography :—

The art / science of achieving security through encryption

method to convert plain text to cipher text

[Easily readable & Understandable] [Non-Meaningful Text]

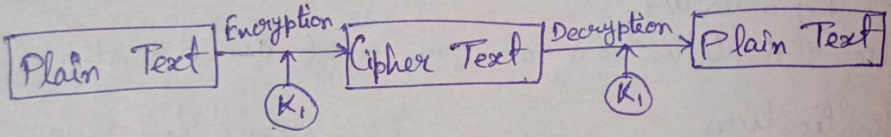
Key

① Symmetric key cryptography (Private key cryptography)

② Asymmetric key cryptography (public key cryptography)

[used → (i) public key (ii) private key]

① Symmetric key

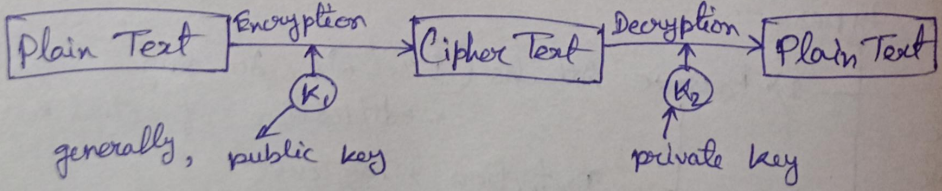


- One of algorithm

(i) Data Encryption Standard (DES) / DEA → Algorithm

② Assymmetric : (public)

(public key + private key)



- Spacial case → vice-versa

(*) A B C D . . . . . Z

0 1 2 3 25

(*) $K \geq 1$, non-negative , $K \leq 25$

$1 \leq K \leq 25$ for ceaser cipher

Ex: HELLO, key = 4

$e(H) = E(H, 4) = (H+4) \bmod 26 = (7+4) \bmod 26$

$= 11 \bmod 26$

$= 11$

$\Rightarrow L$

E → I
L → P
L → P
O → S

Cryptography Algorithm is divided into 2 parts

- Substitution
  +4 / +const
- Transposition (changing position of character)
  - Key based
  - Key less

Hash Code: → Do not use any key

→ Uses Hash fn

Message Digest:
Fixed length for var.

MD5

1st Algo. ever proposed

Ceaser Cipher → Mono alphabetic Cipher

C	B	A	S	E	R
+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓
F	H	D	V	H	U

Poly

H E Y THERE
+ + + + + + +
J G X A Y

Example:

Meet me at Two PM, key = 4

+4 +4 +4 +4 +4 +4

Cyclic after Z

W	X	Y	Z
+4 ↓	+4 ↓	+4 ↓	+4 ↓
A	B	C	D

Formula: → Encryption

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

C → Cipher
26 → no. of Alphabet

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

Crypto

Sem - 6

31/1/2025

Data Encryption Standard (DES):

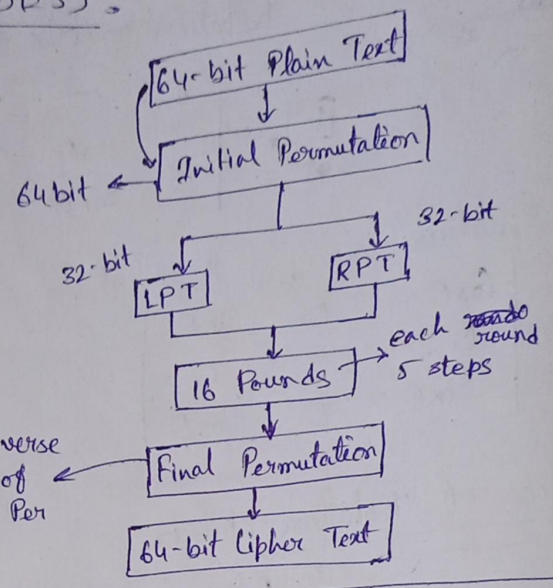
64-bit Plain Text

Key (56 bit) → DES

64-bit Cipher Text

every 8th bit discarded

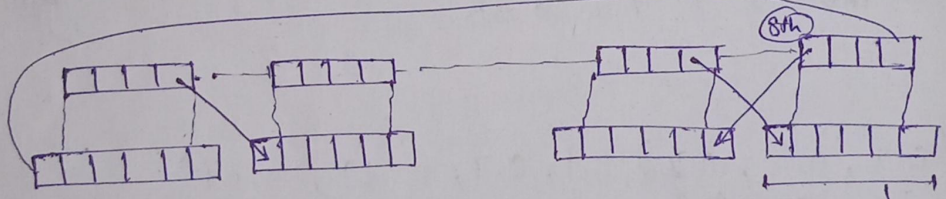
64 → 56



Steps

1. Key Transformation [56 bit → 48 bit Key] (left circular shift)
2. Expansion Permutation [32 bit → 48 bit]
3. S-box
4. P-box
5. XOR and Swap

