6720 $\sqrt{p}\sqrt{x} = 10-5x$

$60\sqrt{x \times 13} =$

CNS - Part 1

CLOUD MODEL TYPES

1) Public Cloud Model

$2x+5+2\sqrt{x}\sqrt{x+5} = 25$

$2x+2\sqrt{x}\sqrt{x+5} = 20$

$2\sqrt{x}\sqrt{x+5} = 20-2x$

$\sqrt{x}\sqrt{x+5} = 10-5x$

(Rivest, Shamir & Adleman)

Harman Singh Jolly
IT-E
3545203116

RSA Cryptosystem Algorithm

→ Public key algorithm
- Key 1 (Public) Encryption
- Key 2 (Private) Decryption

→ Asymmetric Encryption

Algorithm

1) Choose 2 large Prime nos P and Q such that $P \neq Q$.
2) Calculate $N \leftarrow P \times Q$.
3) Choose E (Public key) such that E is not a factor of $(P-1)$ & $(Q-1)$
4) Choose D (Private Key) such that $(D \times E) \% (P-1)(Q-1) = 1$
5) Cypher Text $(CT) = (P.T)^E \% N$
6) Plain Text $(P-T) = (C-T)^E \% N$

Eg.

$N = P \times Q$.

$E = (P-1)(Q-1)$

D such that $(D \times E) \% (P-1)(Q-1) = 1$

29/11

Authentication | Confidentiality
Encryption | Non-repudiation
Integrity

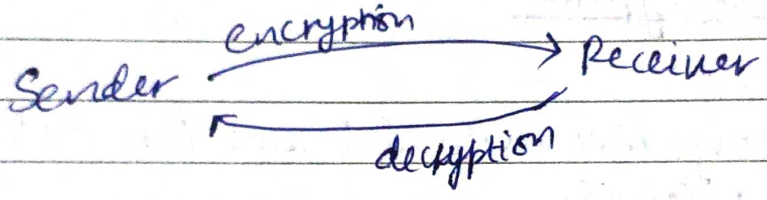
AEICN

DELTA Page No.
Date / /

UNIT-1

Basic Cryptography Techniques

1) **Encryption** - Encryption is to convert the data is some unreadable form. Helps in protecting th privacy while sending the data from sender to receiv

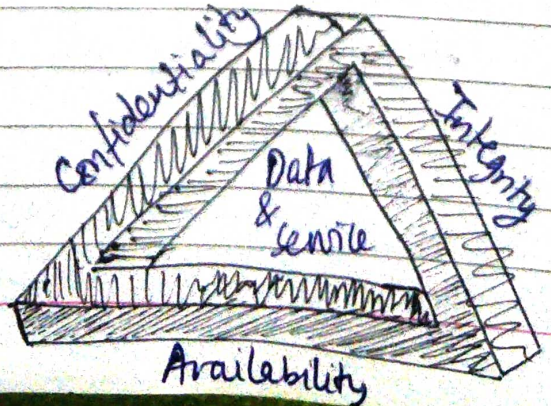


Extra info required for encr & decryp is ca 'key'.

2) **Authentication** - It ensures that the message was orig from the senders claimed in the messa This is some basic level of password clearance.

3) **Integrity** - Communication system can face the loss of integ of message being sent from sender to receiv It should ensure that the messages received are not alter anywhere on the path. Done by the concept of cryptograph

4) **Non-repudiation** - What if sender denies sending a messa So, to prevent this from happening one should achieve digital signatures



EAIN || CANIE

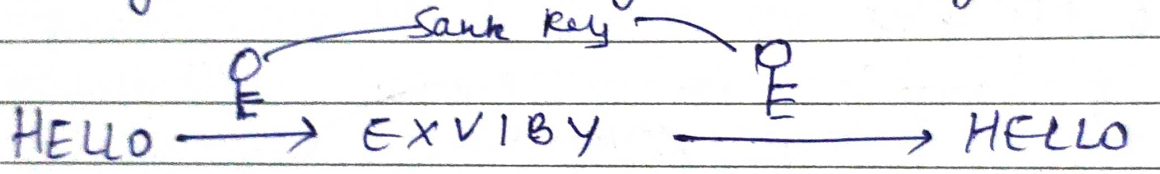
DELTA Page No. Date / /

Types of Cryptography

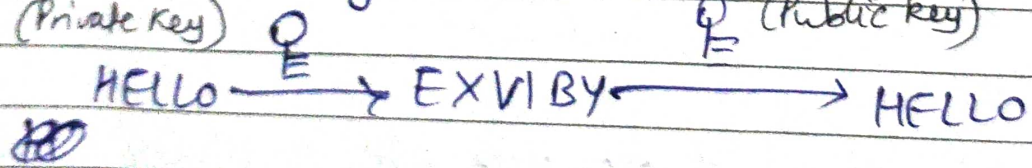
There are 3 types of cryptography techniques:-

- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions.

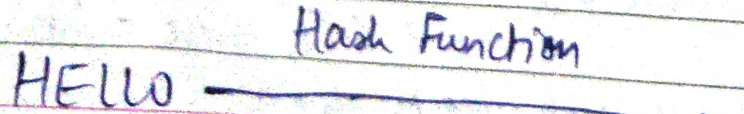
1) Secret Key Cryptography - It uses just a single key. The sender applies a key to encrypt a message while receiver applies the same key to decrypt the message. Also called "Symmetric Encryption"



2) Public Key Cryptography - It uses two keys wherein either the sender or receiver encrypts it with its private key & then receiver decodes it with its public key.



3) Hash Functions - This doesn't involve any key but uses fixed length hash value that is computed on the basis of plain text message.
Used to check integrity of message or to check that they are not altered.



The OSI Security Architecture

- The open system Interconnection (OSI) security architecture provides a systematic framework for defining security attacks, mechanisms and services.

- Defines a systematic way of defining and providing security requirements. Provides a useful, abstract, overview of concepts. Consider 3 aspects of Information security:-

a) Security Attack - These are classified as either passive attacks which include unauthorized reading of message or traffic analysis, and active attacks such as modification of messages or files and denial of service.

b) Security Mechanism - Any process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack. Eg- Encryption algo, digital signature and authentication protocols.

c) Security Services - It includes authentication, access control, data confidentiality, data integrity, non-repudiation and availability.

a) Security Attack - Types:

i) Active attack ⇒ An active attack attempts to alter system resources or affect their operation. Here, modification of original message is done. Can be prevented easily.

a) Interruption
b) Modification
c) Fabrication (DOS Attack)
d) Masquerade
e) Replay

ii) Passive attack ⇒ Here, the attacker attempts to obtain information. He/she doesn't pretend or perform any modification in data. i.e they are harder to detect.

a) Traffic Analysis
Hacker tries to analyse message using a pattern that provides some clues regarding the communication

b) Release of message content to others

c) Masquerade

b) Security Services (X.800 defines a security service provided by a protocol layer) CIANE

Confidentiality
Authorization
Non-Repudiation
Integrity
Encryption

i) Authentication - Assurance that communicating entity is the one that it claims to be.

a) Peer-to-Peer - Used in association with a logical connection to provide confidence in the identity of the entities connected.

b) Data-Origin - Provides assurance that the source of received data is as claimed, in a connectionless transfer.

ii) Access Control - Prevention of unauthorized use of resource.

iii) Data Confidentiality - Protection of data from unauthorized disclosure.

a) Connection-Confidentiality - Protection of all user data on a connection.
b) Connectionless Confidentiality - Protection of all user data on single data block.
c) Selective-Field Confidentiality - Confidentiality of selected fields within the user data on a connection or in a single block.
d) Traffic-flow Confidentiality - Protection of all the info that might be derived from observation of traffic flows.

iv) Data Integrity - The assurance that data sent are exactly the same when received by authorized entity.

a) Connection Integrity with Recovery: Provides integrity of all user data on a connection with recovery options in case of ~~of~~ modification detection.
b) Connection Integrity w/c Recovery: Provides integrity of all user data with only detection w/c recovery.
c) Selective-Field Connection - Provides integrity of selected fields within user data of data block transferred over a connection.
d) Connectionless Integrity - Provids integrity of a single connectionless data block
e) Selective-field connectionless - Provides integrity of selected field with a single connectionless data block.

v) Non-Repudiation - Provides protection against denial by one of the entities involved in all or part of the communication.

a) Non-Repudiation Origin - Proof that message was sent by specified party

b) Non-Repudiation Destination - Proof that msg was received by specified party.

c) Security Mechanisms

i) Specific Security Mechanisms - May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

a) Encipherment : Use of mathematical algos to transfer data into a form that is not readily intelligible.

b) Digital Signature - Data appended to data block that allows recipient to prove the source & integrity of data block.

c) Authentication Exchange - Mechanisms intended to ensure identity of an entity by means of information exchange

d) Traffic Padding - Insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

e) Routing Control - Enable selection of a particular physical route for certain data type and allows routing changes.

ii) Pervassive Security Mechanisms – Mechanisms that are not specific to any particular OSI security service or layer.

a) Security Label – The marking bound to a resource (may be a data unit) that names or designates the security attributes of that resource.

b) Security Audit Trail – Data collected & potentially used to facilitate a security audit.

c) Security Recovery – Deals with requests from mechanisms, like event handling, management functions & takes recovery actions.

d) Event Detection – Detection of security-relevant events.

Encryption Techniques

Conventional Encryption

→ Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using same key. There are 2 types of attacks on encryption algo :-

- Cryptoanalysis: Based on properties of encryption algorithm
- Bruteforce: Based on trying all possible keys.

→ Substitution Techniques

① Ceaser's Cypher-

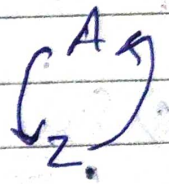
Encryption ⇒ $C = E(k, p) = (p + k) \bmod 26$.

Decryption ⇒ $P = D(k, C) = (C - k) \bmod 26$

Eg

Plain Text = HELLO WORLD

$k = 3$.



So,

Cypher Text = KHOORZRUOG

② Playfair Cypher - We make 5×5 table incase of a plaintext with no numbers and a 6×6 table incase of numbers in plaintext.

Eg

Keyword = PLAYFAIR

Plain txt = HELLO BRO

HE	LX	LO	BR	OX

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

KG | YM | RV | CB | SV

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

W	X	Y	Z
22	23	24	25

DELTA Page No. Date

(3) Hill Cypher – Also called polygraphic substitution cypher

Plain text = DOG

$[3 \quad 14 \quad 6]$ or $\begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix}$

Encryption

$$Key = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

$$C = (K \times P) \bmod 26$$

$$\begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} \quad \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} = \begin{bmatrix} 22 \\ 11 \\ 24 \end{bmatrix}$$

3×1 3×3

18 + 6 + 336 = 360

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} = \begin{bmatrix} 22 \\ 11 \\ 24 \end{bmatrix} \quad \begin{bmatrix} W \\ L \\ Y \end{bmatrix}$$

3×3 3×1

Decryption

$$P = (K^{-1} \times C) \bmod 26.$$

$$A^{-1} = \frac{1}{|A|} \text{Adj } A$$

(4) One time Pad (Vernam Cipher) = One type pad (key)

Length of plain text = Length of key

Encryption

PT → H E L L O

	7	4	11	11	14
Key →	23	12	2	10	11
Add	30	16	13	21	25
Subtract 26 (if >)	4	16	13	21	25
convert according to alphabet	E	Q	N	V	Z

HELLO ⇒ EQNV2

PT = HELLO

Key = XMCKL

CT. E Q N V Z

	4	16	13	21	25
key →	23	12	2	10	11
(Subtract) CT − key →	−19	4	11	11	14
Add 26	7	4	11	11	14

⇒ HELLO ✓

→ Transposition Techniques

(1) Rail Fence Cypher

* Rearrange of plain text (order of) and there is no replacement / substitution

Eg : welcome to my session (Plaintext)

W L O e e y e s o
e c m t m s s l n

wloeoyesoecmtmssln (cypher text)

(2) Row Transposition Cipher

Eg Plant text : Welcome to my session
key : 32451 (unique nos from 0 to 9)

60

3	2	4	5	1	(Key)
W	E	L	C	O	
M	E	T	O	M	
Y	S	E	S	S	
I	O	N	X	Y	

↓ DUMMY

Cypher Text →

1	2	3	4	5
O	E	W	L	C
M	E	M	T	O
S	S	Y	E	S
Y	O	I	N	X.

⇒ OMSYEESOWMYILTENCOSX.

Block Cipher

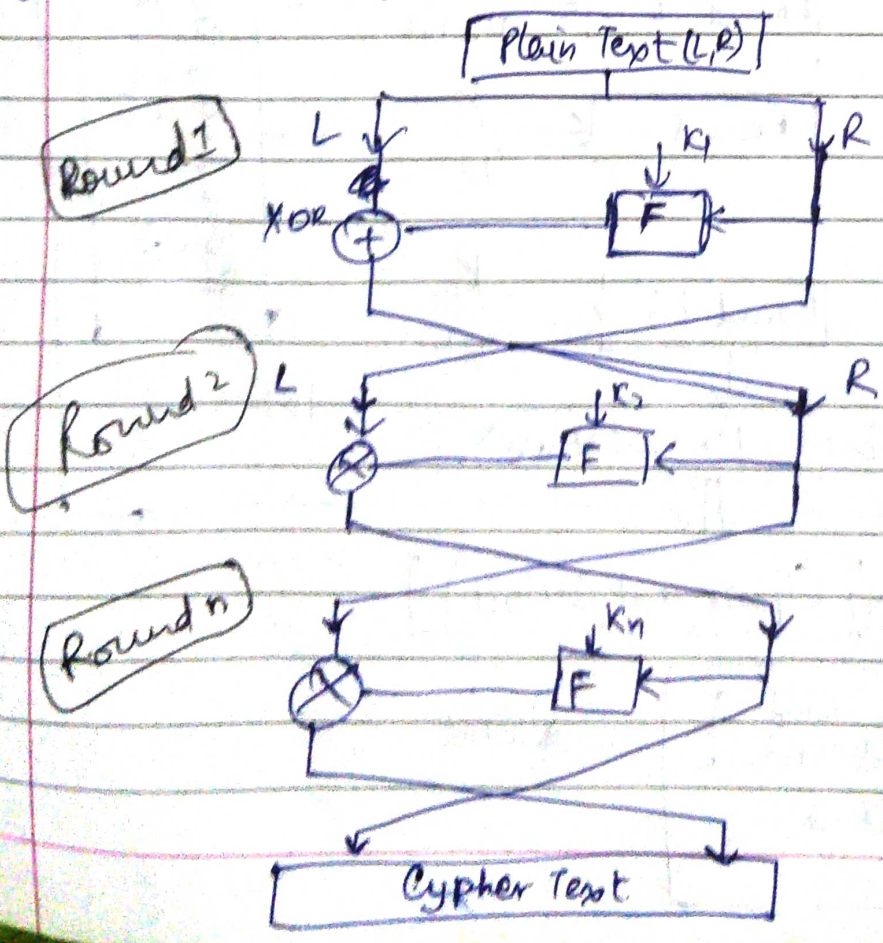
⇒ An encryption/decryption scheme in which a block of plaintext is treated as a whole and is then used to produce a cipher block of equal length.

