Unit-3 Cryptograph

DOMS | Page No. | Date / /

Cryptography is the art or science or method that converts the plain text into cipher text & cypher text back to plain text.

Key Terms:

- Plain Text : Original Message or Text.
- Cipher Text : Coded Message or Text.
- Crypt Analysis : It is the study of method for obtaining the meaning of encrypted information.
- Caesar Cipher : Letters are replaced by other letters. Each letter of the alphabet is replaced with the letter standing three places further down the alphabet.
  eg: HELLO → KHOOR
- Modified Version of Caesar Cipher : It is a simple substitution technique. It's key range is 1 to 25. Any no. can be used as a key value.
- Mono-Alphabetic Caesar : It is a form of symm. encryption as the same key can be used to both encrypt & decrypt a message.
  eg → HELLO ABNMZ
- Homophonic Substitution Cipher : HELLO → ABTMZ
- Polygram Substitution Cipher : One word is changed into the other word.
  eg: Hello → xyota
- Poly-alphabetic Substitution Cipher → Frequency Analysis

- Transposition Method: The position or the order of the letters of the plain text get changed.

Types:

1. Row Column Transposition:

Write: Row by Row

Read: Column by Column.

Key: Order of the column.

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

eg: Plain → Are You Ready For The Test.

key ⇒ 213

⇒

2	1	3
A	R	E
Y	O	U
R	E	A
D	Y	F
O	R	T
H	E	T
E	S	T

⇒ ROEYRESAVRDOHEEUA FTTT

2. Rail Fence Method: In this, the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

dept → No. Of rows of matrix

eg Plain : HELLO Depth = 2

H L O ⇒ HLOEL

E L

Depth = 3

H O

E L ⇒ HOELL

L

Depth = 4

H

E

L O ⇒ HELOL

L

Plain : HIBCA Depth : 3

H A

O

I C ⇒ HAICB

B

- One Time Pad : It is a type of substitution cipher. In this we assign a number to characters of plain text (a=1, b=2 ... z=26)
~~Key~~ Length of key = Length of plain text.

eg Plain : H E L L O
8 5 12 12 15

Key : A G H T P
1 7 8 20 16

Ciptur = 9 12 20 32 31

I L T F E

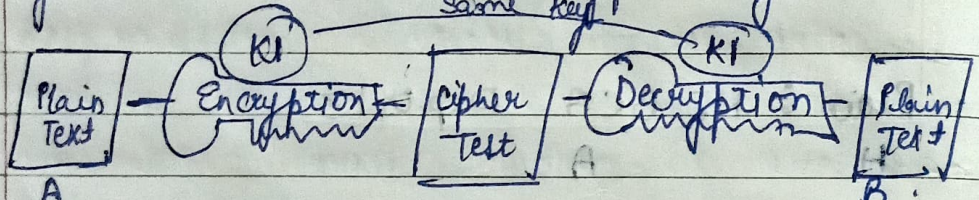
eg

	25	5	12	8	15	15	5
Msg :	W	E	L	C	O	M	E
Key :	H	E	L	L	O	H	I
	8	5	12	12	15	8	9

Cipher :	31	10	24	15	30	21	14
	E	J	X	O	D	U	N

⇨ Types of Cryptography :

1. Symmetric Cryptography : It is the simplest kind of encryption technique that involves only 1 key to encrypt and decrypt (cipher and decipher) information.
In this Sender key = Receiver Key.
The most popular Symmetric Key cryptography System is DES (Data Encryption System.

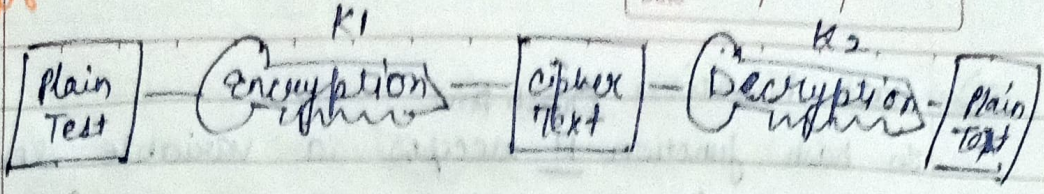


In this Sender has to share key with receiver so there are chances of attack. Because the key get shared on the network.