performed only on RPT

② 

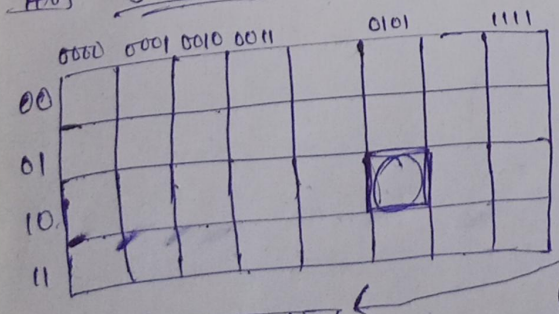
③ Substitution Box:

XOR operation of 48 bit (for ①) and 48 bit (for 2).

Then 48 bit result in S-box.

Final output 32 bit from S-box

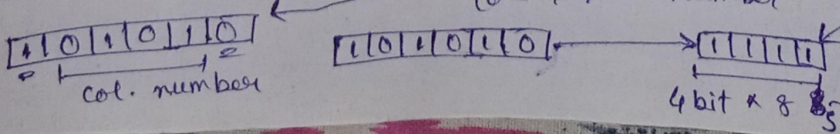
8 S-box, 64-bit, matrix / array



16 Col.

4 rows

values (0-15) → 4 bit, 1111



④ Permutation Box :→ 32 bit output after permutation

⑤ (LPT 32 bit) XOR (32 bit) → 32 bit output for next Round

Old RPT → Swap → New LPT for next Round

After 16 pounds

LPT + RPT → 64 bit ← Final Permutation (Inverse of initial) → 64 bit Cipher Text

Analysis of DES:

1. Avalanche Effect:

A small change in plain text or key should create a significant change in Cipher Text.

2. Completeness Effect:

Each bit of the Cipher Text needs to depend on many bits of the plain Text.

Weakness / Disadvantage of DES

(i) Parallel Processing in < 2 min —

(ii) Plain Text $\xrightarrow{\text{Enc.}}$ Cipher Text $\xrightarrow{\text{Enc. Again}}$ Plain Text

4 weak keys. All 0's, All 1's, Half 0's, Half 1's

(iii) 6 semi — weak keys

(iv) 48 possible weak keys

(v) 2 diff. plain Text → Same Cipher

(vi) 2 diff. keys → same Cipher Text

Cryptography

7/2/2025

(*) Diffie-Hellman Key Exchange Algorithm:

1. $n, g \rightarrow$ prime numbers
2. Alice, x, $A = g^x \bmod n$
3. Alice send A to Bob.
4. Bob, y, $B = g^y \bmod n$.
5. Bob sends B to Alice.

Large Prime Number

Alice, Bob

6. Alice → $K_1 = B^x \bmod n$.

7. Bob → $K_2 = A^y \bmod n$.

Example:

1. $n = 7$, $g = 11$ | let, $x = 3$, $y = 6$
2. Alice → $A = 7^3 \bmod 7$ $= 2$
3. Alice → 2 → Bob
4. Bob → $B = 7^6 \bmod 11 = 4$
5. Bob → 4 → Alice
6. $K_1 = 4^3 \bmod 11 = 9$
7. $K_2 = 2^6 \bmod 11 = 9$ ✓