All blocks cypher follow one similar structure called the 'Feistel Structure'

(1) Divided in two equal halves → * Consists of no. of identical rounds of processing
* A substitution is performed at each round on half of the data being processed
* Then a permutation is done that changes the two halfes.

Fiestal Cipher Structure → A design model from which many diff. block ciphers are derived. DES is an example.

→ Any system based on Fiestal cipher structure uses the same algorithm for encryption & decryption.



(1) Plaintext $\leq 2^L$
(2) No. of Round
(3) No. of subkeys.
(4) Swapping

→ The essence of this is to develop a block cipher with a key length of 'k' bits and block length of 'n' bits, giving 2^k possible transformation

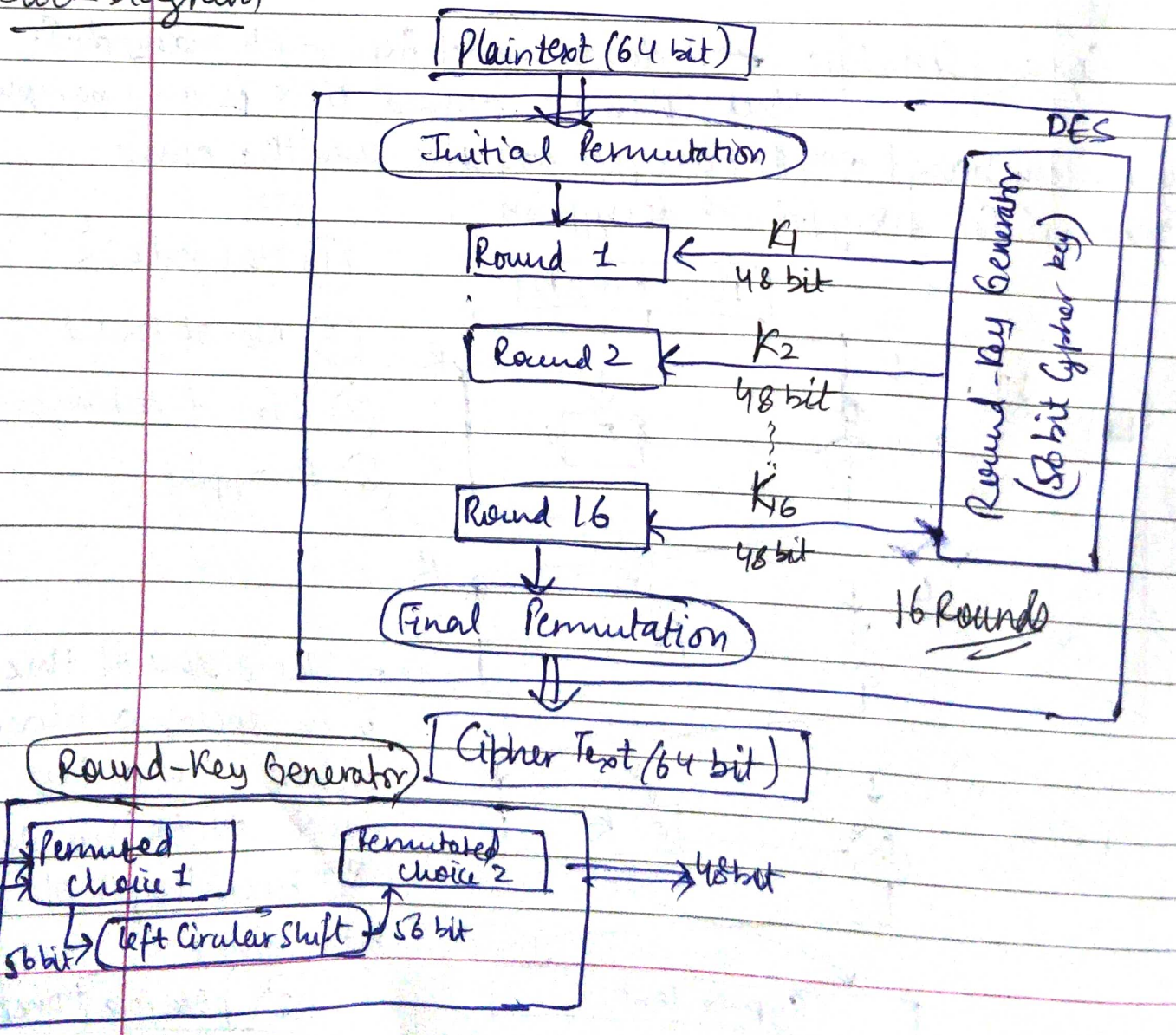
DES (Data Encryption Standard)

→ DES is an outdated symmetric-key method of data encryption.

→ It uses the same key to encrypt and decrypt the message, so both sender and receiver must know and use the same private key.

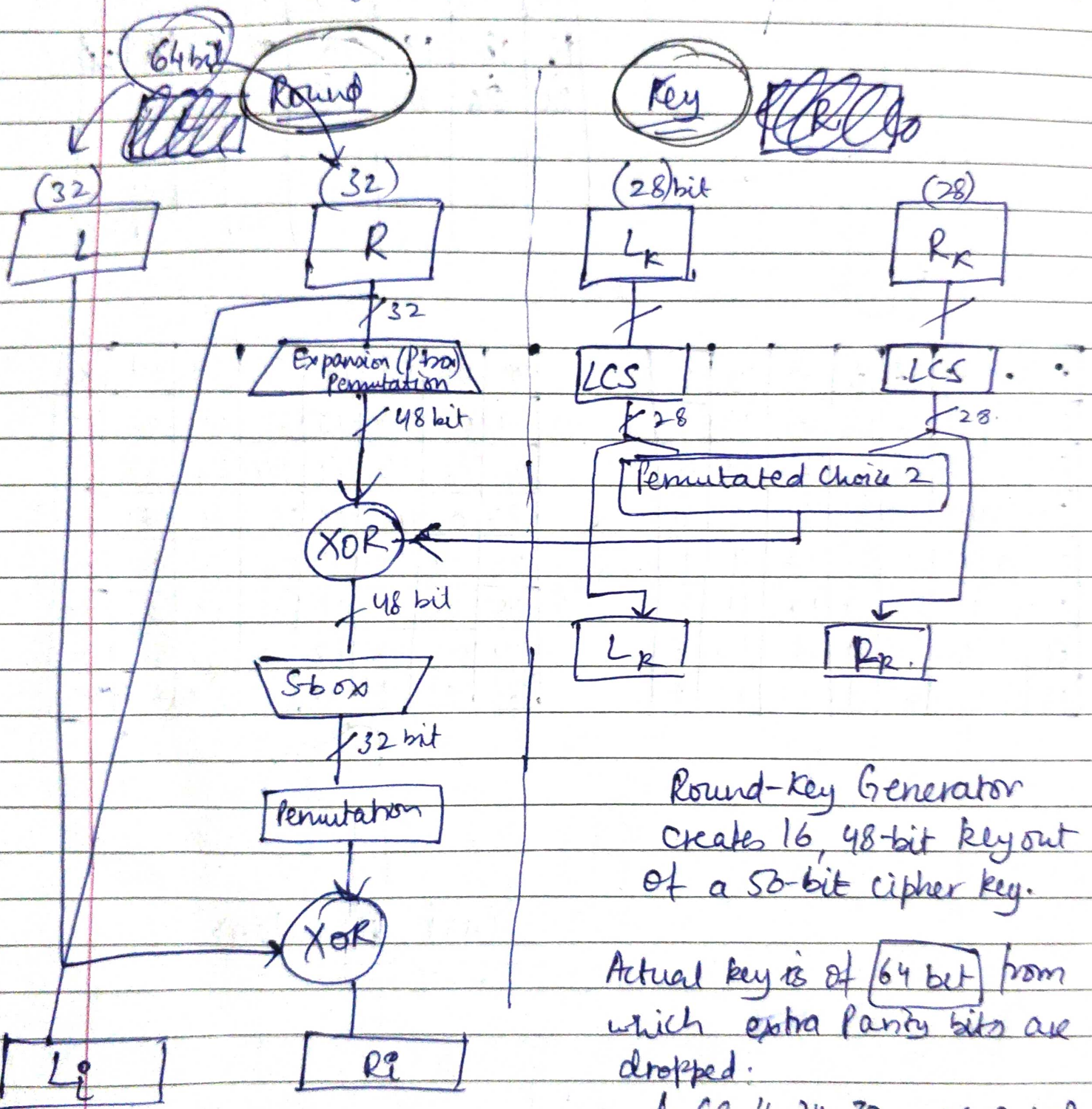
Block size ⇒ 64 bits, No. of Rounds = 16 Rounds, Key size = 64 bit
No. of subkey ⇒ 16 subkeys, sub-Key size = 48 bits., Cipher Text=64 bi

Block Diagram



Round function

DES function applies 48-bit key to the rightmost 32 bits to produce 32 bit output



Round-Key Generator creates 16, 48-bit key out of a 56-bit cipher key.

Actual key is of 64 bit from which extra Parity bits are dropped.

↳ (8, 16, 24, 32, 40, 48, 56, 64)

Multiple of 8.

DELTA Page No.
Date / /

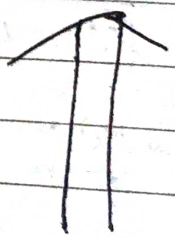
Initial Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

⇒

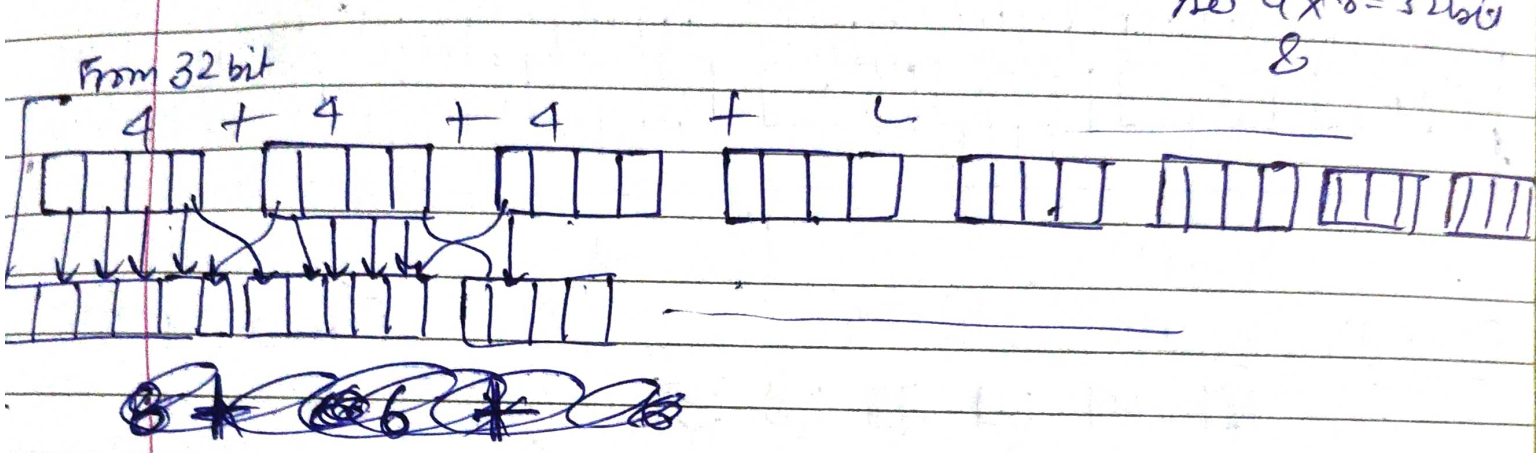
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25



Final Permutation

Expansion P-box

Since R_{I-1} is 32 bit input and K_I is a 48 bit, we expand R_{I-1} to 48 bits.