2. Asymmetric Cryptography : It is also called public key cryptography. It uses two keys i.e a pair of keys for encryption and decryption.
Public key → known to everyone
Private key → known only to that particular person.

Muskan Bhagria

DOMS | Page No.
Date / /



Sender key ≠ Receiver key

⇨ Diffie Hellman key Exchange Method:

Used to exchange secret keys between 2 users.
It is not an encryption algorithm
we will use asymmetric encryption to exchange the secret key

$A = g^x \bmod n$

$B = g^y \bmod n$

$K1 = B^x \bmod n$

$K2 = A^y \bmod n$

g, n is the prime number
Public on network

x is decided by sender & y is decided by receiver

Through this way we don't need to share key on network.

Let $g = 4$ $x = 2$ $y = 3$ $n = 7$.

$A = 4^2 \bmod 7 = 16 \bmod 7 = 2$

$B = 4^3 \bmod 7 = 64 \bmod 7 = 4$

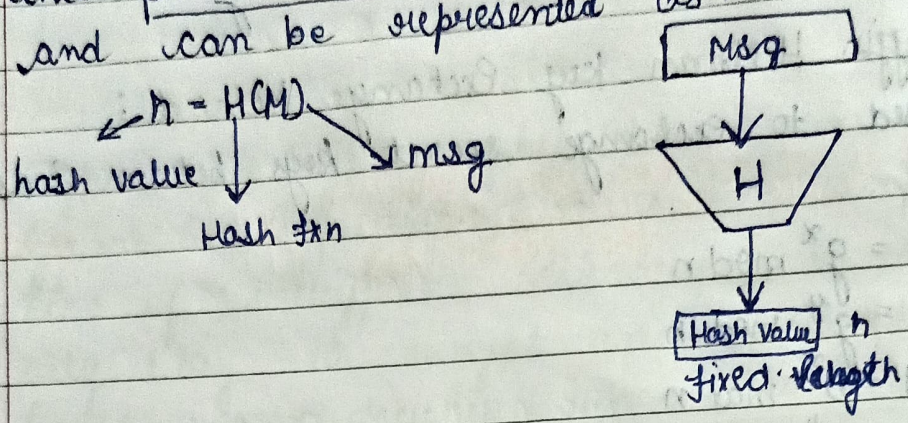
$K1 = 4^2 \bmod 7 = 16 \bmod 7 = 1$

$K2 = 2^3 \bmod 7 = 8 \bmod 7 = 1$

This is same

⇨ Hash Function (Hash fxn)

In hash function H accepts a variable length block of input data called a M (message) and produces the fixed size hash value and can be represented as.



- When hash function provides security it is called cryptographic hash functions.
- Hash function protects the integrity of the message. If encryption process is apply on message with hash function, it also provide authentication and confidentiality.
- Hash value appended with the message and forwarded to the receiver. At the receiver end, receiver computes the new hash value and compare this value with the appended hash value.
  If the comparison is true or both the hash values are same the integrity maintains otherwise receiver drops the msg.
- A hash function provides a property that hash function applied on variable

amount of data (M) and then it produces the fixed amount of output data.

- If any bit or bits changes in the data then whole hash function output will also change.
- The most popular hashing algorithm is MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

Properties of Hash function

1. Compression: As per compression property, output of the hash function is much smaller than the size of input.

2. Pre-image resistance: It means difficult to find the input from given hash output. i.e, $h = H(M)$. So if h is given, it is difficult to find message(M).

3. Weak collision resistance: Given message m1, weak collision resistance means that it is difficult to produce another message m2 such that $H(m1) = H(m2)$ i.e it means it is infeasible to find two different messages with the same hash value.