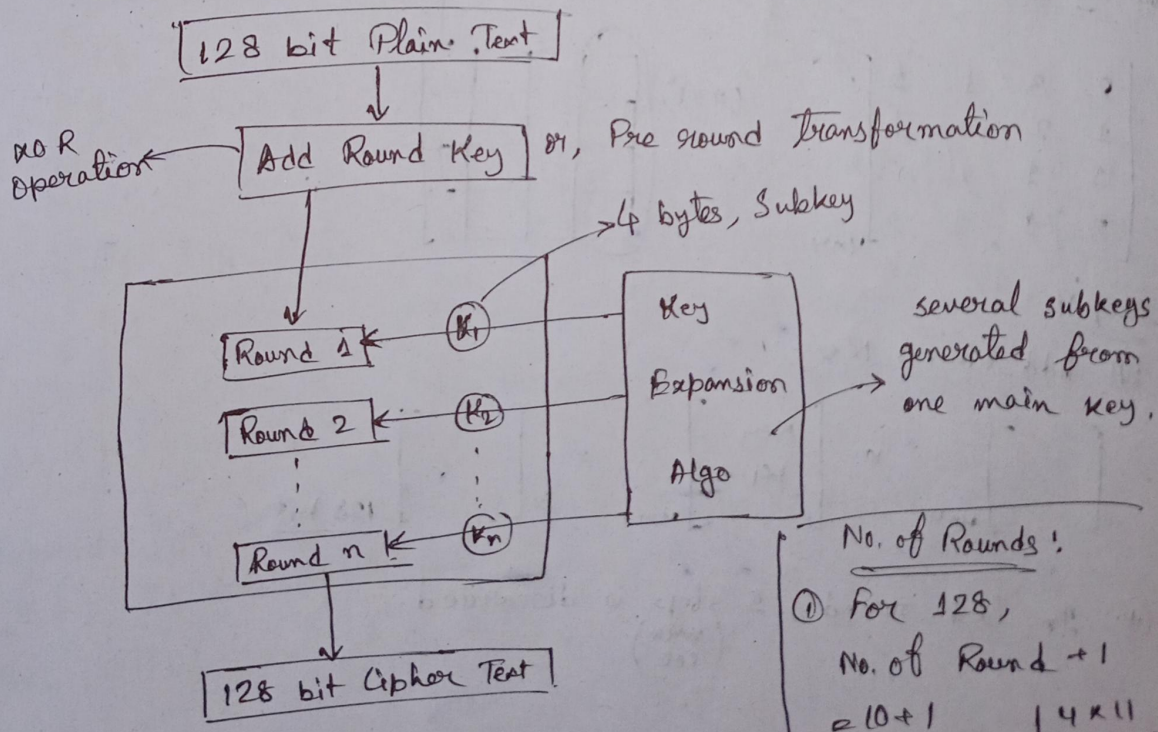
(+) Advanced Encryption Standard (AES):

2000
Rijndael
2001

128 bit, plain Text → 128 bits Cipher Text

Rounds	Length of Key	
10	128 bits	AES-128
12	192 bits	AES-192
14	256 bits	AES-256

(++)



No. of Rounds:

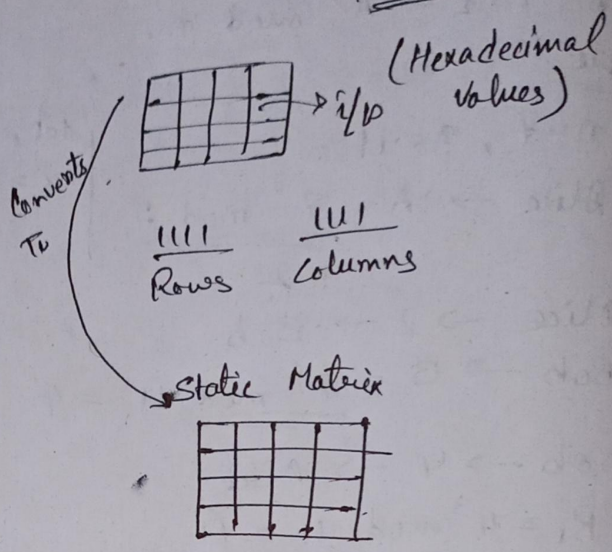
① For 128,
No. of Round + 1
= 10 + 1
= 11 subkeys
[0 to 10]

4 × 11
44 bytes subkeys

Steps:

1. Substitution Bytes.
2. Shift Rows.
3. Mix Columns
4. Add Round Key

4 words



Step 1

ABS ⟶ S-box

16×16

Step 2 Shift Rows

0	1	2	3D	51
1	0	1	F	C
2	7	8	A	B
3	A	F	D	8

i/p

Left Shift

1	2	3D	51
1	F	C	0
A	B	7	8
8	A	F	D

0 shift
1 shift
2 bit left shift
3 bit left shift

4×1

(4×4) States Matrix

Mix Columns:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}_{4\times4} \times \begin{bmatrix} & \\ & \\ & \\ & \end{bmatrix}_{4\times4} \rightarrow (4\times1)$$

Step 4

Add Round Key

$$\begin{bmatrix} \quad \end{bmatrix}_{4\times4} \times \begin{bmatrix} \text{Key} \\ \text{K1} \end{bmatrix}_{4\times1} = \begin{bmatrix} \quad \end{bmatrix}_{128\text{ bit}}$$

(*) In last round, 1 step is discarded. (mix col)