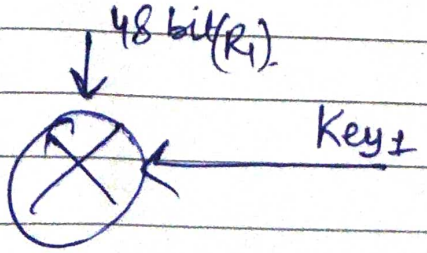
6 + 6 ... & true (6×8) ⇒ 48 bits

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Added 1 bit

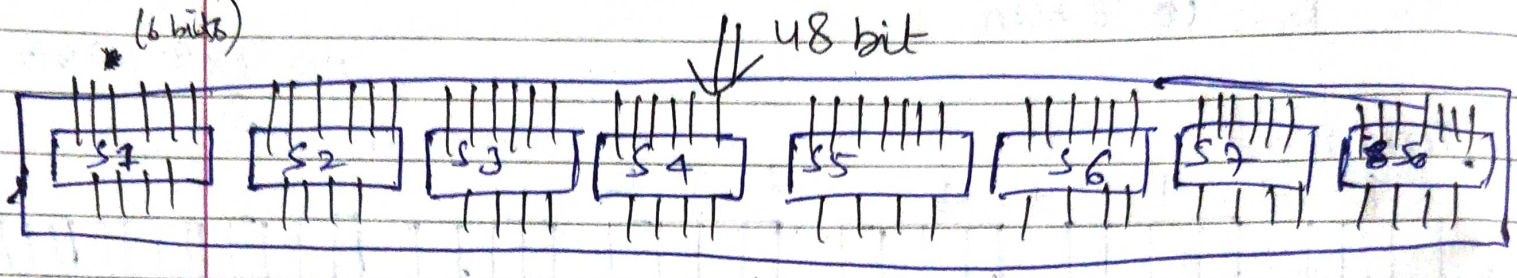
Added 1 bit

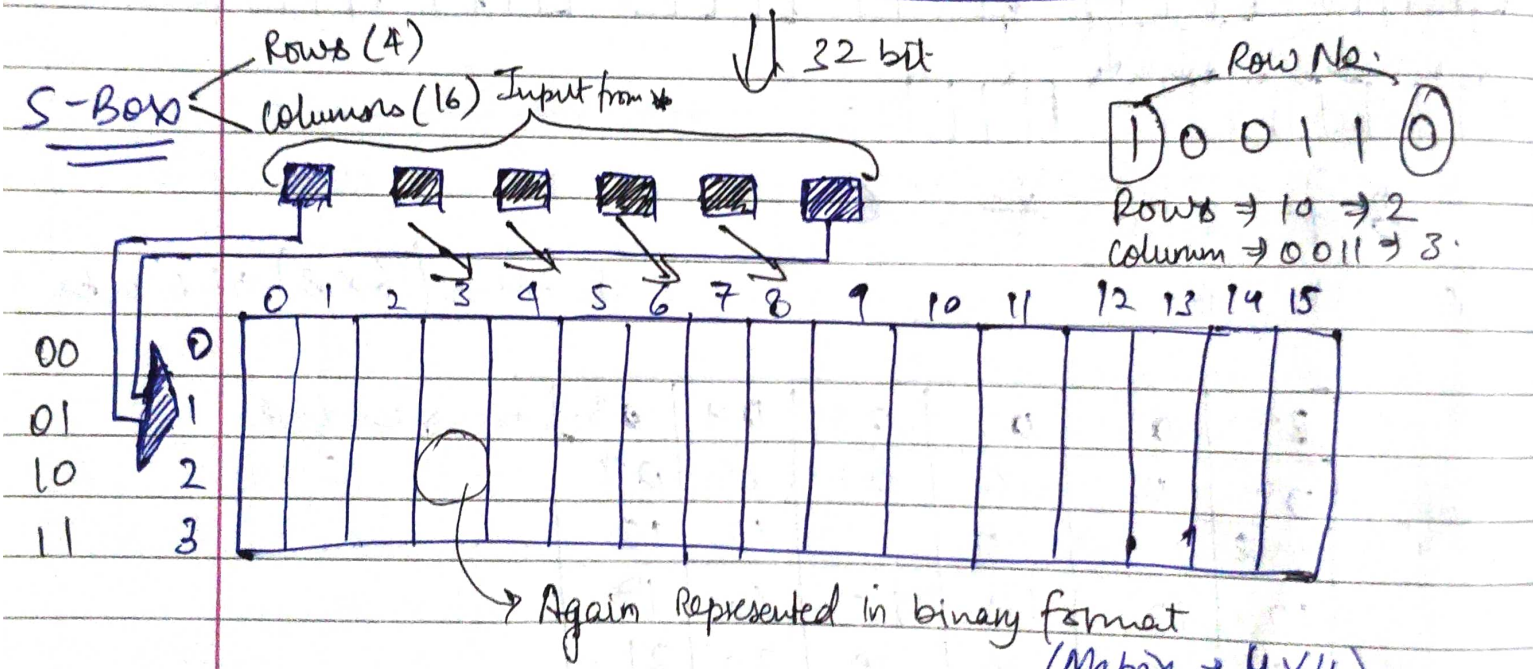
Whitener ⇒ It is the XOR operation b/w 48 bit key and 48 bit output from expansion P-box.



S-box (Substitution Box)

Contains 8 S-boxes with 6-bit input & 4 bit output.





So, like this we will be having 8, S-boxes. ([redacted])

Decryption

→ The same algorithm is used as encryption.

→ Reversed order of keys is used ($K_{16} \dots K_1$).

CNS Part-2

DELTA Page No. Date

Properties

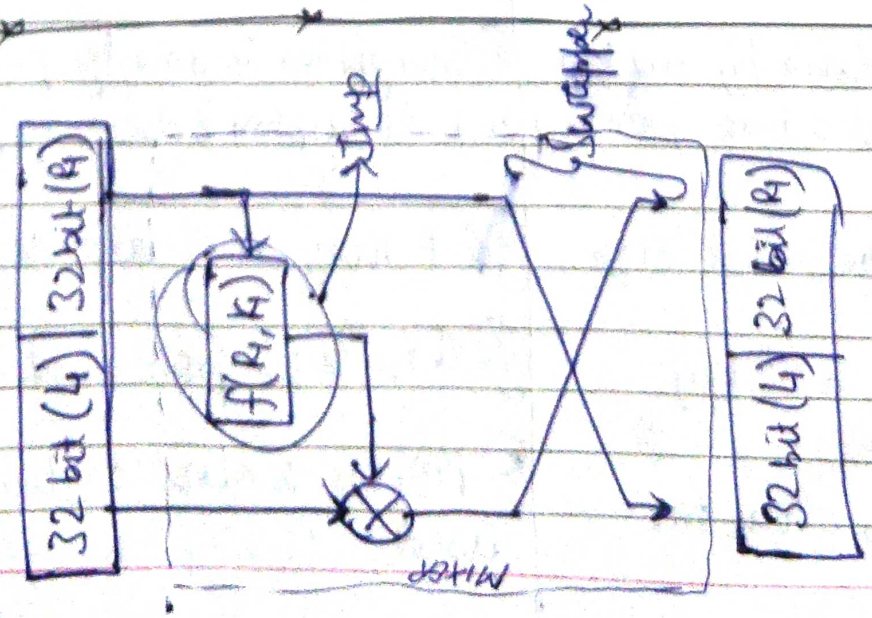
1) Avalanche Effect - A small change in ~~cipher~~ plain text causes a great deal of change in cipher text.

2) Completeness - Each bit of the cipher text depends on many bits of plain text
   - Diffusion (P-box)
   - Confusion (S-box)

Strength of DES

1. Use of 56 bit Keys - (a) There are approx 2^{56} keys.
   (b) Broken by Electronic Frontier Foundation in 1998.
2. Nature of DES - Cryptoanalysis is possible by exploiting the characteristics of DES. But still no one has so far succeeded in discovering the fatal weakness in the S-boxes.
3. Timing Attack - Info about key or plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various cipher texts.

Rounds



Symmetric Key

1. Same key or one key is used for encryption & decryption
2. Encryption is done by one key and decryption is also done by same key
3. C-T of same & less size.
4. There is a problem of key exchange.
5. Process is fast as only one key is used.

Asymmetric Key

1. Different keys are used (private and public)
2. Encryption is done by public key and decryption is done by private key
3. C-T may be of large size.
4. There is no problem of key exchange
5. Process is slow as two key are used.

Asymmetric Encryption Techniques

1) RSA Algo (Rivest, Shamir, Aldeman)

→ Public key algorithm
- key 1 (Public) Encryption
- key 2 (Private) Decryption.

Algo

1) Consider two large prime numbers (P, q)
2) Calculate, $n = p \times q$
   $\phi(n) = (p-1)*(q-1)$
3) Assume E, such that $1 < e < \phi(n)$ and $\gcd(E, \phi(n)) = 1$
   or E should be coprime to $\phi(n)$
4) Assume D, such that $DXE \equiv \mod(\phi(n))$
   so $DXE \equiv 1 \mod(\phi(n))$
   or $DXE \bmod(\phi(n)) = 1$ ✓
5) Cipher Text (CT) = $(P\text{-}T)^E \% n$
6) Plain Text (P-T) = $(C\text{-}T)^D \% N$

P=3, Q=5,

so $n = p*q = 15$, $\phi(n) = 2*4 = 8$.

so $\gcd(e, \phi(n)) = 1$

3, 5, 7 as 3 & 8 are co-prime

Assuming E=3

DELTA Page No.
Date / /

e = 3

So $d \times e \bmod \phi(n) = 1$

$(d \times e) \% 8 = 1$

$(d \times 3) \% 8 = 1$

so d = 3 hence $(3 \times 3) \% 8 = 1$ ✗ Not good

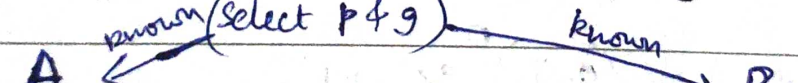
so now as small nos where considered, e & d are equal.

C.T. ⇒ Plain text is considered to be = 4

So C-T ⇒ $(4)^3 \% 15 \Rightarrow 4$ ✓

P-T ⇒ $(4)^3 \% 15 \Rightarrow 4$ ✓ → No security but answer matches.

b) Diffie-Hellman Key Exchange



$R_1 = g^x \bmod (p)$ → R_1

$R_2 = g^y \bmod (p)$ ← R_2

$K = (R_2)^x \bmod (p)$

$K = (R_1)^y \bmod (p)$

Shared Key

$a=4, b=3$

$K_A = y^a \bmod p$ $\quad$ $x_b = x \bmod p$

* Not an encryption algorithm
* It is used to exchange secret/symmetric key.

Algorithm

Here $Q = P$ & $\alpha = G$

1) Consider a prime number 'Q'
2) Select α such that α is primitive root of 'Q'
   $\alpha < Q$.
3) Assume X_A (Private key for User A) where $X_A < q$ and calculate Y_A (Public key for User B) $\boxed{Y_A = \alpha^{X_A} \bmod Q}$
4) Assume X_B (Private key for User B) where $X_B < q$ and Calculate Y_B (Public key for User A) $\boxed{Y_B = \alpha^{X_B} \bmod Q}$

Key Generation

A: $K = (Y_B)^{X_A} \bmod Q$ $\quad$ should by equal $\quad$ B: $K = (Y_A)^{X_B} \bmod Q$.

der $\quad$ Receiver

TYPES OF CRYPTANALYSIS ATTACK

1) Ciphertext Only Attack - Attacker has access to only ciphertexts. No access to corresponding plaintexts is given. COA is successful only when the corresponding plaintext can be found from a given set of ciphertexts.

2) Known Plaintext Attack - The attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt rest of the ciphertext using this information.

3) Chosen Plaintext Attack - The attacker has the text of his choice encrypted. So, he has the ciphertext-plaintext of his choice. Simplies the task of find key.

4) Dictionary Attack - Attacker builds a dictionary of CTs and corresponding PTs that he/she has learnt over period of t. He refers to dictionary to find the PT if in future he gets CT.

5) Brute-Force Attack - Attackers tries to determine the key by attempting all possible keys. All possible options for keys are tried and time to complete it is very long.

6) Birthday Attack - Attacker uses the senders birthday combination as the key to decrypt the text.

7) Man-In-Middle - Eavesdropping is a form of MIM attack. Attacker intercepts the request of public key and sends his public key instead. Thus whatever host A sends to B, the attacker can read it.

AES (Advanced Encryption Standard)

⇒ AES performs all its computation on bytes rather than on bits

so, AES treats 128 bits of P.T as a block of 16 bytes (8 bits = 1 byte)

1 word = 32 bits.

Plain Text ⇒ 128 bits / 16 bytes. so 4 words.
No. of rounds ⇒ 10 Rounds.
Key Size ⇒ 128 bits / 16 bytes. so 4 words.
↳ No. of sub-keys ⇒ 44 subkeys
↳ Each subkey size = 32 bits / 4 bytes so 1 word.

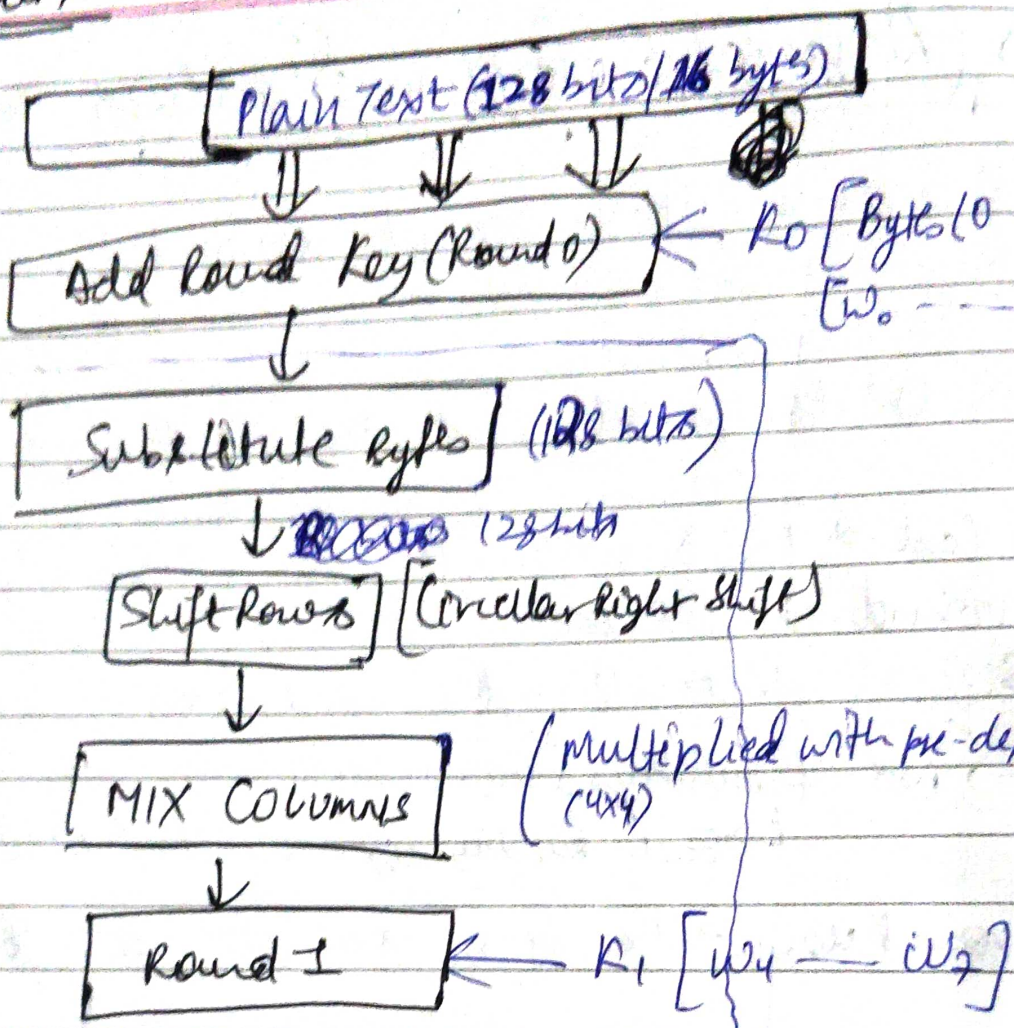
Each round uses ⇒ 4 subkeys (so 4 × 32 = 128 bits or 16 bytes)

Pre-Round Calculation → 4 subkeys used

Hence, Rounds × Subkey used in each round
10 × 4 ⇒ 40 + 4 = 44 subkeys.