DOMS | Page No.
Date / /

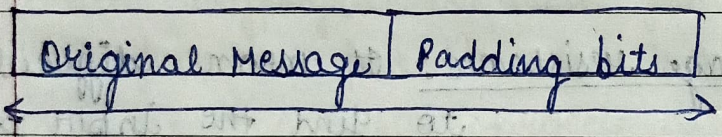
⇨ Message Digest 5 (MD5)

[Step 1: Append Padding bits]

- It produces 128 bit message digest.
- Input text is ~~512 bits~~ 2^{64} ~~blocks~~, which are further divided into 16 sub-blocks, each block contains 32 bits.
- Output of the algorithm is four 32 bit blocks (128 bit MD)

Step 1: Append Padding bits

Original Message + Padding (1-512 bits)



The total length of this should be 64 bits less than a multiple of 512.

For eg: Original message = 1000 bits.
We add ~~536~~ bits to it to make it the multiple of 512.
It will become ~~1536~~ that is the multiple of 512.
Padding bits ⇒ ~~984~~ 536 - 64 = 472.
472 are the padding bits.

472 → 1st bit is 1 and the left over 471 are 0
1000---0

Step 2: Append length bits

In this step, we add the length bit in the output of the first step in such a way that the total no. of bits is the perfect multiple of 512.

$1472 + \boxed{64} = 1536$

↓ length bit.

Msg	Padding bit	length bits

$msg = 2^{10}$

From 64 bits the 1st ten bits are 1 & the left over 54 bits are 0.

111---000---

Step 3: Initialize MD Buffer

Here we use 4 buffers i.e. A, B, C, D. The size of each buffer is 32 bits.

Process:

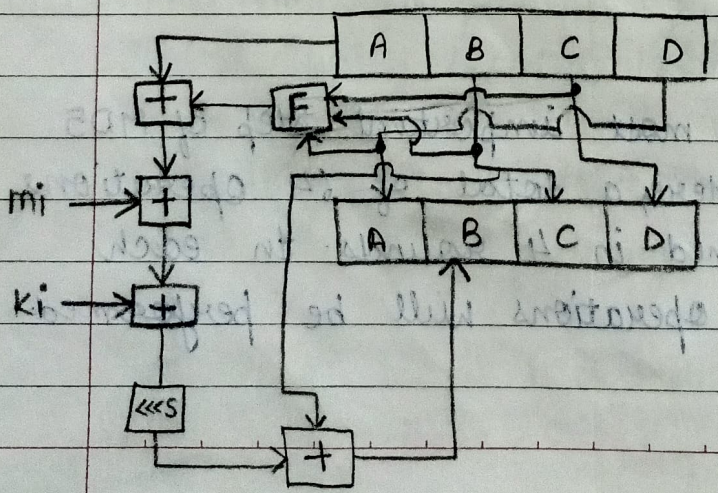
This is the most important step of MD5 algorithm. Here, a total of 64 operations are performed in 4 rounds. In each round 16 operations will be performed.

We apply a different function on each round. These functions are F, G, H and I. We perform OR, AND, XOR and NOT for calculating functions. We use 3 buffers for each function i.e B, C, D.

A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210

Total 64 operations
1 Function = 16 op.
2 " = 16 op.
3 " = 16 op.
4 " = 16 op.

F Ist fxn $(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$
G IInd " $(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$
H IIIrd " $(B, C, D) = B \oplus C \oplus D$
I IVth " $(B, C, D) = C \oplus (B \vee \neg D)$



V = OR ∧ = AND ¬ = NOT ⊕ = XOR

[+] = Addition modulo 2^{32}

[<<s] = Left Shift

Mi = 32 bit

ki = constant

⇨ SHA1 Algorithm [Secure Hash Algorithm]

Length of output is 160 bits

Here we 5 buffers A, B, C, D and E.