11/2/25

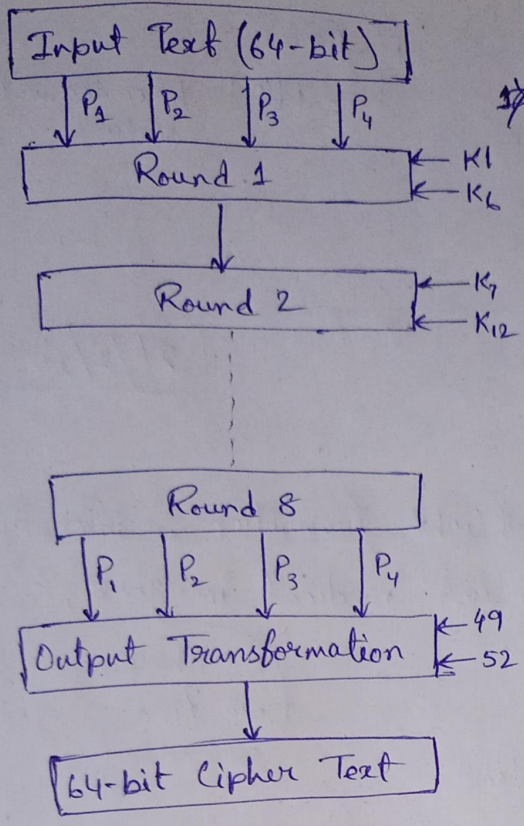
Cryptography

AES (4-steps)

International Data Encryption Algorithm (IDEA)

Plain Text (64 bits)

- Rounds – 8
- Keys – 128
- 6 – Subkeys
- 14 – steps are present



14-Steps

1) Multiply — P_1 and K_1
2) Add — P_2 and K_2
3) Add — P_3 and K_3
4) Multiply — P_4 and K_4
5) XOR — 1 and 3
6) XOR — 2 and 4
7) Multiply — Step 5 and K 5
8) Add — Step 6 and Step 7
9) Multiply — Step 8 and K_6
10) Add — Step 7 and Step 9
11) XOR — Step 1 and Step 9
12) XOR — Step 3 and Step 9
13) XOR — Step 2 and Step 10
14) XOR — Step 4 and Step 10

12-Rounds Rivest Cipher-5 (RC-5)

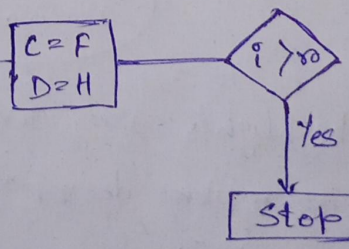
Rohar Rivest proposed that technique

Rounds → 0-255
Keys → 0-255
8-bits

2-word i/p → 16, 32, 64

3-Steps
1) XOR
2) CLS (Circular Left Shift)
3) Add with the key

1) Divide the Plain Text into two parts (Equal)
2) Add A and S[1] → C
3) Add B and S[2] → D
4) XOR C and D → E
5) Circular Left Shift E by D bits
6) Add E with S[2·i] → F
7) XOR E and F → G
8) Circular Left Shift G by F bits
9) Add G with 2[2*i+1]



H.W.
Take one Binary Number & Solve

Blow Fish :-

Key Size ⟶ 32 to 448 bits
Plain Text ⟶ 64-bits
Sub Keys ⟶ 18
S-box ⟶ 4
(256 bits)

P-Array
↳ P[0] = hexo decimal values

Cryptography

Date: 14/2/2025

1) Encrypt the following plain text using ceaser cipher:

Plain Text: ~~All the Best~~ ALL THE BEST

Key: 4

2) Encrypt the plain text "HOW ARE YOU" using key "NCBTQZARG" by the substitution technique called Vernam Cipher.

3) Transform the below mentioned plaintext into cipher text using the key "COLLEGE" by using play fair cipher.

Plain Text: STUDENTS ARE PLAYING FOOTBALL

Answers

1) Encryption:

E(A) + K = 4 ⟶ E

E(L) + K = 4 ⟶ P

E(T) + K = 4 ⟶ X

E(H) + K = 4 ⟶ L

E(E) + K ⟶ I

E(B) + K ⟶ F

E(S) + K ⟶ W

∴ Cipher Text = EPP XLI FIWX

2) A → D.

7 14 22	0 17 4	24 14 20
H O W	A R E	Y O U
N C B	T Q Z	A R G
13 2 1	19 16 25	0 17 6
20 16 23	19 33 29	24 31 26
U Q X	T H D	Y F A

33%26=7 29%26=3 31%26=5 26%26=0

3)

COLLEGE

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

STUDENTS ARE PLAYING FOOTBALL

CT: TU SH ET UT BQ G N CD VN PE BB RB BD D2 LD XL

Cryptography

21/02/2025

Symmetric	Asymmetric
(i) This is also known as private key or secret key cryptography.	(i) This is also known as public key cryptography.
(ii) Only one key is used for both encryption and decryption.	(ii) Two different keys (public key and private key) are used for encryption and decryption respectively.