Cipher Text ⇒ 128 bits / 16 bytes.

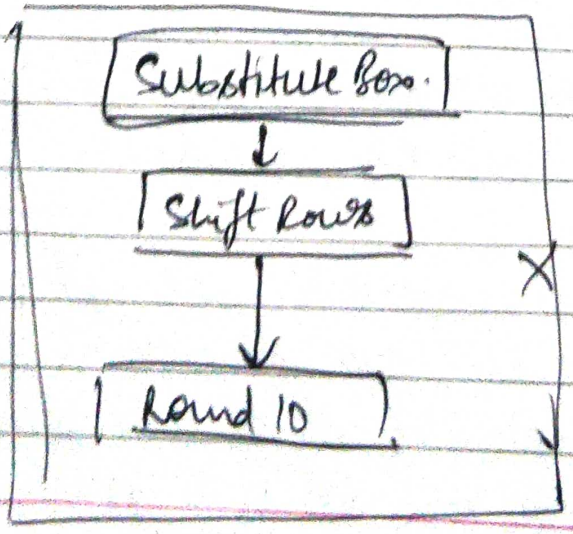
Block Diagram



Round 0 = $W_0 - W_3$ (K_0)
Round 1 = $W_4 - W_7$ (K_1)
Round 2 = $W_8 - W_{11}$ (K_2)
= $W_{12} - W_{16}$ (K_3)
[.]
Round 10 = $W_{40} - W_{43}$ (K_9)

This round function is processed 10 time

Only Sub 10th Round



Main Text

→ 1 byte = 8 bits

Input ⇒

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

} 16 bytes (128 bits)

Intermediate Results ⇒ (State Array)

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

1 word.

Output ⇒

O_0	O_4	O_8	O_{12}
O_1	O_5	O_9	O_{13}
O_2	O_6	O_{10}	O_{14}
O_3	O_7	O_{11}	O_{15}

Key ⇒

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

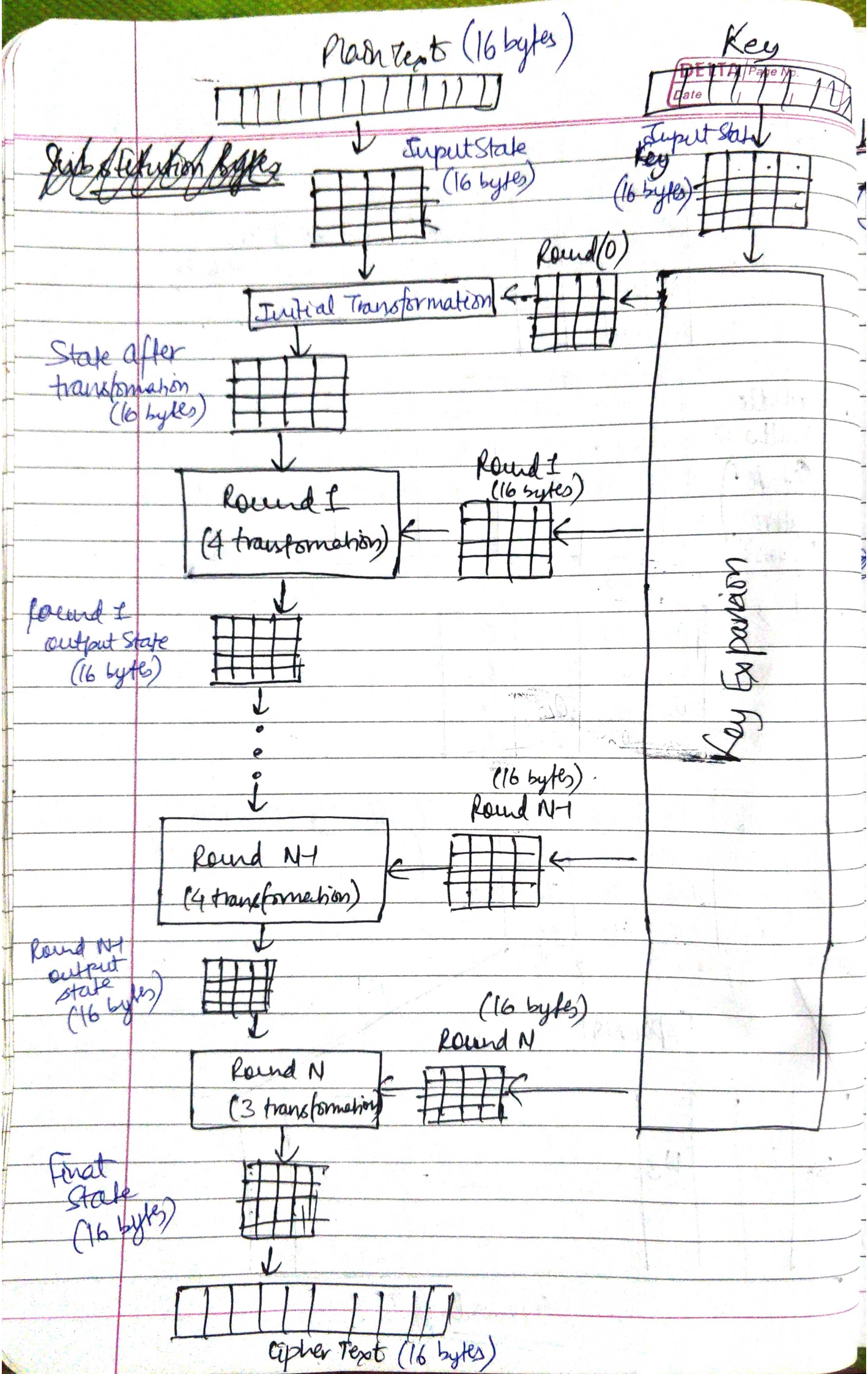
} 128 bits or 4 words

W_1 W_2 W_3 W_4

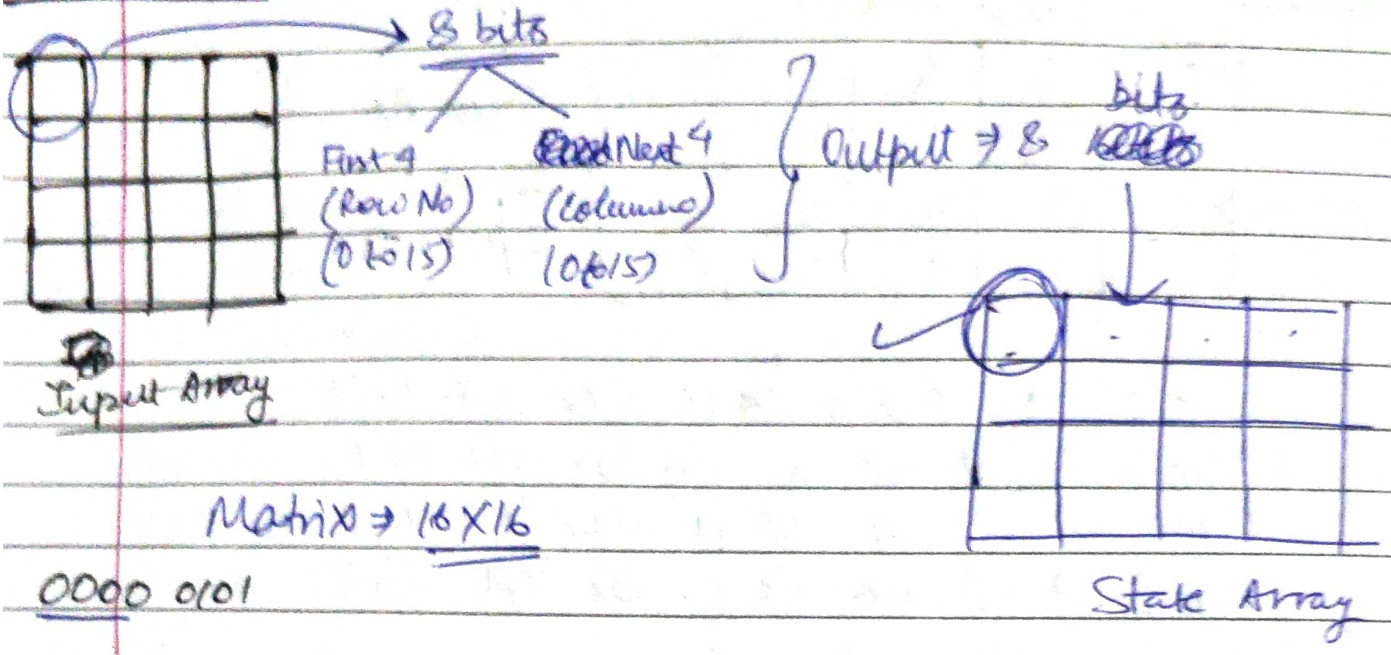
Expansion

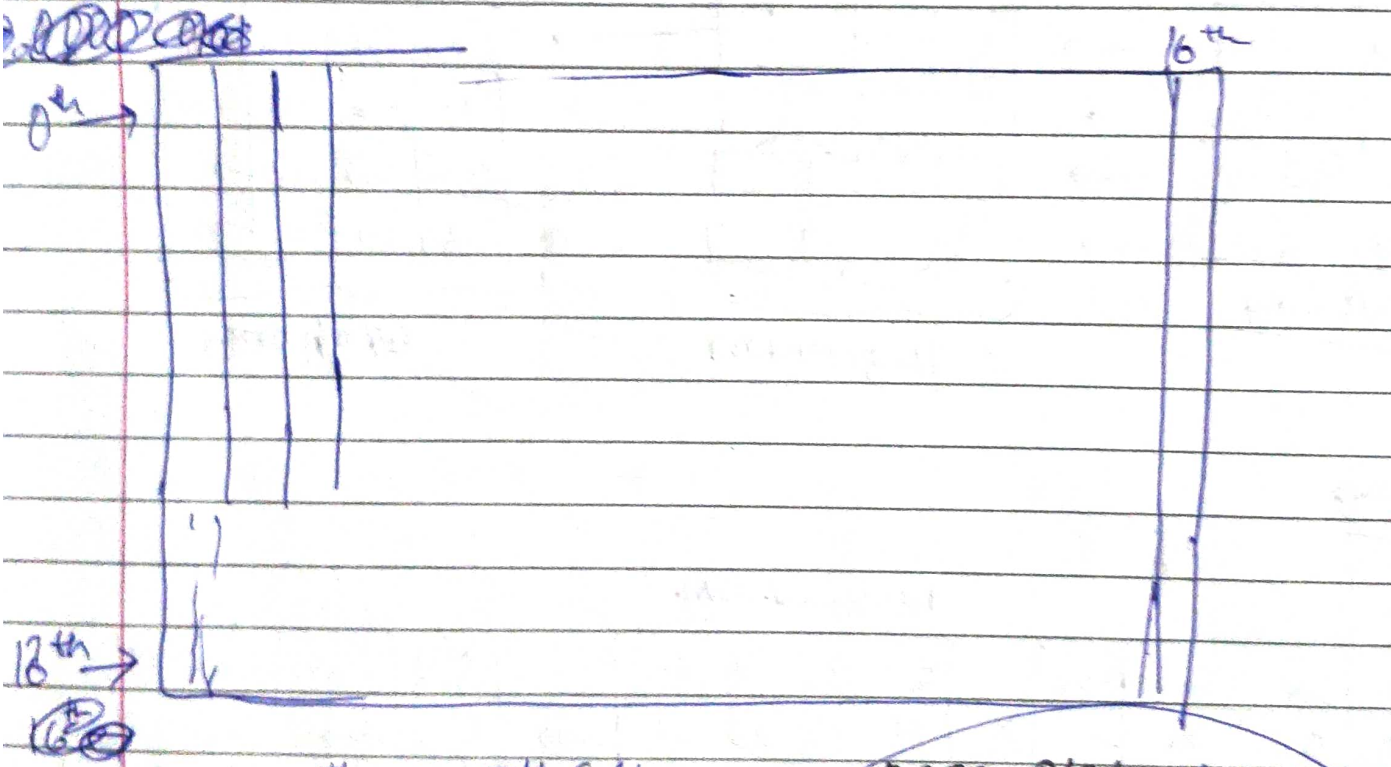
W_0	W_1	W_2	W_3												

44 words


Plain Text (16 bytes)
Key
Input State
(16 bytes)
Input State
Key
(16 bytes)
Round (0)
Initial Transformation
State after transformation (16 bytes)
Round 1
(4 transformation)
Round 1 (16 bytes)
Round 1 output State (16 bytes)
Key Expansion
(16 bytes)
Round N-1
Round N-1
(4 transformation)
Round N-1 output state (16 bytes)
(16 bytes)
Round N
Round N
(3 transformation)
Final State (16 bytes)
Cipher Text (16 bytes)

Substitution Box





So 0th row, 5th Column, 0000, 0101 Input

Suppose value is 52

0101, 0010 Output

Shift Rows

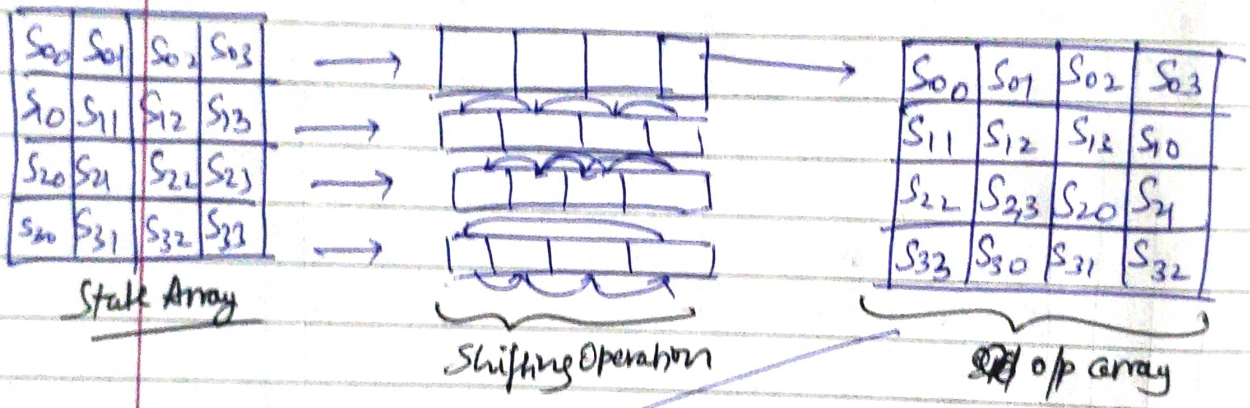
State Array

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

Given As Input to Shift Rows.