Process:

Here, a total of 80 operations are performed in 4 rounds. In each round 20 operations are performed.

A = 0123456 7

B = 89ABCDEF

C = FEDCBA98

D = 76543210

E = C3D2E1F0

Functions

F = (b ∧ c) V (¬b ∧ d)

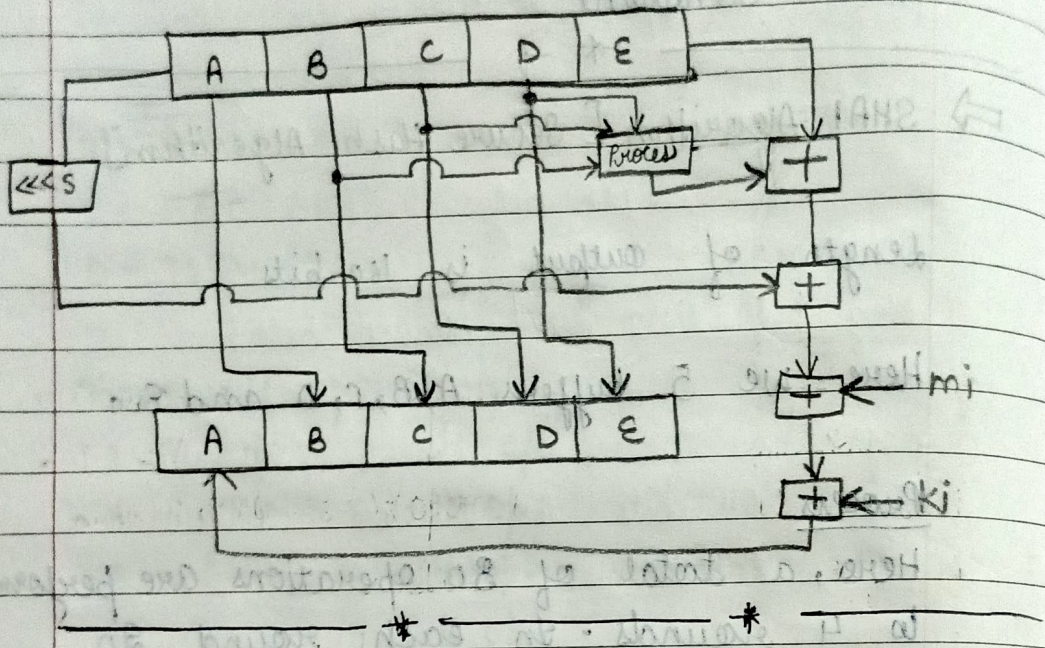
G = b ⊕ c ⊕ d

H = (b ∧ c) V (b ∧ d) V (c ∧ d)

I = b ⊕ c ⊕ d

DOMS | Page No.
Date / /

Value of k in 4 rounds (20 op).
0 to 19 → 5A827999
20 to 39 → 6ED9EBA1
40 to 59 → 9F1BBCDC
60 to 79 → CA62C1D6



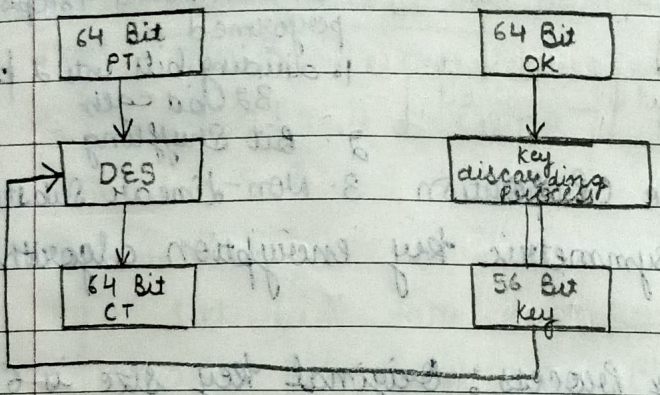
⇨ Difference between Encryption & Decryption.