Symmetric	Asymmetric
(iii) This is faster in execution.	(iii) This is slower in execution.
(iv) It is less complex and less computational power is required.	(iv) It is more complex and more computational power is needed.
(v) It is used for the transfer of bulk data (because it executes faster).	(v) It is used for secretly exchanging the secret key
(vi) Sharing the key between sender and receiver is not safe.	(vi) No problem of key sharing because of private key concept.
(vii) Commonly used algorithms are DES, AES, RC5, 2DES, 3DES etc.	(vii) Commonly used algorithms are RSA, DSA etc. ↓ Digital Signal Algorithm

~~DES Algorithm~~ DES Analysis

(i) ~~Avalanch Effect~~

(i) Avalanche Effect —

A small change in plain text or the key should create a significant change in cipher text.

(ii) Completeness Effect —

Each bits of the cipher text needs to depend many bits of the plain text.

Weakness of DES :—

(i) Key Size : In DES 56 bits keys are required for encryption. Hence a total of 2^{56} combinations can be made out of these 56 bits keys. In today's parallel processing, it is very easy to crack the actual key.

(ii) Weak Keys: There are 4 weak keys. These are -
(a) All 0's, (b) All 1's, (c) Half 0's, (d) Half 1's

(iii) Semi Weak Keys: 6 pairs of keys are called semi-weak keys.

(iv) Possible Weak Keys: There are 48 possible weak keys out of 2^{56} combinations.

(v) Key Clustering: It means that 2 or more keys can create the same cipher text from the plain text.

(vi) Weakness in Cipher Design: Two specifically chosen input to X-box array can create same output.

Imp. Questions:
1. Types of Adapt
2. What is security, types,
3. Virus, Worm, Trozan Horse
4. Hill Cipher

Book:
ATUL KAHATE
CRYPTOGRAPHY
Text Book

Transposition

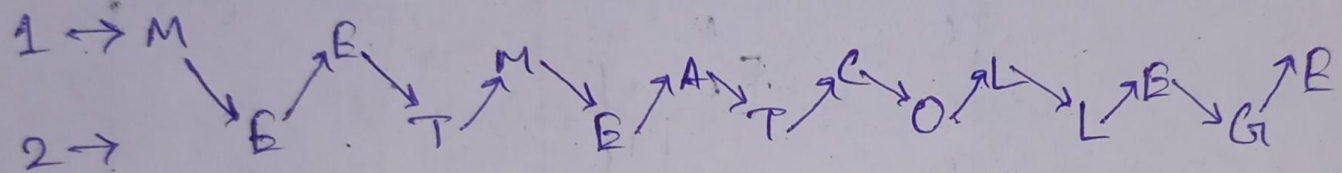
Cryptography

Rail Fence Technique (Keyless Transposition)

Plain Text → MEET ME AT COLLEGE

No. of row = 2 . (by default) (fixed)

No. of columns: depends upon the length of the input text.



Cipher Text → MEMACLEEETETETOLG
(nonspaces)

Row Transposition / Simple Columnar Technique :-
(Keyed Transposition)

PT → MEET ME AT COLLEGE

Key → Integer (Ex - 41235, 52134)

CRYPTO (Here the alphabet)
1 4 6 3 5 2

Write → Row
Read → Column

1	4	6	3	5	2
M	E	E	T	M	E
A	T	C	O	L	L
E	G	E	X	Y	Z

Dummy bits / Bogus Characters

Cipher Text →

MAEELZTOXETGMLYECE

Double Columnner Technique

Step - 1

PT → MEET ME AT COLLEGE

key → CRYPTO

1 2

4. Keyed Transposition —

PT → ATTACK POSTPONED UNTIL TONIGHT

key → 4 3 1 5 2

↓ ↓ ↓ ↓ ↓

1 2 3 4 5

** Input Text length = key length

Input → ATTAC KPOST PONED UNTIL TONIGHTXYZ

⇒ ATACT SOKIP ENPDO ITULN INTGOYXHZT

Input Text's 4th character will be 1st character of the cipher text

Cipher Text → ATACTSOKTPENPDOITULNINTGOYXHZT

Substitution Method

Vernam Cipher —

Plain Text → HOW ARE YOU

key → NCBTZQARX

Keysize = Input size

Encryption

PT →	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
key →	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
subtract 26 from those which is ≥ 26 →	U	Q	X	T	Q	U	Y	F	R

Cipher Text → UQXTQUYFR

Decryption (CT as PT)

PT →	U	S	X	T	S	U	Y	F	R
	20	16	23	19	18	20	24	5	17
Key →	N	C	B	T	Z	S	A	R	X
	13	2	1	19	25	16	0	17	23
subtract →	7	14	22	0	-9	4	24	-12	-6
Add 26 →	7	14	22	0	17	4	24	14	20
with those which is <0	H	O	W	A	R	E	Y	O	U

**Playfair Cipher — (I & J are considered as a single character) 5×5 matrix

PT → SISTER NIVEDITA UNIVERSITY

Key → CRYPTOGRAPHY

- whatever input text is given, we have to change it as a pair i.e. 2.
- Oneach can be filled in the matrix as 1 time.
- After writing the key in the matrix we have to write the other rest alphabet.