So,

Row 0 ⇒ 0 bits are circular left shift
Row 1 ⇒ 1 bit is circular left shift
Row 2 ⇒ 2 bits are circular left shift
Row 3 ⇒ 3 bits are circular left shift



Mix Columns

Pre-defined Matrix

$$\begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} \times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \Rightarrow \begin{bmatrix} S'_{00} & S'_{01} & S'_{02} & S'_{03} \\ S'_{10} & S'_{11} & S'_{12} & S'_{13} \\ S'_{20} & S'_{21} & S'_{22} & S'_{23} \\ S'_{30} & S'_{31} & S'_{32} & S'_{33} \end{bmatrix}$$

C_0 C_1 C_2 C_3

Similarly

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 02 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S_{00} \\ S_{10} \\ S_{20} \\ S_{30} \end{bmatrix} \Rightarrow \begin{bmatrix} S'_{00} \\ S'_{10} \\ S'_{20} \\ S'_{30} \end{bmatrix}$$

4×4 4×1

State Array

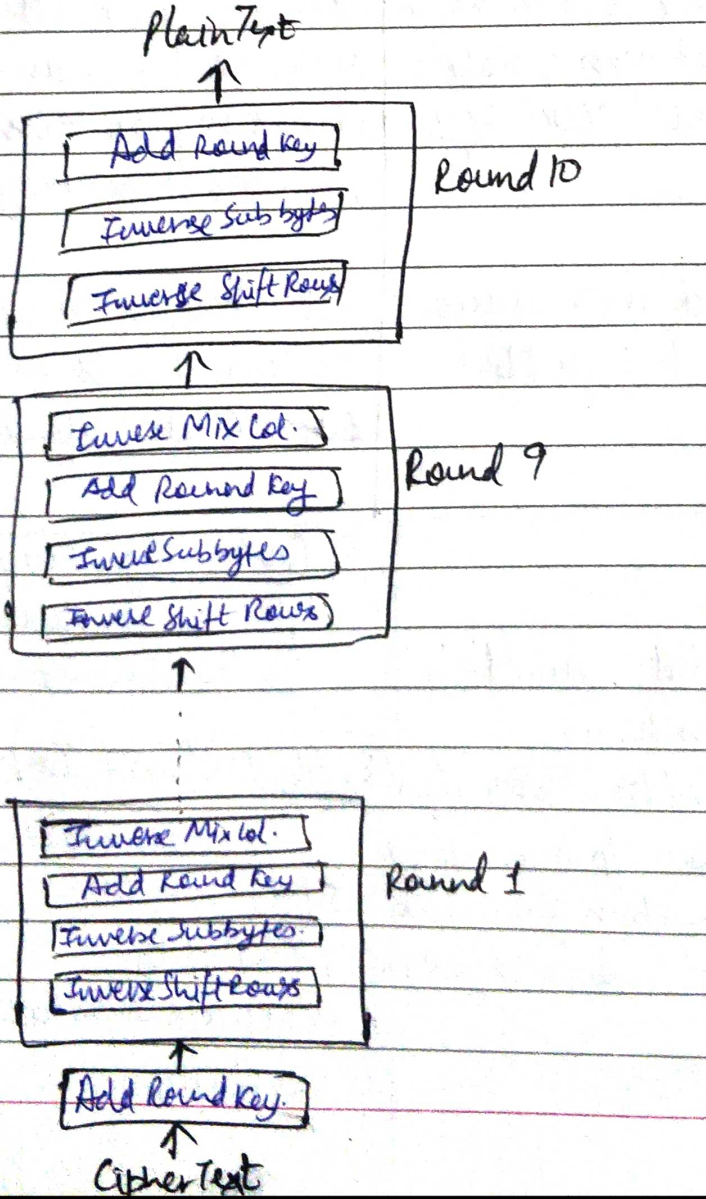
DELTA Page No.
Date / /

Add Round Key

State Array (O/p from Mixed Columns) ⊕ Key = Resultant Array

$$\begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} + \begin{bmatrix} & & & \\ W_1 & W_2 & W_3 & W_4 \\ & & & \end{bmatrix} = \begin{bmatrix} S'_{00} & S'_{01} & S'_{02} & S'_{03} \\ S'_{10} & S'_{11} & S'_{12} & S'_{13} \\ S'_{20} & S'_{21} & S'_{22} & S'_{23} \\ S'_{30} & S'_{31} & S'_{32} & S'_{33} \end{bmatrix}$$

Decryption



UNIT-II

Types of CryptoAnalysis (Linear & Differential)

Linear CryptoAnalysis	Differential CryptoAnalysis
→ Based on finding linear approximation to describe the transformations performed in the cipher	→ Based on block cipher primary It describes how differences in inputs can affect output.
→ The attacker obtains high probability approximations for the parity bit of secret key by analysing.	→ Used for tracing differences thro the network of transformations, disc non-random behaviour & exploiting it recover secret key.
→ The role of the attacker is to identify the linear relation between some bits of plaintext, ciphertext & secret key.	→ The role of attacker is to analyze the changes in some choosen plaintext diff in outp resulting from encrypting each one.
⇒ It focuses on statistical analysis against one round of decrypted cipher text.	⇒ It focuses on statistical analys of two inputs and two outputs of a cryptographic algorithm.

Evaluation of AES

(1) Security - Refers to effort required to cryptoanalyze an algorithm.
- (A) Actual security ⇒ Compared to another algo
- (B) Randomness ⇒ Extent to which o/p is indistinguishable from a random permutation of I/p Block
- (C) Soundness ⇒ Mathematical basis for algorithm security

(2) Cost - High Computation efficiency
- (A) Memory requirements
- (B) Licensing requirements

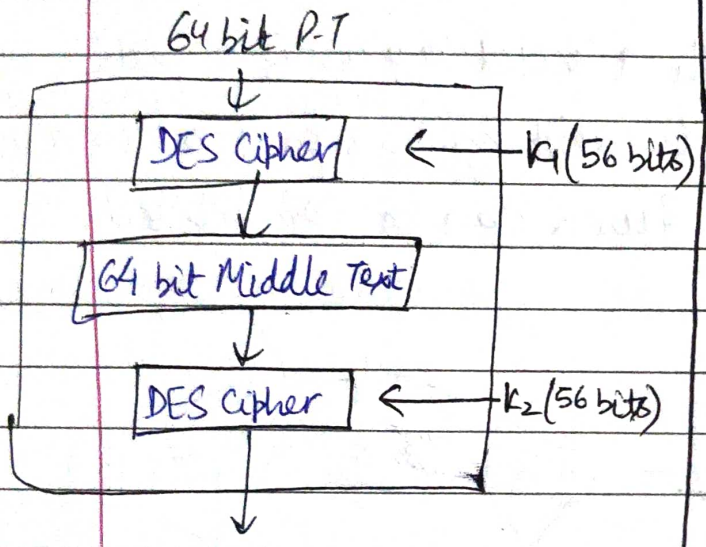
(3) Algorithm & Implementation
Includes variety of characteristics and parameters: -
- (A) Flexibility
- (B) Hardware & Software Suitability
- (C) Simplicity

Triple DES

- 3-Key Triple DES (3DES)
- 2-Key Triple DES (2DES)

2DES

→ For different instance diff key is used so (56+56 = 112 bits) of key used.

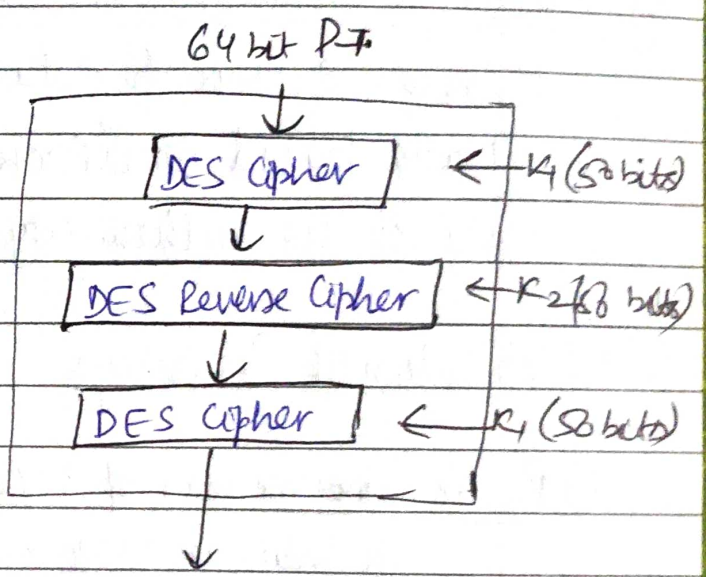


Encryption ⇒ $C = E(K_1, D(K_2, P))$

Decryption ⇒ $P = D(K_1, E(K_2, P))$

3DES

⇒ For different instance diff key is used so (56+56+56) = 168 bits of key used.



Encryption ⇒ $C = E(K_3, D(K_2, E(K_1, P)))$

Decryption ⇒ $P = D(K_3, E(K_2, D(K_1, P)))$

Key Management

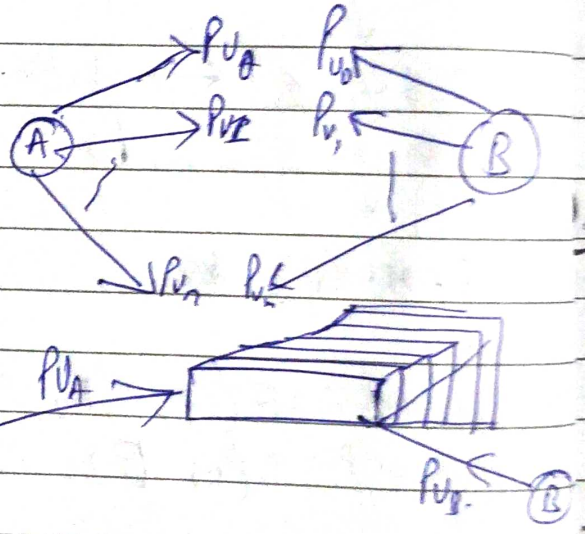
⇒ Public key encryption schemes are secured only if the authenticity of the public key is assured. A public-key certificate scheme provides the necessary security.

Eg Diffie-Hellman Key Exchange

Enables 2 users to establish a secret key using a public-key scheme based on discrete logarithms. This protocol is secure only if the authenticity of 2 users can be established.