Encryption	Decryption
• It is the process of converting plain text into cipher text.	It is the process of converting cipher text into plain text.
• It is the process which take place at sender's end.	It is the process which take place at receiver's end.
• Any msg can be encrypted with secret key or public key.	Any msg can be decrypted with secret key or private key

• In this, the sender sends the data to receiver after encrypted it.	Receiver receives the cipher text & convert it into plain text.
• Output of encryption is cipher text.	Output of description is plain text.

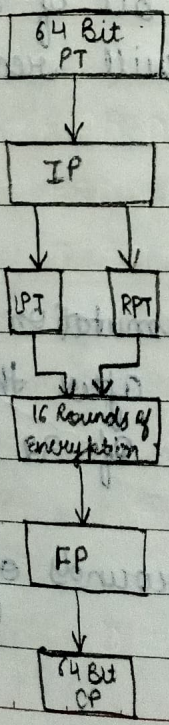
⇨ Data Encryption Standard (DES)

1.



PT → Plain Text
CT → Cipher Text
Ok → Original Text

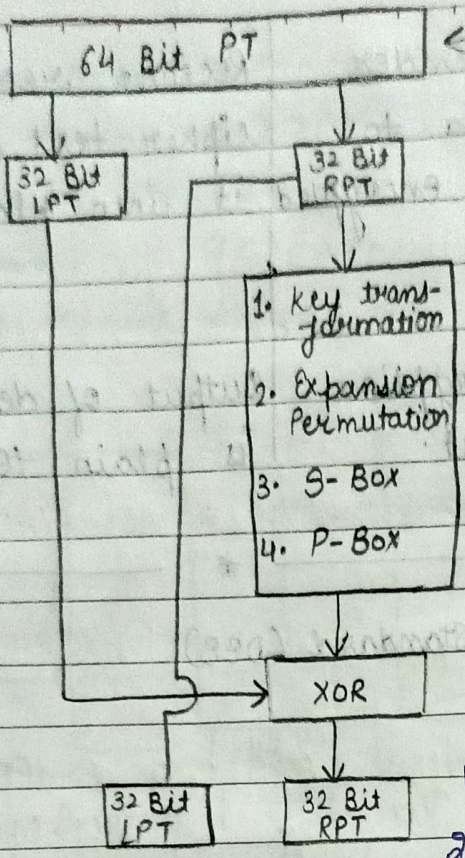
2.



IP → Initial Permutation
FP → Final Permutation
LPT → Left Plain Text
RPT → Right Plain Text

DOMS | Page No.
Date / /

3.



← after applying IP we get this

- Block cipher algorithm
- Converts plain text to cipher text.

Has total of 16 Rounds.

Text Size = 64 bits

Key Size = 48 bits

8 bits gone for parity & 8 for rearrangement

In each round 4 steps are performed:

1. dividing bits into 2 parts 32 bit each.
2. Bit Shuffling.
3. Non-linear Substitution
4. Exclusive OR operation

It is a symmetric key encryption algorithm.

Key discarding process: Original key size is 64 bit. Every 8th bit of original key is discarded. Finally we will receive 56 bit key.

Step to convert into 56 bit ←

Steps for DES:

1. 64 bit PT is given to initial permutation fun (IP)
2. IP is performed on 64 bit PT after that PT is divided into two halves of 32 bits named as LPT & RPT.
3. Each LPT & RPT perform 16 rounds of encryption process.

4. LPT & RPT rejoint & final permutation is performed on combined block.
5. After final permutation the resultant text the cipher text of 64 bits.

For diagram 3

1. Initial Permutation: It performs only once. In this bit sequence has been changed as per IP table.
[Rearranging of bits / change the position]
eg: 10001000

1	2	3	4	5	6	7	8
4	5	8	2	1	6	3	7

⇒ 01001000

eg: 1st bit take the the 20th position, 58th bit take the 1st position.