PT → SI ST ER NI VE DI TA UN IV

ER SI TY

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

** যদি same row তে 2টি ch থাকে তাহলে তাদের replaced হবে immediate next ch দিয়ে, Ex → AB → HO

TA LL

TA LX XL

I_ → TZ

** যদি same column থাকে, তাহলে তাদের replace হবে immediate next down ch দিয়ে, Ex → FW → NY

If not same col^m / same row →

diagonally form a sub matrix first ch-এর same row-তে 2nd ch-এর corresponding যেটা থাকে, তাদের এই মানের replace হবে।

Ex → NZ → SW

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

ZB MG QF RM EK YB WL EX MG ZB CP

Cipher Text → QKZBMGQFRMEKYBWLEXMGZBCP

H/W

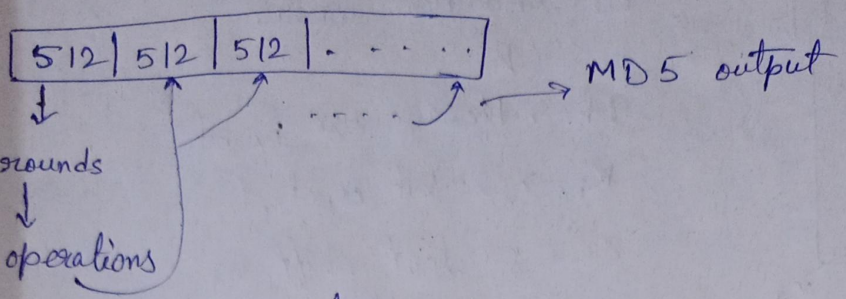
PT → NETWORK SECURITY

Key → SOFTWARE

Cryptography

Rivest

MD-5 (Message Digest-5)



1. Add Padding bits
2. Add length bits / Appending length
3. Initialize MD buffer
4. Process each 512 blocks
5. Output Message Digest

1. Add Padding bits (we have to add bits)
   - Multiple of 512 - 64 → 472 bits

2. | original msg | Padding | Length |
   (Length: 64-bit)

   2^8 | 2^{10}

   2^8

   1111111100 - - - 0

   no. we have to mod 2^{64} > 64

   = ... (no. of 1) - - 0

3. Buffers

A =	0	1	2	3	4	5	6	7
B =	8	9	A	B	C	D	E	F
C =	F	E	D	C	B	A	9	8
D =	7	6	5	4	3	2	1	0

functions

$F(B,C,D) \rightarrow (B \wedge C) \vee (\neg B \wedge D)$

$G(B,C,D) \rightarrow (B \wedge D) \vee (C \wedge \neg D)$

original msg. bits 1000 bits

$512 \times 1 = 512$

$512 \times 2 = 1024$

1024
64
960 ×

$512 \times 3 = 1536$

1536
- 64
1472

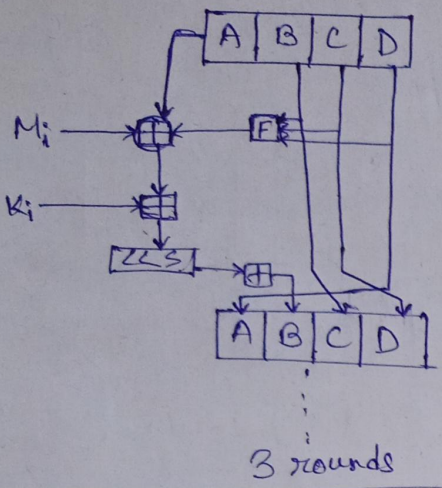
$1536 - 64 + 64 = 1536$

4 round has 4 functions :-
each round has 1 func

$\wedge$ = AND
$\vee$ = OR
$\neg$ = Negation
$\oplus$ = XOR

$H(B,C,D) \rightarrow B \oplus C \oplus D$

$I(B,C,D) \rightarrow C \oplus (B \vee \neg D)$



$\boxplus$ → Addition modulo 2^{32}

M_i → Message size 82-bit

K_i → 32-bit constant

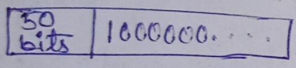
<<< 5 → left shift by 5 bits

1/4/25

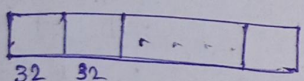
Secure Hash Algorithm (SHA-1):-

512 → 16 0 bit

1. 448 + 64



2.