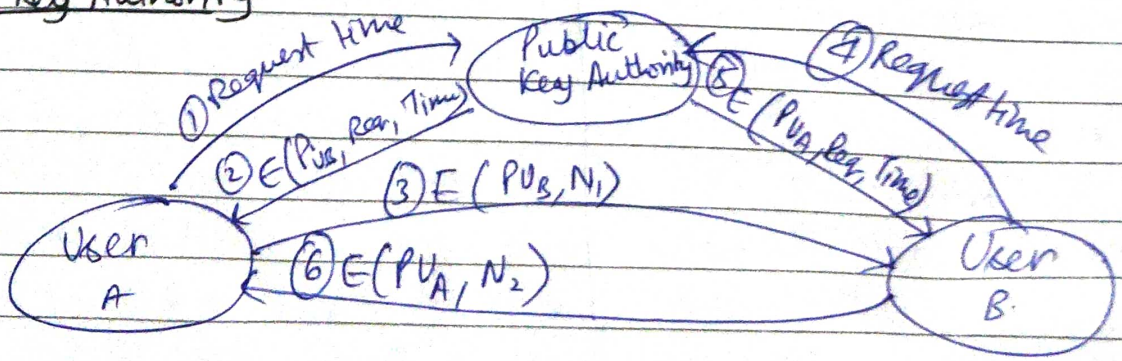
(A) Distribution of Public Keys

i) Public Announcement of Public Key –
Anybody can forge such a public announcement

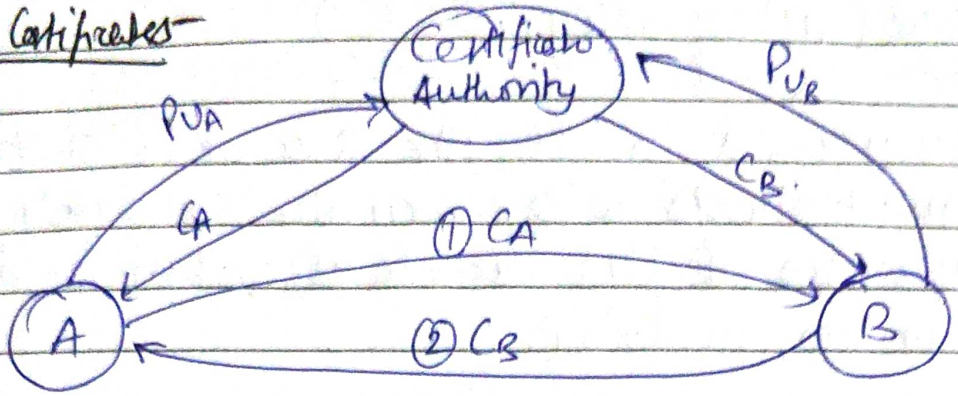


ii) Publicly Available Directory –
Anybody can tamper with records available kept by authenority

iii) Public Key Authority

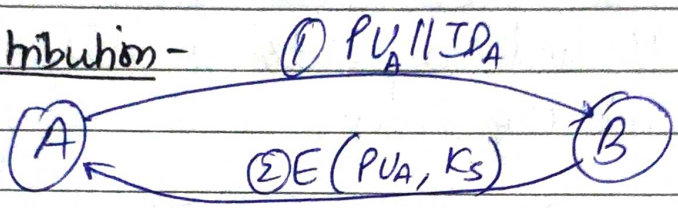


iv) Public-Key Certificates-

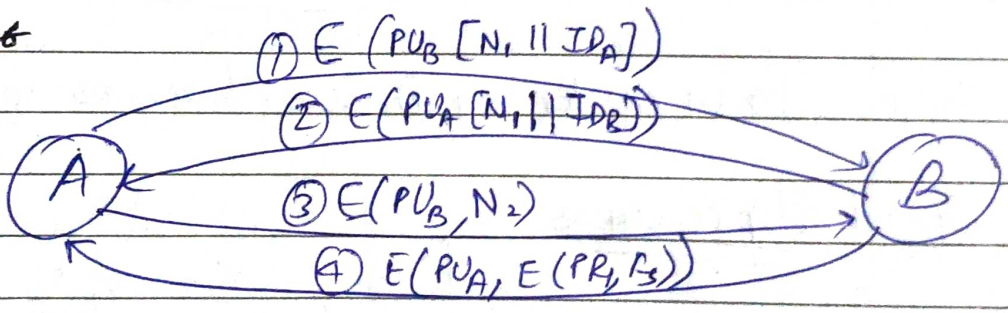


Distribution of Secret Key Using Public Key Cryptography

i) Simple Secret Key Distribution -



ii) Secret Key Distribution with Confidentiality & Exchange



(Kerberos)

iii) Hybrid Scheme - Retains use of key distribution centrer (KDC) that shares a secret master key with each user & distributes secret session keys encrypted with master key.

iv) Diffie-Hellman - Used to establish a shared secret that can be used for secret communications while exchanging data over public network using the elliptic curve to generate points & get the secret key using parameter.

Elliptic Curve Cryptography (ECC)

- ⇒ It is a term used to describe a suite of cryptographical tools and protocols where security is based on special versions of the discrete algorithm and does not use numbers modulo p.

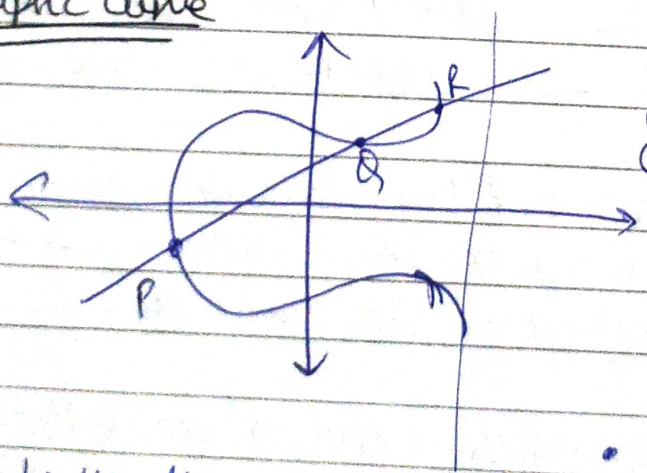
* Based on sets of numbers that are associated with mathematical objects called elliptic curves.

* It is believed that the discrete logarithm problem is much harder when applied to points on elliptic curve which prompts the switching from:-

number modulo P → Points on an elliptic curve.

* It results in shorter key, ① Ease of key Management ② Efficient computation

Eg: Eq. of elliptic curve



$y^2 = x^3 + ax + b$.

- Let $E_p(a, b)$ be the elliptic curve
- Consider eq ⇒ $Q = kP$
  where $Q, P \in E_p(a, b)$ & $k < n$.
- It should be easy to find Q given k & p.

- The security of ECC depends on how different it is to determine k given Q and P.

Authentication Requirements

DELTA Page No. Date / /

TYPES OF ATTACKS (MESSAGE AUTHENTICATION)

1) Disclosure - release of message contents to any person or process not possessing the appropriate key.

2) Traffic Analysis - Discovery of the pattern of traffic b/w parties. The ? and duration of connections could be determind and then the number or length could be found.

3) Masquerade - Insertion of message into the network from a fraudulent source. A person pretends to be the sender or masquerades to be a authenticated party.

4) Content Modification - Changes to the contents of a message, including insertion, deletion & modification.

5) Timing Modification - Delay or Replay of message in a connection-oriented application can cause chaos. Entire session could replay or be delayed.

6) Source Repudiation - Denial of transmission of message by source.

7) Destination Repudiation - Denial of receipt of message by destination.

8) Sequence Modification - Any modification to a sequence of messages between parties, including insertion, deletion & recording.

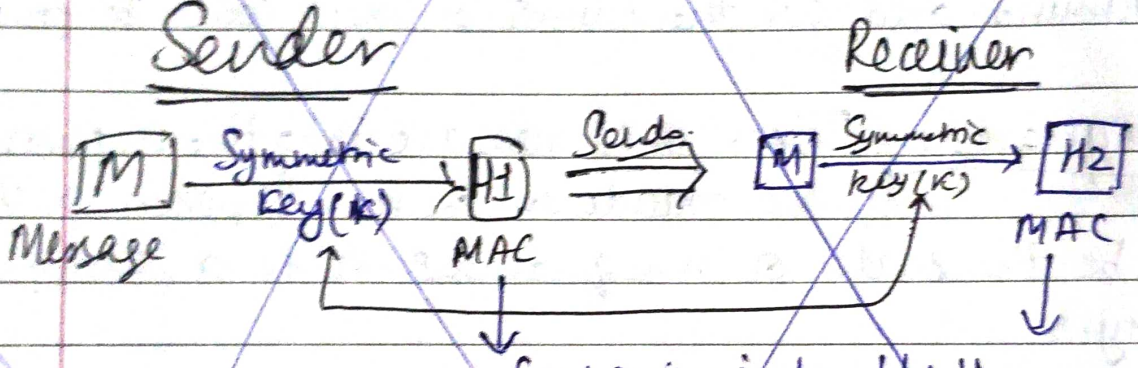
Consider this to be correct

DELTA Page No. Date

(MAC) Message Authentication Code

→ Similiar to MD (Message Digest) except the fact it contains a cryptographic process.

→ Achieved by using message authentication codes (or authenticated encryption (AE) or digital signatures.



if $H1 = H2$, no change in message.
$H1 \neq H2$, change in message.

Significance

~~1) Assurance of [illegible] message receiving and [illegible]~~

1) Ensures that Receiver knows whether the message has been altered.

2) Receiver is assured of authenticity i.e. correct sender

(Hash Based) HMAC – Used for security implementation in Internet Protocol (IP) and also in SSL (Secure Socket Layer Protocol) Protocol.

Original Msg $\xrightarrow{MD5/SHA}$ MD $\xrightarrow[(K)]{Encryption}$ MAC [HMAC]

Original Msg $\xrightarrow[(K)]{Encryption}$ MAC [MAC]

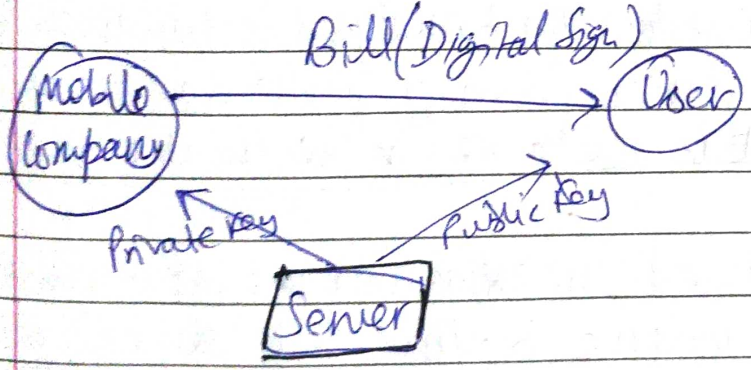
→ MAC is an algorithm that requires the use of a secret key. A MAC takes a variable length message & a secret key as input to produce an authentication code. (Hash)

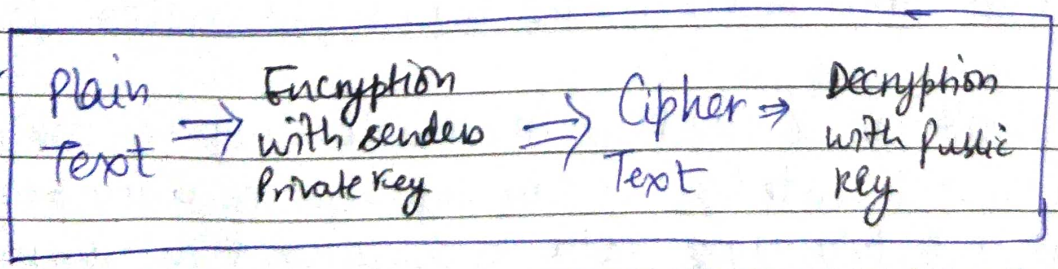
A recipient in possession of the secret key can generate an authentication code to verify integrity of message.

Digital Signatures

↳ Assymmetric-Key Cryptography
↳ Encryption with private-key
& Decryption with Public Key
↳ Used for Authentication & Non-Repudiation, Data Integrity

Eg





A technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any 3rd party.

Signing the hash is more efficient that signing the data.

Encryption with Digital Signature

* By combining digital signature with encryption schemes/message

Non Repudiation is assured.

Sign then Encryt

⇒ Can be exploited by receiver to spoof identity of sender and send that data to 3rd party.

Encrypt then Sign

⇒ More reliable as first signature is verified using sender's public key. After ensuring validity of the sign, then retrieve the data

Cyber Forensics (Computer Forensics)

⇒ Its the application of investigation & analysis techniques to gather and preserve evidence from a particular computer device in a way that is suitable or presentable in court

⇒ Goal is to perform structured investigation while maintaining a documented chain of evidence to find out exactly what happened on comp. device & who was responsible for it.

⇒ Ethical Hacking is the key to strengthening network security and by that knowledge we can improve security breaches and can collect/analyze data to monitor & interpret weaken

UNIT-III

DELTA Page No. Date

Buffer Flow Attack - An anomaly where a program or process attempts to write more data to a fixed length block of memory or buffer than the buffer is allocated to hold.

Buffer - Memory area set aside to hold data, used to move one section of program to another.

* Caused in C-based languages as they don't perform any kind of array bounding checking. When a buffer overflow occurs in a prog, it will crash & become unstable.
* Occurs when data written to a buffer also corrupt data values in memory addresses adjacent to destination buffer due to insufficient bounds checking
* Can occur when copying data from one buffer to another without checking that the data fits with the destination buffer.

Heap Based

⇒ Difficult to execute & least common of the two. Attack an app by flooding memory space reserved for a prog.

Stack Based

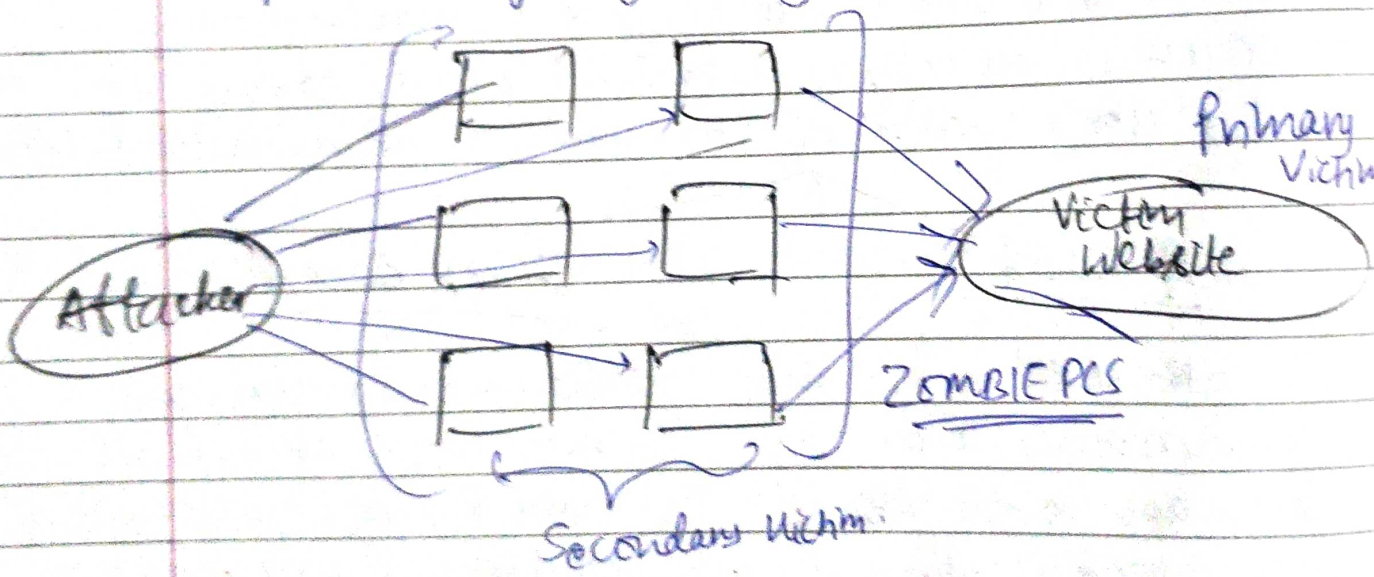
⇒ Common to execute & more easy. It exploits apps & prog. by using stack memory space used to store user input.