2. Output of IP is divided into two parts LPT & RPT.
16 rounds of encryption:
- Key Transformation: It has two sub parts. 1. Key bit Shifted per round 2. Compression permutation.
- 56 bit is divided into two halves each of 28 bit
- Circular left shift is performed on each half.

- Shifting of bit is dependent on rounds.
For round no 1, 2, 9 & 16 shift is done by 1 position otherwise it is performed by 2 positions.

Compress permutation:

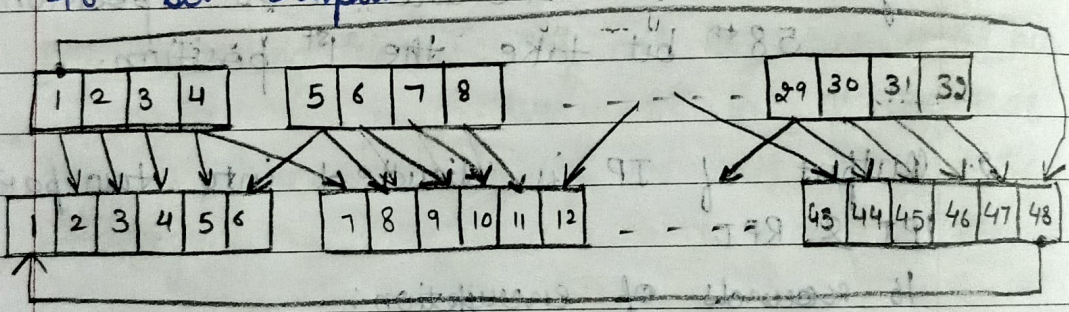
- 56 bit input with bit shifting positions.
- It generates 48 bit key.
- It will drop 9, 18, 22, 25, 35, 38, 48 & 54 (8) bits.

- Expansion Permutation [Increase in bits]

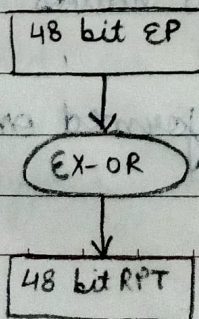
Implement on

- 32 bit RPT of IP is expanded to 48 bits.
- Steps to perform:

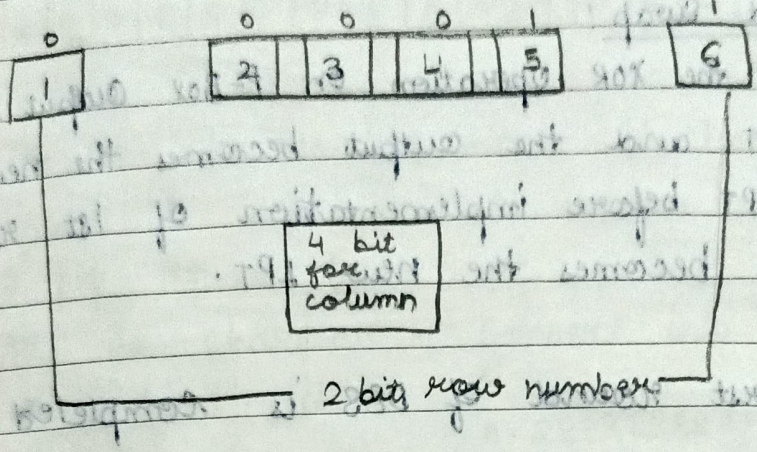
1. 32 bit RPT is divided in 8 blocks of size 4 bits.
2. Each 4 bit is expanded to 6 bits & produce 48 bit output.