16 blocks

$$w_t \Rightarrow w_t - w_{16} + w_t - w_{14} + w_{t-8} + w_{t-3}$$

$w_{16} = w_0 + w_2 + w_8 + w_{13}$

Buffers

A = 67452301

B = efcdab89

C = 98badcfe

D = 10325476

E = C3D2E1F0

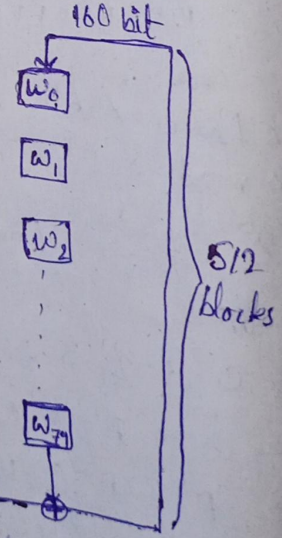
2^{64}

2^{14}

111111 00000...

1st no. of 1

80 steps in each blocks (512)



each buffer is having 32 bit Hexadecimal values.

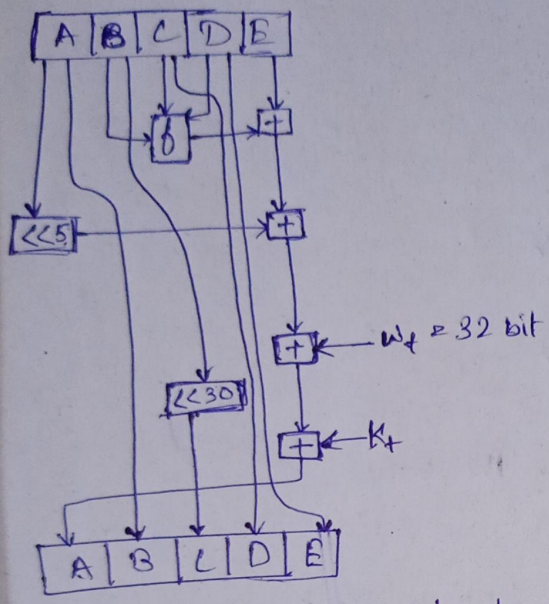
$F_1 = B \wedge C \vee \neg B \wedge D \xrightarrow{K_t} W_0 - W_{19}$

$F_2 = B \oplus C \oplus D \rightarrow W_{20} - W_{39} \rightarrow K_{2t}$

$F_3 = B \wedge C \vee B \wedge D \vee C \wedge D \rightarrow W_{40} - W_{59} \rightarrow K_{3t}$