Destributed Denial of Service Attack

⇒ DDoS attack makes computer system inaccessible by flooding servers networks or even end user systems with useless traffic so that legitimate users can no longer gain access to those resources

⇒ These force the system to shut down or even crash because of the flooding of incoming messages

⇒ Attacker recruits a no. of hosts throughout the Internet simultaneously or in a coordinated fashion to launch attack upon the target by sending useless packets to target



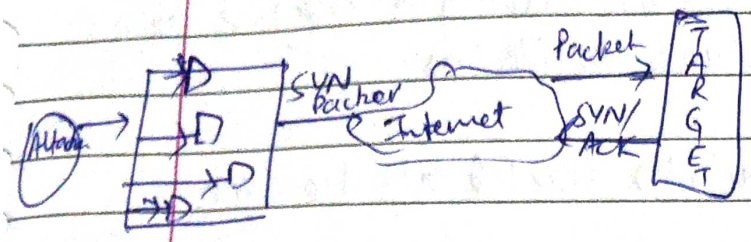
4 pillars of DDOS attack:-

i) Using Internets insecure channel
ii) Huge Traffic usage as a weapon.
iii) Circumventing the security defense of a victim
iv) Hiding attacker's Id.

DELTA Page No. Date / /

Types

i) Internet Host Resource Attack

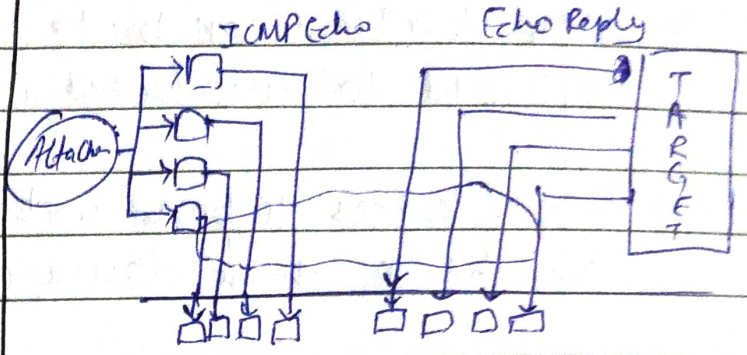


a) Attacker uses many slave hosts or zombie pcs to send TCP/IP SYN (synchronize/initialization) packets with erroneous return IP add.

b) Each SYN packet requests to open TCP connection and responds with SYN/ACK packet and server becomes so bugged down as traffic floods in.

c) legitimate requests are denied while attacker continues and bogus requests are fulfilled.

ii) Attack consuming Data Transmission Resources



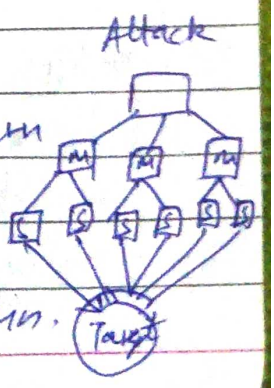
a) Attacker uses many slaves hosts over internet instructing them to send Icmp echo packets with target's spoofed IP address acting as reflectors.

b) Nodes at bounce site receive multiple spoofed requests & then respond by sending echo reply to target.

c) Target router is flooded with packet from bounce site leaving no data transmission for legitimate traffic.

iii) Direct DDOS

Attacker implants zombie s/w on a no. of sites distributed throughout the internet
- Master Zombies
- Slave Zombies



Attacker co-ordinates and triggers master zombies which in turn co-ordinate & trigger slave zombies.

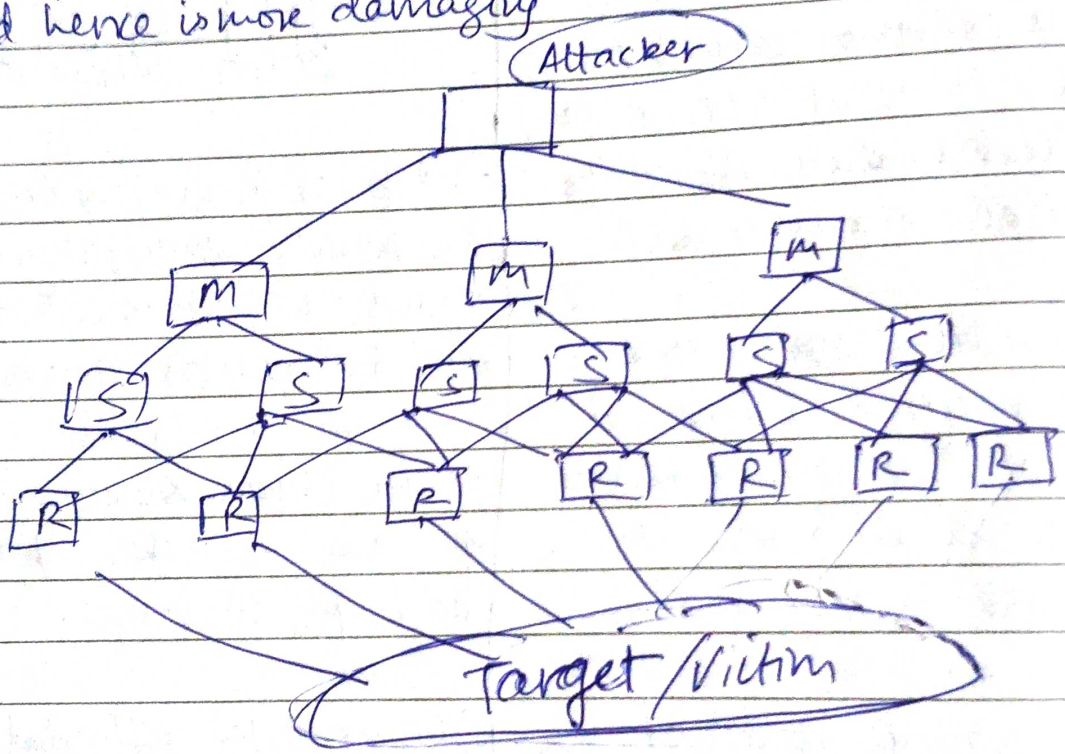
Two level of zombies makes it difficult to trace back origin.

iv) Reflector DDOS

* Adds another layer of zombies called 'reflectors'.

* Slave zombies constructs packets requiring a response and are sent to uninfected machine → reflectors.

* These reflectors respond with packets directed at the target and hence is more damaging



Weak Authentication

"Authentication" refers to the process of providing an identity to an application or system. Demonstrating who you are:-

* Any scenario in which the strength of the authentication mechanism is relatively weak as compared to value assets to be protected.

* For avoiding weak authentication, following should be done:-
  - two-factor authentication
  - Strong password policy
  - Authentication token security.

Substitution Box (S-Box)

* S-box is a basic component of symmetric key algorithm which performs substitution and used depict relationship between key and cipher text.

* Takes 'm' no. of input bits and transforms them into 'n' no. of output bits where $n \neq m$.

Main criteria of good S-box are:-

- It should have a high algebric degree
- Non-linearity of its component func^n should be high.
- Non-Zero linear combinations should be balanced and highly non-linear

Approaches to Design S-Box

- **Random** - Use some pseudo random no. generation or some table of digits to generate the entries in the S-box.
- **Human-Made** - Manual approach with only simple mathematics to support it.
- **Math-Made** - Generate S-box according to mathematical principles. S-box can be constructed by linear & differential cryptoanalysis.
- **Random with Testing** - Choose S-box entries randomly, then test to support it. Results are tested to verify criteria & throw away those that don't pass.

Hash Functions

A hash function is a function which takes on input/msg & returns a fixed size alphanumeric cipher text known as "Hash Value"

↳ h generated by function "H"

* Fixed length o/p
* Compression func
* Digest (smaller rep of larger info)

$h = H(M)$

h = (hash value)
H(m) = (Hash Function)
M = Message of length n

Hash value is appended to the msg at the source then the msg is assumed to be correct. The receiver authenticates the msg by recomputing the hash value.

Security of Hash Function

There are 3 main characteristics :-

- One-Hand Function - One way Rule should apply.
- Resistance to preimages - Given x, it shall be hard to find 'M' such that $H(M) = x$
- Resistance to second preimages - Given m & H(M), it shall be hard to find m' (distant from m) such that.
  $H(M) = H(M')$
- Resistance to collision - It should be hard to find M & M' distant from each other such that $H(M) = H(M')$
- Bruteforce Attack
- Cryptoanalysis

Secure Hash Algorithm (SHA)

O/p – 128 bit = SHA 1
256 bit = SHA-256
512 bit = SHA-512

H(M) = h → 512 bit

SHA-512

Plain Text Block Size = 1024 bits
No. of Rounds/steps = 80
Each Round
→ dword = 64 bit
→ Constant = K
→ Buffers = Store intermediate result, store o/p (hash code)
Buffer Size = 64 bits
hence Buffers are 8

① Add padding according to the multiple of 1024 bits and 128 bits <.

② Represent original P.T in 128 bits and append it such that length is multiple of 1024 bits.

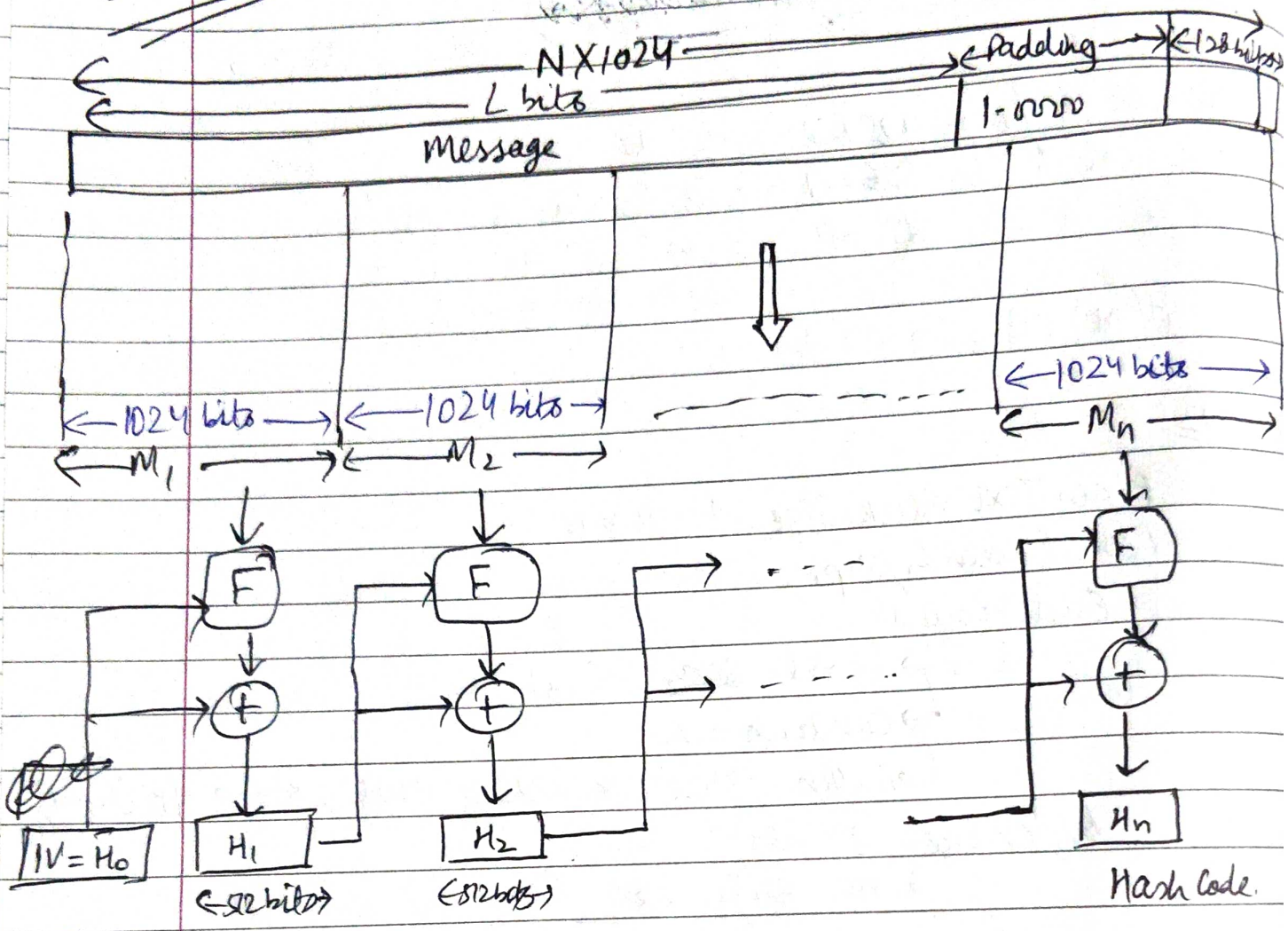
③ Initialize the buffers (A, b, c, d, e, f, g, h) → 64 bits each

④ Process each block of P.T in 80 rounds

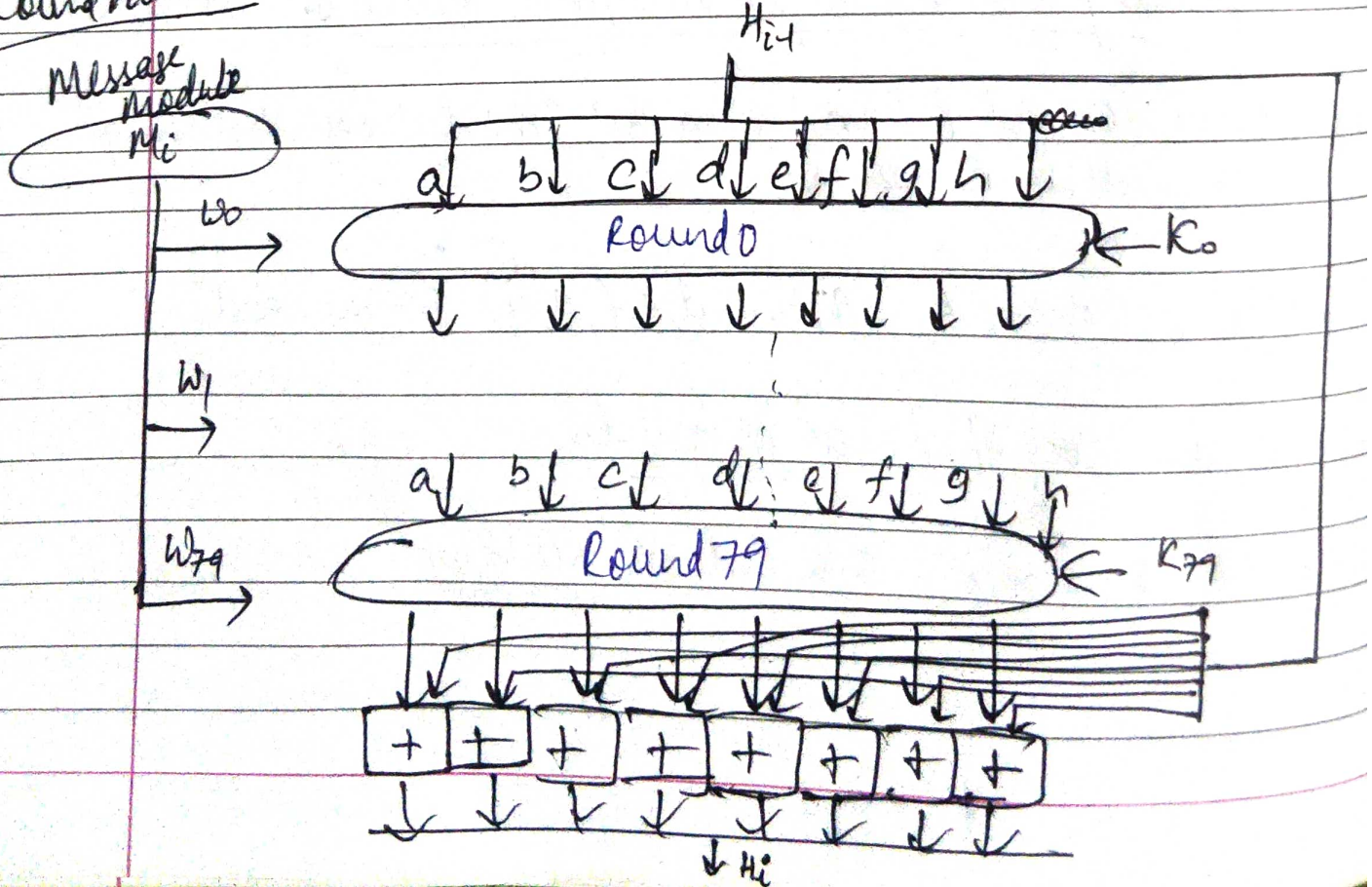
⑤ O/p in Buffers is Hash Code of 512 bits

DELTA Page No.
Date / /

Block Diagram



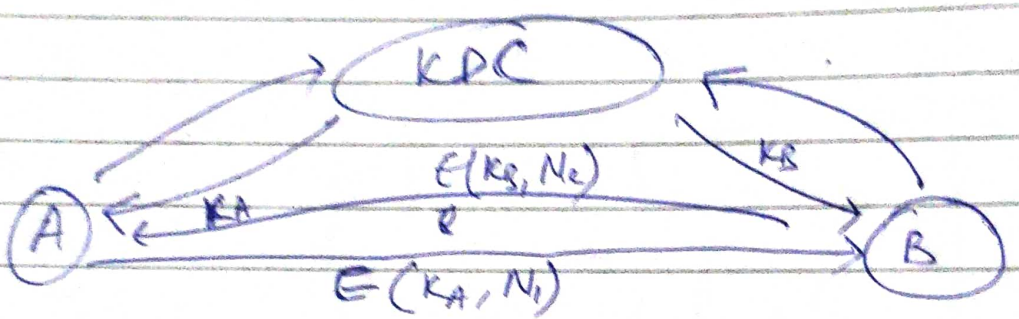
Round function



Kerberos

⇒ It is a comp. network authentication protocol which works on the basis of 'tickets' to allow nodes to communicate over a non-secure n/w to prove their identity to one another in a secure manner.

⇒ Requires trusted 3rd party (KDC) < Authentication (AS), Ticket Granting (TGS)



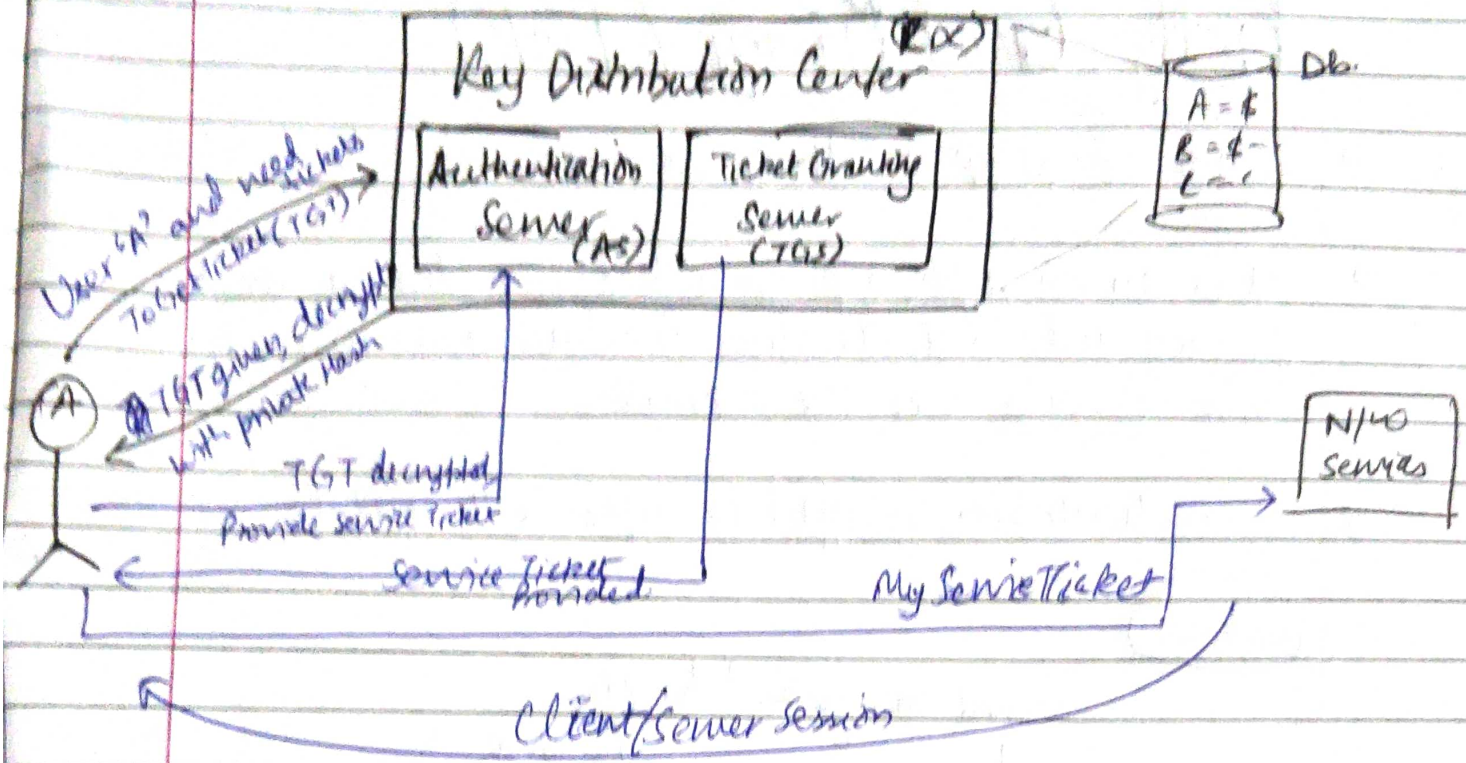
Requirements of Kerberos

1) Secure- No n/w eavesdropper should be allowed to obtain any info. Kerberos should be strong enough that no weak link can be found.

2) Reliable- Should be highly reliable, as all the servers rely on Kerberos for access control. Should use good architecture to support & backup server also

3) Transparent- User should be aware of the authentication taking place, beyond the requirement of password

4) Scalable- The system should be capable of supporting large number of clients & servers.



- To start the process, the initialization client sends a request to AS for access to a service
- The initial request is sent as plain Text because no sensitive info is included.
- The AS retrieves the initializing clients private key, from client's name in KDC db.
- AS generates a session key for accessing the services otherwise user not authorized.

IP Security (IPsec) ⇒ Used for protecting communications over IP n/w.
⇒ End-to-End scheme, secures application at IP layer.

It is a security model or n/w protocol security suite that authenticates and encrypts the packets of data sent over network.

Includes protocols for establishing mutual Authen s/w agents at the beginning of the session & negotiation of keys to use during the session

Protect data flow b/w:- Host & Host, network & Host
Sec gateway & Host,

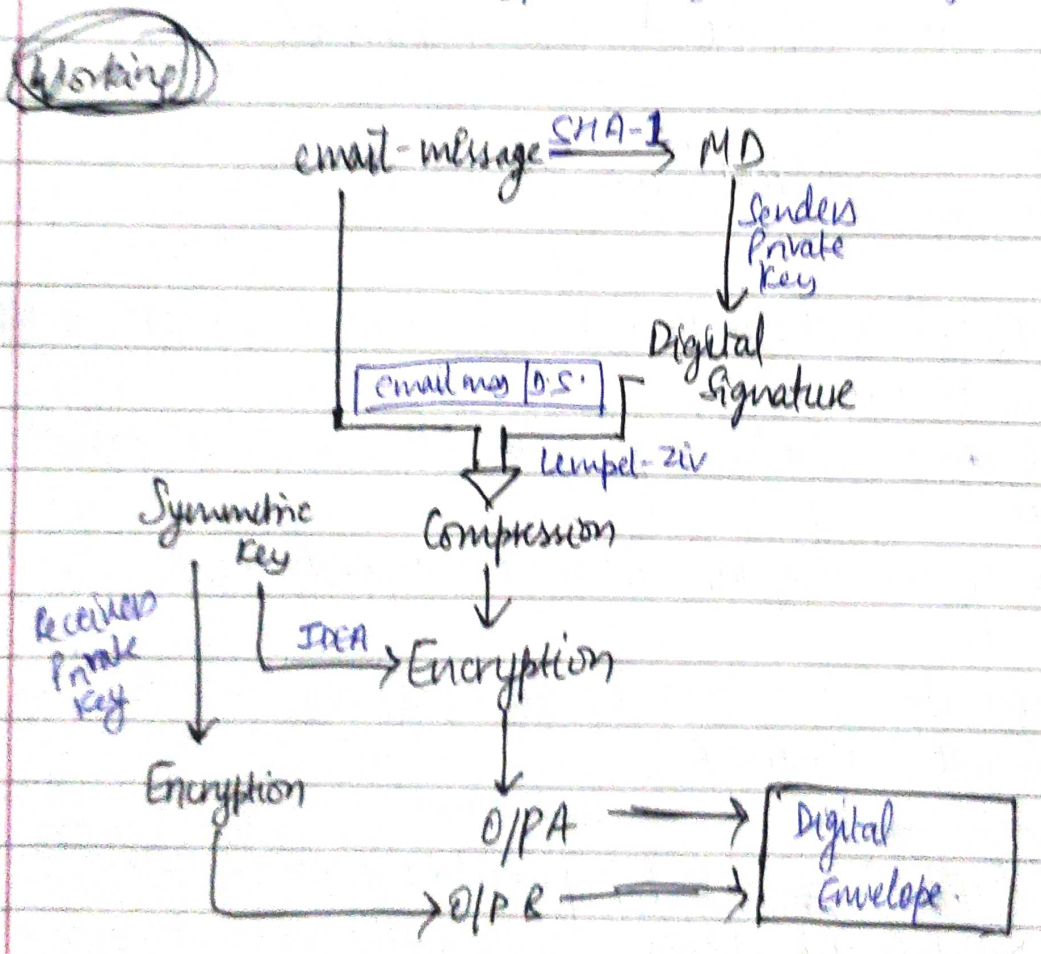
Pretty Good Privacy (PGP)

→ Father of PGP → Phill Zimmerman

→ It is an encryption program that provides cryptographic privacy and authentication for data communication for Emails over the Internet

→ It authenticates, encrypt & decrypts with digital signatures.

Working



Each user has an encryption key i.e. publically known & a private key i.e. known only to user. One can send an encrypted message by using the public key and they can decrypt it using their private key.

PGP provides security even though open source through

(A) Authentication - Through the use of digital signatures
(B) Confidenciality - Through the use of symmetric block encryption
(C) Compression - Through zip algorithm
(D) Email Compatibility - Through the radix-64 encoding scheme
(E) Segmentation & Reassembly - To accomodate long E-mails.

PGP is widely used because :-

(1) It is freely available & runs on a variety of platforms
(2) It is based on algorithms that are extremely secure
(3) It has a wide range of applicabity.
(4) It is now on Internet Standard track.

Side Channel Attack -

An attack based on information gained from physical implementation of crypto-system, rather than bruteforce or weakness in algo.

They monitor power consumption & electromagnetic emission while device is performing making it simple and inexpensive to execute.

Cache Attack - Attacks monitors cache access made by victim
Timing Attack - Attacks based on how much time tasks take
EM Attack - Based on leaked EM radiation which can provide P-T & other info
Accoustic Attack - Exploits sound produced during computation
Power Monitoring Attack - Based on power consumed by hardware during analysis.