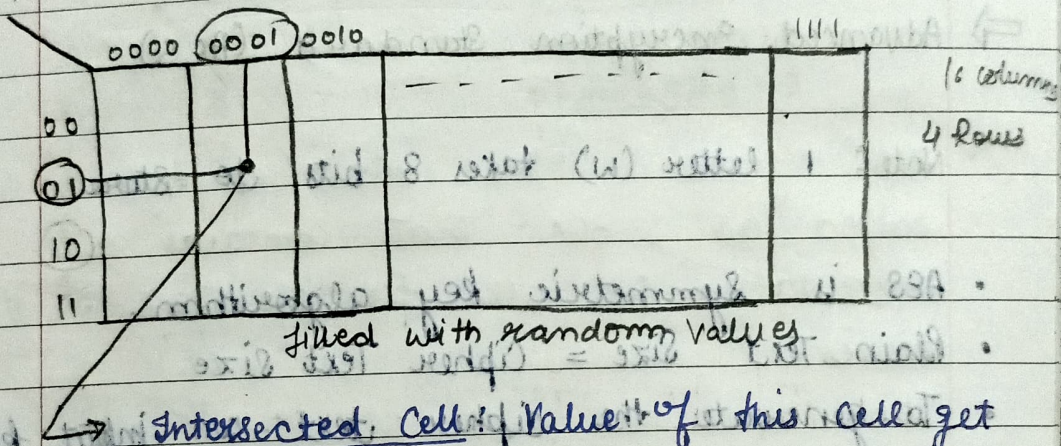


3 XOR the results of step 2 that is 48 bit then it generate 48 bit RPT



4. Convert 48 bit RPT into 32 bit with the help of S-Block





→ Intersected Cell : Value of this cell get changed with the above given value.

5. Output of S-Box is given to P-Box (Permutation Box)

6. 32 bit is permuted with 16 X 2 permutation table :

	0	1	2	3	4	5	6	7	8 columns
eg 1	5	2	4	6					
2									01 0011

As per this example bit received from

the S-Box at 5th bit position takes the 1st position after P-Box Implementation.

XOR and Swap!

Perform the XOR operation on P-Box output & 32 bit LPT and the output becomes the new RPT. And RPT before implementation of 1st round of DES becomes the new LPT.

The first round of DES is completed.

⇨ Advanced Encryption Standard (AES)

Note: 1 letter (w) takes 8 bits to store.

- AES is Symmetric key algorithm.
- Plain Text Size = Cipher Text Size
- To generate the cipher text an input key is also required.
- The data length is accepted by an AES are 128, 192 & 256 bits.
- And supporting three different keys respectively 128, 192 & 256 bits.

AES consist of multiple rounds of processing different key bits like 10 rounds for processing 128 bits, 12 for 192 & 14 for 256.

DOMS | Page No.
Date / /

Plain text transform in matrix form for eg: GOD IS ONLY ONE

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
G	O	D	I	S	O	N	L	Y	O	N	E	Z	Z	Z	Z

- We have to use 4x4 matrix 16 characters equal to 128 bits. It means one cell 8 bits at a time.
- All the characters convert into numbers.