$F_4 = B \oplus C \oplus D \rightarrow W_{60} - W_{79} \rightarrow K_{4t}$

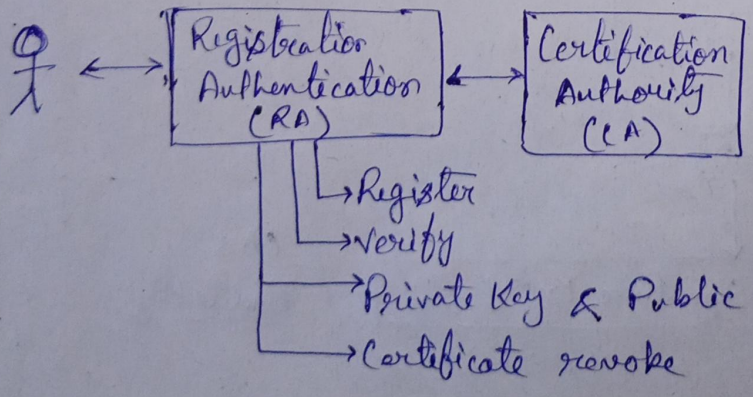
[+] → Addition modulo 2^{32}



Digital Certificate - standard of Public Key Infrastructure

- Assymetric key
- Message adjust

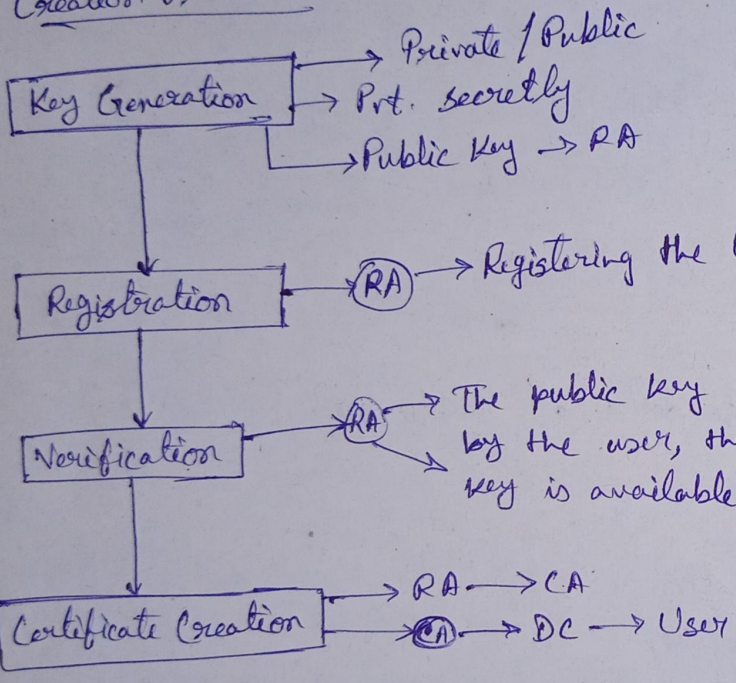
Authentication function
Encryption Services



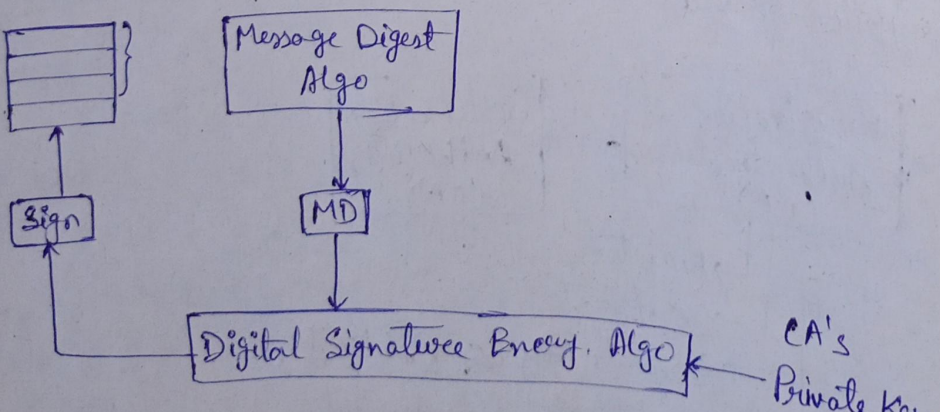
fields of DC

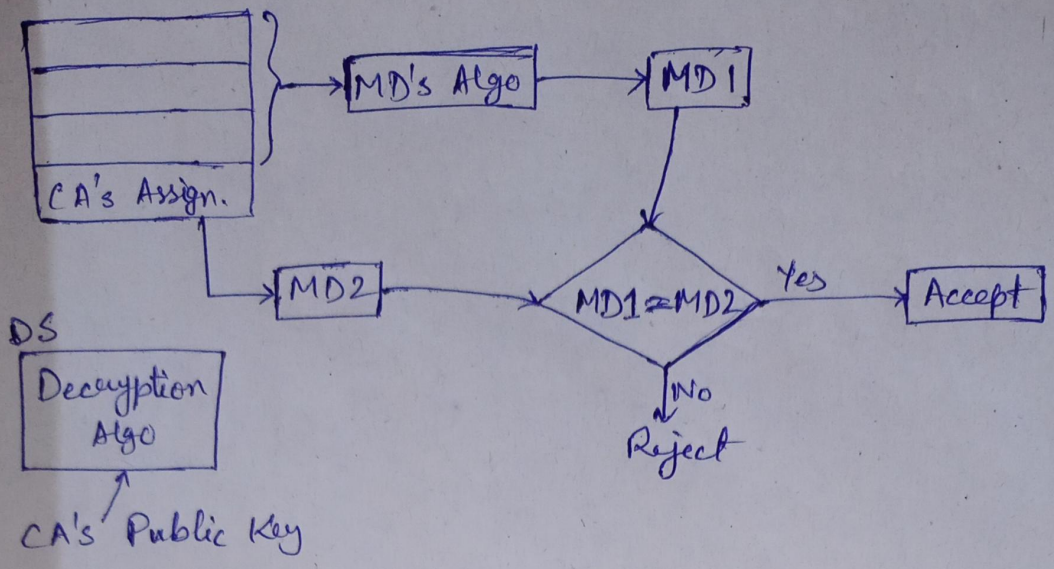
Name : "A B C D"
Public Key : "1 2 3 @ #"
Other Info : "Email ID"
Period from : 01/4/2025
Period to : 01/03/2035
Sign Authority : verisign

Creation Process :-



Verification of DC :-




MD's Algo
MD1
CA's Assign.
MD2
MD1 = MD2
Yes
Accept
No
Reject
DS
Decryption Algo
CA's Public Key