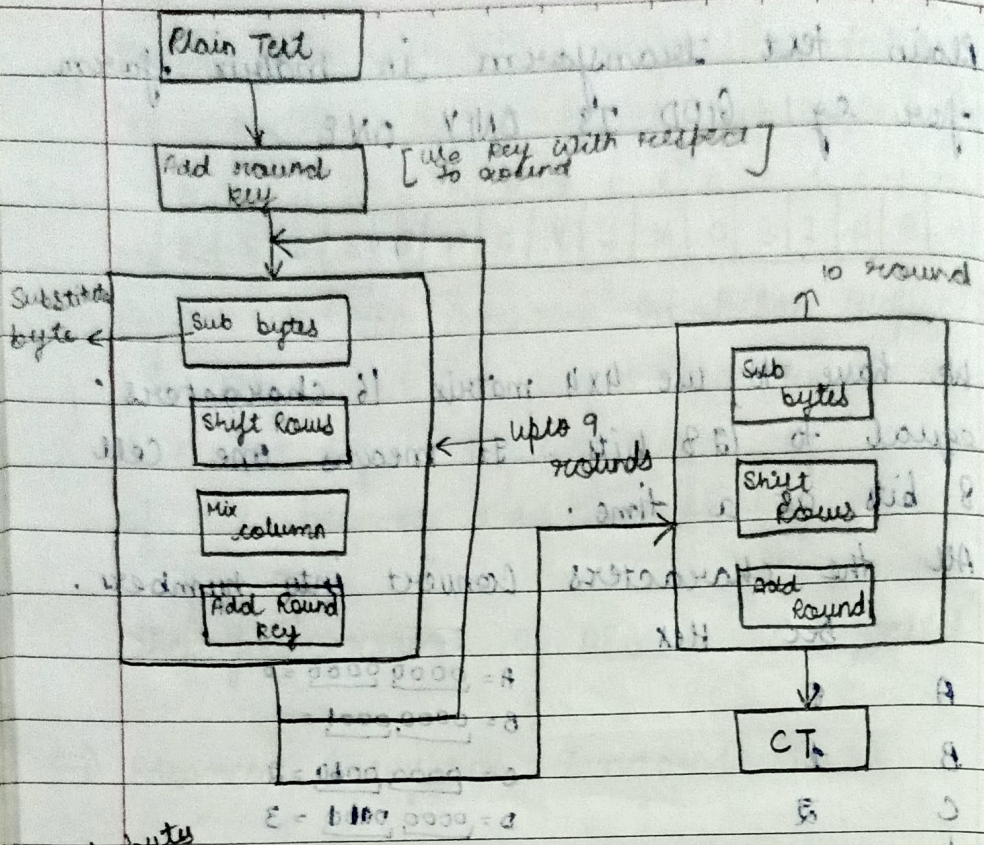
	Dec	Hex
A	0	A = 0000 0000 = 0
B	1	B = 0000 0001 = 1
C	2	C = 0000 0010 = 2
⋮	⋮	⋮
Z	25	Z = 0001 1001 = 19

eg: 4x4

If we fill row wise then it is row major order, if we fill column wise, then it is column major order. ⟹ It is called state matrix

- The first four bytes of 128 bit I/P block occupy the 1st column in the 4x4 matrix of 16 cells. The next 4 bytes occupy the 2nd column.

16 bytes = 128 bits.



Sub bytes

- AES defines a 16 X 16 matrix of byte values, called as S-BOX. That contains a permutation of all possible 256 8 bit values.
- Each individual byte of State matrix is mapped into a new byte in the way (write) represented below.
- The left most 4 bits of the byte are used as a row value & the right most 4 bits are used as the column value.

S-BOX

	0	1	2	3	4	5	6	...	F
0	63	7C	77	7B	F2	FF	←		FE
1	CA	82	79	7D	FA	98			EF
2	-	-	-	-	-	29	-		-
⋮	-	-	-	-	-	-	-		-
F	-	-	-	-	-				DE

(16X16)

14 → 1 (row) 4 (column)

eg:

14	28	FF
FA	29	DE

eg:

00	04	11	1F
01	05	12	25
02	0F	13	2F
03	10	14	FF

⇒

63	F2	82	98
7C	FF	79	EF
77	FF	7D	29
7B	CA	FA	DE

Shift Row Transformation :

Rules for Shifting Row

1st Row → No Shift
IInd Row → 1 Byte Circular Shift
3rd Row → 2 Byte Circular Shift
4th Row → 3 Byte Circular Shift

eg:

	0	1	2	3
0	00	01	02	03
1	10	11	12	13
2	20	21	22	23
3	30	31	32	33

→

	0	1	2	3
0	00	01	02	03
1	11	12	13	10
2	22	23	20	21
3	33	80	31	32

Mix Column : Each byte of a column is mapped into a new value that is a function of all 4 bytes in that column

Pre defined Matrix:

	0	1	2	3
0	02	03	01	01
1	01	02	03	01
2	01	01	02	03
3	03	01	01	02

Digital Signature: