__/__/__

Information Security Sessional-I

Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

Objectives of IS are:-

(i) Confidentiality :- means information is not disclosed to unauthorized individuals, entities and process.

(ii) Integrity :- means maintaining accuracy and completeness of data. This means data cannot be edited in any unauthorized way.

(iii) Availability :- means information must be available when needed.

Elements of IS :-

(i) Physical Elements :- Gaurd, cameras, R-zone etc.

(ii) System elements :- Antivirus, Malicious S/w detection solution, disable USB ports.

(iii) Process Elements :- Authorized user/access control, S/w details, log entry.

Types of Security

(i) Physical security
(ii) Personal security
(iii) Operators security
(iv) Communication security

(v) Network Security
(vi) Information Security

The OSI Security Architecture

ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) recommends X-800 security architecture for OSI that defines a systematic way of defining and providing security requirements.
Furthermore, because this architecture was developed as an International Standard, computer and communications vender have developed security features for their products and services.

X-800 consist of:-

(i) Security Attack :- Any action that compromises the security of information owned by an organization.

(ii) Security Mechanism :- A process that is designed to detect, prevent and recover from a security attack.

(iii) Security Service :- A processing and communication service that enhances the security of data processing system and information transfers of an organization.

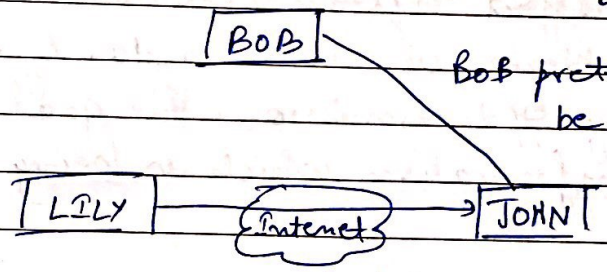
The services are intended to counter security attacks and they make use of one or more security mechanisms to provide service.

__/__/____

Types of Security Attack:-

1) **Active attacks** :- An active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as follows:-

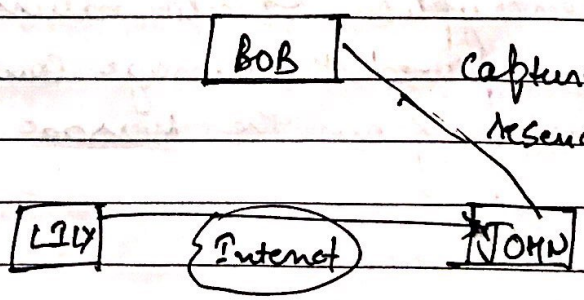
(i) **Masquerade**:- Masquerade attack takes place when one security entity pretends to be different entity



(ii) **Modification of messages**:- It means that some portion of message is altered or that message is delayed or recorded to produce an unauthorized effect.

(iii) **Repudiation**:- This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message.

(iv) **Replay** :- In involves the passive capture of a message and it subsequent the transmission to produce an unauthorized effect.



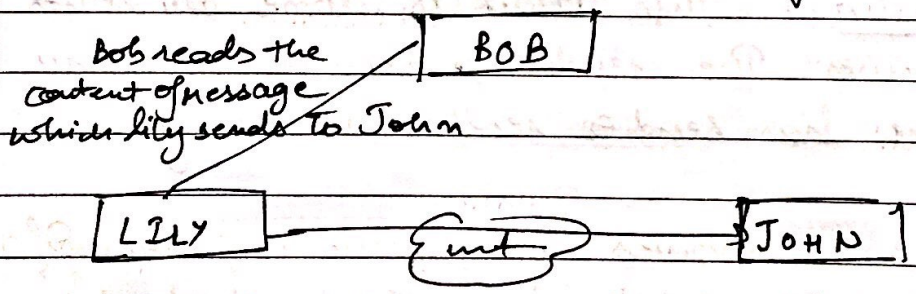
(v) Denial of Service :- It prevents normal use of communication facilities. This attack may have a specific target.
Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.

2) Passive Attacks :- A passive attack attempts to learn or make use of information from the system but does not affect system resources.
Passive attacks are in the nature of eavesdropping or monitoring of transmission. The goal of opponent is to obtain information which is being transferred.

478
433082

Types of passive attacks :-

(i) The release of message content :- Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information.



(ii) Traffic analysis :- Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

Active Attack	Passive Attack
1) Modification in information takes place.	1) Modification in the information does not takes place.
2) It is danger of for integrity as well as availability.	2) It is danger for confidentiality.
3) Attention is on detection.	3) Attention is on prevention.
4) In this, victim gets informed about the attack.	4) In this, victim does not gets informed about the attack.
5) System resources can be changed.	5) System resources are not changed.

Security Services Types:-

(i) X-800

(ii) RFC 2828

X-800

X-800 defines it in 5 categories:-

(i) Authentication:- assurance that the communicating entity is the one claimed.

(ii) Access Control:- prevention of the unauthorized use of a resource.

(iii) Data confidentiality:- protection of data from unauthorized user.

(iv) Data Integrity:- assurance that data received is as sent by an authorized entity.

(v) Non-Repudiation:- protection against denial by one of the parties in a communication.

__/__/__

Substitution Cipher

Monoalphabetic Polyalphabetic

Monoalphabetic

1) Ceaser Cipher :- It is a monoalphabetic cipher in which each letter of plain text is substituted with another letter to form a cipher text.

It is a simplest form of substitution cipher scheme.
This crypto system is generally referred to as shift cipher.
The concept is to replace each alphabet by another alphabet which is shifted by some fix Number of position between 0-25.

For this type of schema both sender and receiver agree on a secret shift number for shifting the alphabet.

Process of Shift cipher:-

1) In order to encrypt a plain text letter, the sender positions the sliding ruler underneath the first set of plain text and slides it to the left by the no. of positions of secret shift.

2) The plain text is then encrypted to the cipher text letter on the sliding ruler under-neath. The result of this process is depicted in the following

illustration for an agreed shift to 3-position.

Eg. here plaintext = TUTORIAL

Key, K = 3

Now, the cipher text = WXWRULDO

3) On receiving the cipher text, the receiver who also knows the secret share, positions the sliding ruler underneath the cipher text and slides it to the right by the agreed shift no. by 3.

He then replaces the cipher text letter by the plane tst letter by the sliding ruler underneat

4) Hence, the cipher text is decrypted to TUTORIAL.

Disadvantage

Ceaser Cipher is not secure cryptosystem because there are only 26 possible keys to try out and attacker can carry out exhaustive or search with available limited computing system.

Poly alphabetic Cipher

(i) Playfair
(ii) Vigenere
(iii) Vernam

(i) Playfair

Key = Tutorialss.

Matrix = 5 × 5 (fix)

t	u	o	r	i
a	l	s	b	c
d	e	f	g	h
k	m	n	p	q
v	w	x	y	z

t	u	~~t~~	o	r
i	a	l	s	b
c	d	e	f	g
h	k	m	n	p
q	v	~~x~~	~~y~~	~~z~~

Always skip 'j'

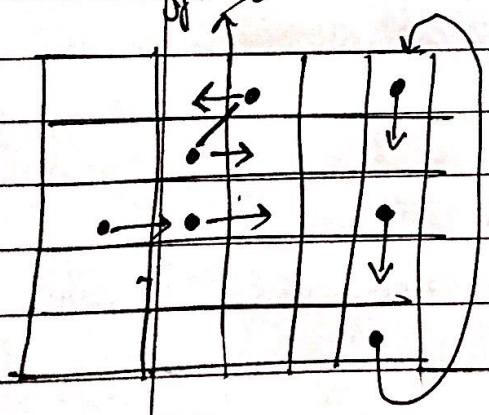
Eg. Hide money

hi de mo ne yz

qc ef nu mf zv

if no pair always pair with 'z'

if diagonal



(ii) Vigenere

Key = ~~Point~~ POINT

P=16, O=15, I=9, N=14, T=20

Encryption

PT	a	t	t	a	c	k	f	r	o	m	S	o	u	t	h	e	a	s	t	
Key	16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14	

a+16=q

Q I C O W A U A C G I D D H B U P B H

Decryption

CT	Q	I	C	O	W	A	U	A	C	G	I	D	D	H	B	U	P	B	H	
Key	16	15	9	14	20	16	15	9	14	20	16	15	9	14	20	16	15	9	14	
PT	a	t	t	a	c	k	f	r	o	m	S	o	u	t	h	e	a	s	t	

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
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

Count reverse.

3) Vernam (One time pad)

Eg. Hello

Suppose One time pad Key

f TO

__/__/____

Vernam

from sender's side

Plain text :- h e l l o
~~One time plain text~~ value :- 8 5 12 12 15
One time Pad text key :- X M C K L (Suppose)
One time Pad text value :- 24 13 3 11 12

Sum of PT & Pad value :- 32 18 15 23 27

After modulo sub :- 6 18 15 23 1
Cipher text :- F R O W A

In modulo sum if sum of PT & Pad value is more than 26 then ~~g~~ fract the sum ~~from~~ with 26 others will remain same.

from receiver's side.

Cipher text :- F R O W A
CT. value :- 6 18 15 23 ~~27~~ 1
One time pad text :- X M C K L
" " " value :- 24 13 3 11 12 ← Sub.
−18 5 12 12 −11
+26 +26
8 5 12 12 15 ⇒ hello.

When the -ve no. comes add with 26.

Transposition cipher

* Rearrange the order of Plain text bits
* No replacement / substitution.

Types:-

(i) Rail Fence
(ii) Row Transposition (or columnar)

(i) Rail Fence

P.T = TEXT BOOK PAGE THREE
Key = 3

from sender side

T	_	_	_	$	_	_	_	P	_	_	_	T	_	_	_	E
_	E	_	T	_	O	_	K	_	A	_	E	_	H	_	E	_
_	_	X	_	_	_	O	_	_	_	G	_	_	_	R	_	_

Cipher Text :- TBPTEETOKAEHEXOGR

from receiver side

Now write sequence wise ~~free~~ in first row with 3 ~~spaces~~ as key value=3

T	_	_	_	B	_	_	_	P	_	_	_	T	_	_	_	E
	E		T		O		K		A		E		H		E	
		X				O				G				R		

Now read diagonally.

TEXT BOOK PAGE THREE

(i) Jumbling of characters in Rail Fence cipher to get the cipher text.
(ii) It is used for short length messages.
(iii) It is easily crackable.

(ii) Row Transposition

P.T = "WELCOME TO MY SESSION"

Key :- 3 2 4 5 1 (unique no. should be considered.)

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

Ciphertext : OMSY, EESO, WHYI, LTEN, COSX
(read it like 12345)

from receivers side.

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

Plaintext :- WeCOME TO MY SESSION.

__/__/__

Steganography

Stegnos (cover/ Hidden)

Graph (to write)

It is a technique of hiding secret data within a ordinary non-secret file or message in order to avoid detection, the secret data is then extracted at the destination.

A plain text message may be hidden in one to two ways. The methods of steganography conceals the existence of message.

Various techniques used :-

(i) Character marking :- Selected letter of printed or written text are overwritten in pensil. The marks are ordinarily not visible unless the paper is held at an angle to brign light.

(ii) Invisible Ink :- A no. of substances are used for writting but leave no trave until som heat or chemical is applied to the paper.

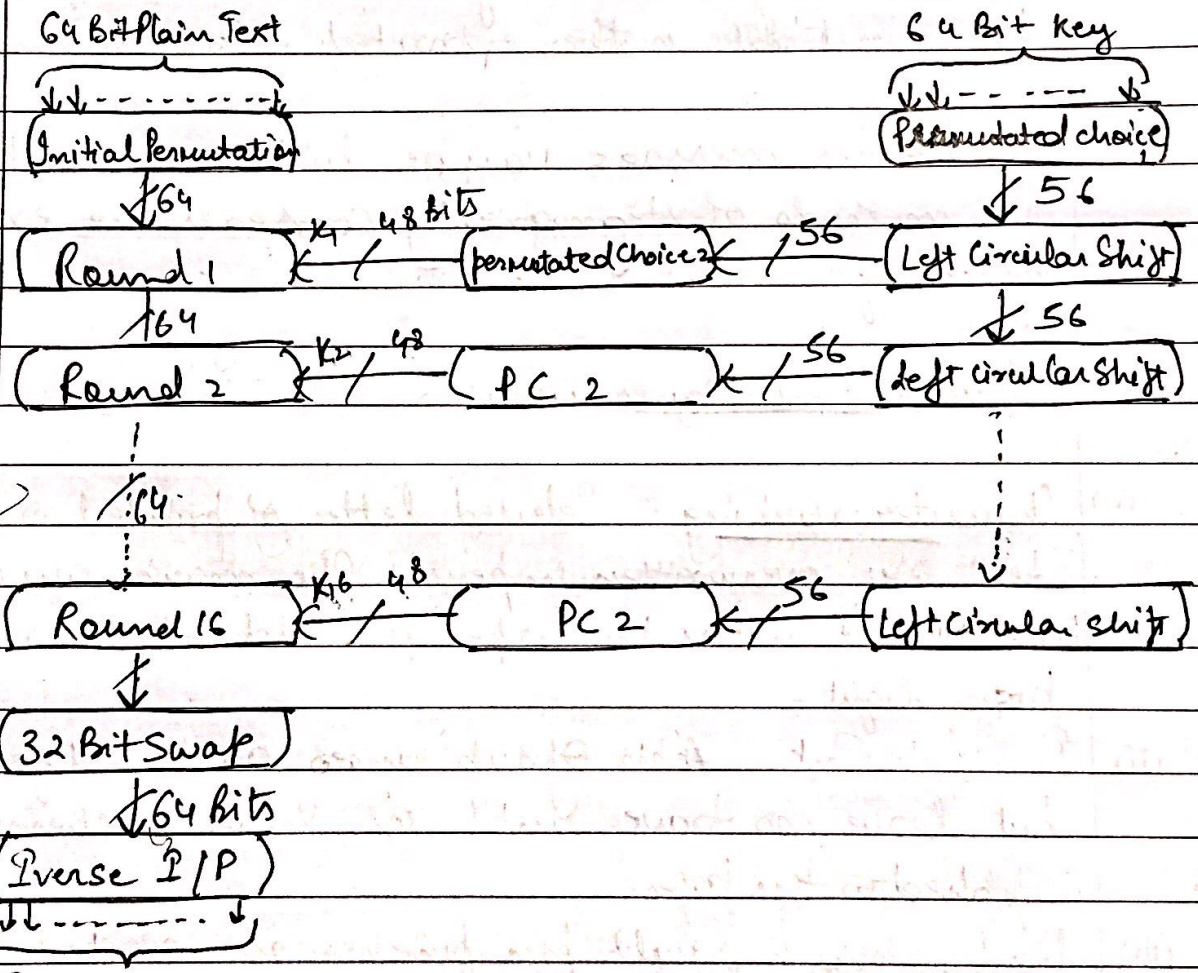
(iii) Pin Punchers :- Small pin punches on selected letters are ordinarly not visible unless the paper is held up in front of the light.

(iv) Type writter correction ribbon :- Used b/w lines typed with black ribbon. The results of typing with correction tape are visible under a strong light.

DES

DES stands for Data Encryption Standard.

(i) ~~Most~~ most widely used block cipher in world
(ii) adopted in 1977 by NBS
(iii) Encrypts 64-Bit data using 56-Bit key
(iv) has widespread use.
(v) has been considerable controversy over its security



Permutated choice means. a table which has random values and after permutation a new value is generated i.e. 64 Bit key is converted to 56 Bit Key.

There are 16 Rounds from the encryption of plain text to cipher text.

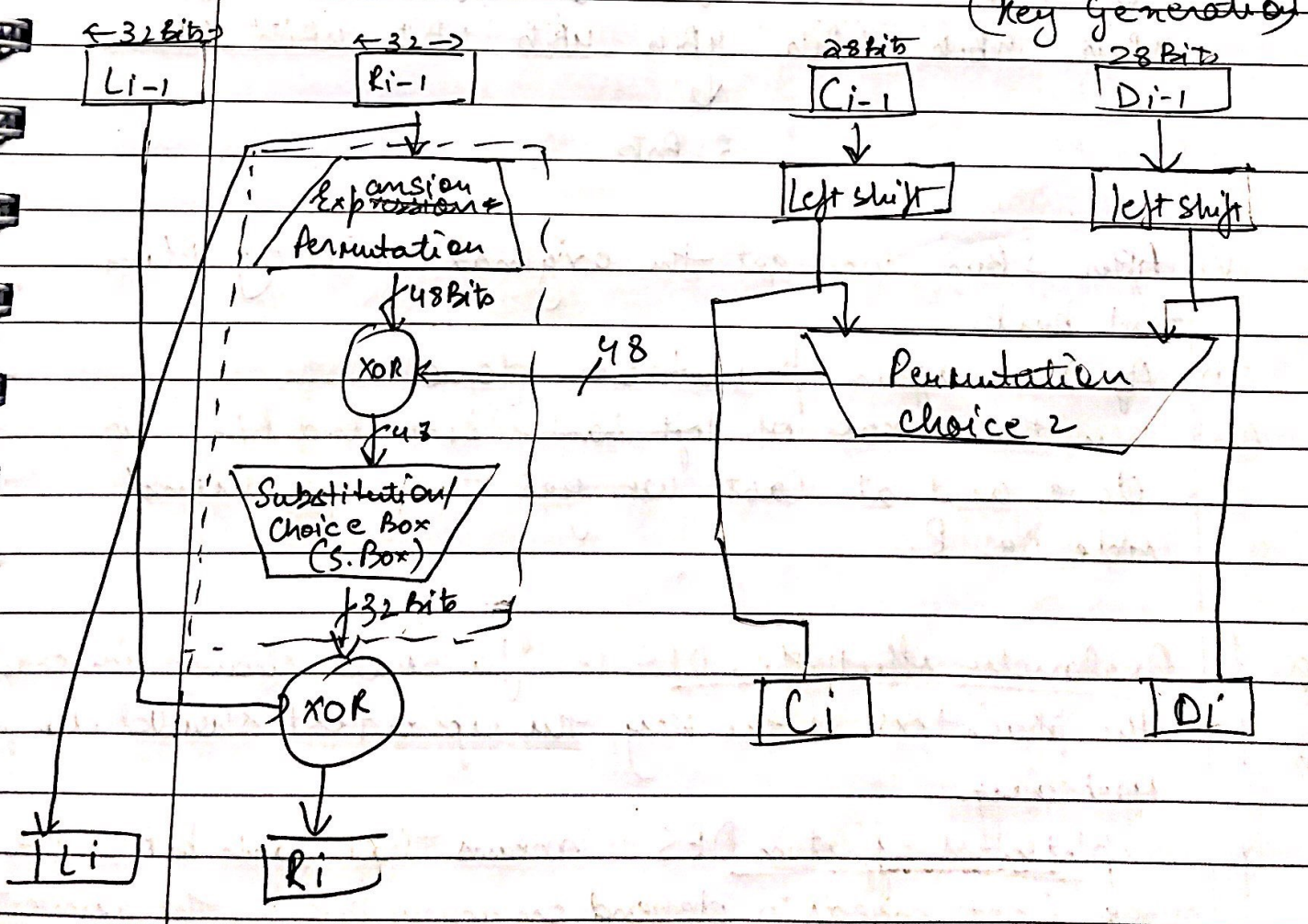
The 8 bits (i.e. 64-56) are ~~for parity~~ used for parity or error checks.

Left Circular Shift shifts the key to the rounds.

Again a permuted choice will be applied on the key we get 48 Bit of key which we will apply on the rounds.

After all the rounds are done a 32 Bit swap will be done and finally inverse Initial permutation will be applied and will give ~~us the~~ Bi generate the Cipher Text.

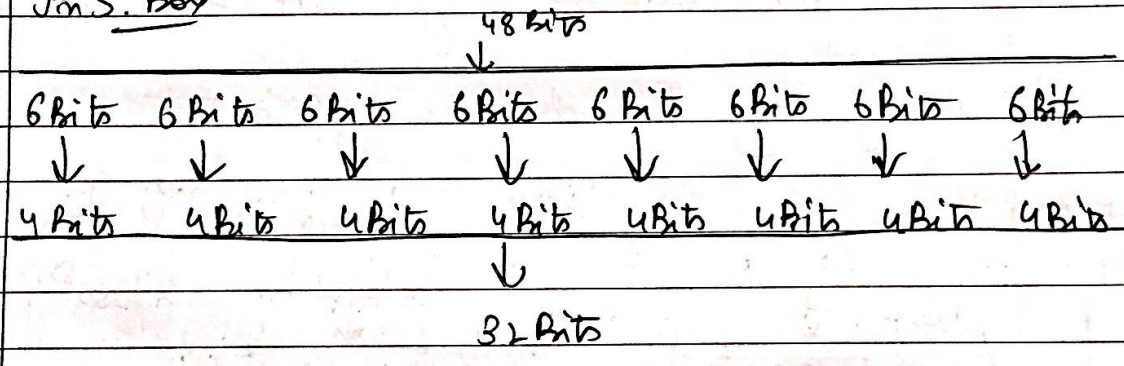
Inside of every Round (Encryption)



(ii) plain text gets divided into 32-32 Bits
(iii) In Round$_{i-1}$ expansion permutation is applied which converts 32 bits of to 48 bits
(iii) In key generation the 48 Bit key is left circular shifted towards the round$_{i-1}$ in which 48 bit plain text is XOR with the 48 Bit key.

(iv) After doing XOR what is produced will be shifted towards Substitution Box i.e. S Box

In S. Box



(v) After S Box we get the original 32 Bit of Plain text back.
(vi) Again Once again permutation done.
(vii) Then the XOR of ~~left hand~~ L_{i-1} and R_{i-1} is done and at last we get the right hand side i.e. R_i

Strength of DES

Avalanche effect in DES :- If a small change in either the plaintext or the key, the ciphertext should change markedly.

Completeness effect in DES :- means that each bit of the cipher text needs to depend on many bits on the plaintext

Symmetric Block Cypher

Triple DES

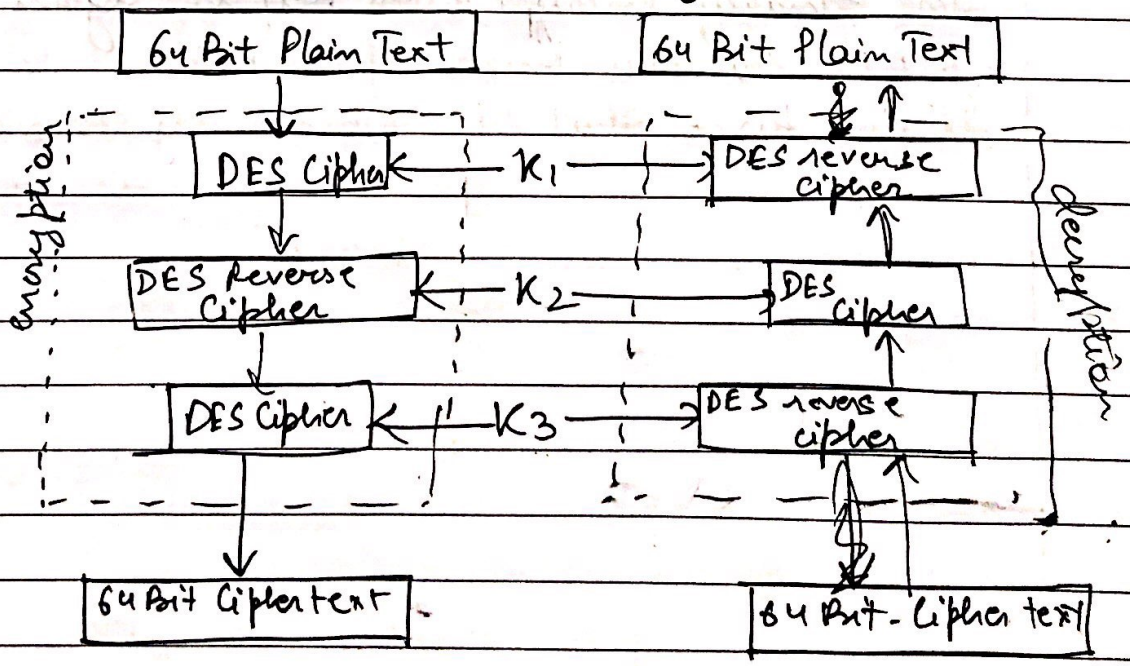
Shortcoming of DES is that it uses 56 Bit key which means key space is relatively small. To overcome this, we run DES multiple times each using different key.

There are two variants of Triple DES :-

(i) 3-key Triple DES
(ii) 2-key Triple DES

(i) 3 key Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 & K_3. This means that the actual 3TDES key has length of $3 \times 56 = 168$ Bits.



The encryption-decryption process is as follows:-

(i) Encrypt the plaintext blocks using single DES with key K_1.

(ii) Now decrypt the output of step 1 using single DES with Key K_2.

(iii) Finally, encrypt the output of step 2 using single DES with key K_3.

(iv) The output of step 3 is the cipher text.

(v) Decryption of a ciphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2 & finally decrypt with K_1.

(ii) 2 Key Triple DES

Second variant of Triple DES i.e. 2TDES is identical to 3TDES except that K_3 is replaced by K_1 in another words, user encrypt plain text blocks with key K_1, then decrypt with key K_2 and finally encrypt with Key K_1, again. Therefore 2TDES has key length of 112 Bits.
It does twice that DES normally does only once.

__/__/____

Blowfish

Blowfish is an encryption method that is very strong weapon against hackers and cyber-criminals. Used in a wide array of products ~~boasting~~ including

- Some Secure e-mail encryption tools.
- Backup software.
- password management tools

Blowfish is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms.

It is a symmetric block cipher that uses a variable-length key from 32 bits to 448 Bits.

Blowfish uses a unique form of key generation. The second part of the blowfish routine is a key expansion that converts a single key of up to 448 Bits into a table of subkeys i.e. 4168 Bytes in size.
The creation of subkeys further increases security, because a hacker would have to crack more than just the original key.

Strength of Blowfish

- Blowfish is an incredibly fast cipher that has a relatively simple structure & is very effective.
- Blowfish generates a really large key and this alone is a huge benefit to security.

IDEA

Full form of IDEA is "International Data Encryption Algorithm".

Elements of IDEA:-

- Key size = 128 Bits
- Block size = 64 Bits
- Round = 8
- Complex functions replace s boxes
- Highly resistant to cryptanalysis.

RC5

RC stands for 'Rivest Cipher".

- RC5 has a variable block size (32, 64 & 128 bits)
- Key size (0 to 2040 Bits)
- No. of rounds (0 to 255)

Confidentiality using Symmetric Encryption

Placement of encryption function has two approaches:

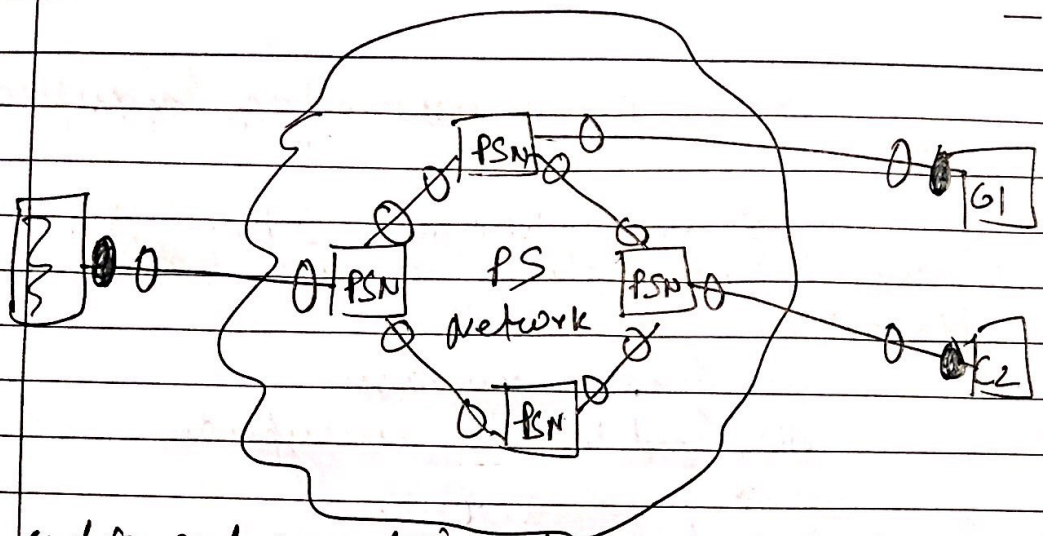
(i) Link Encryption
(ii) End to end encryption

Link to link Encryption

With link encryption, each vulnerable communications link is equipped on both ends with an encryption device. Thus, all traffic over all communication links are secured.
One of its disadvantage is that the the message must be decrypted each time it enters a switch because the switch must read the address in the packet header in order to route the frame. Thus, the message is vulnerable at each step.

End to end encryption

With end to end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data in encrypted form are then transmitted unaltered across the network to the destination terminal or host. The source shared a key with the destination & so is able to decrypt the code. One of its disadvantage is that it does not ensures that the traffic link or pattern is secure or not, because packet headers are transmitted in the clear.



● = end to end encryption device
○ = link encryption device
PSN = Packet switching node

Link Encryption	End to End Encryption
(i) In encrypts all the data along a specific communication path. No only the information is encrypted, but the header, address etc. that are part of the packets are also encrypted.	(i) The header, trailers, routing and addresses are not encrypted enabling attackers to learn more about captured packet and when it is headed.
(ii) Works at physical & Data link layer in OSI model.	(ii) Works at Network layer & above.

Traffic analysis of Traffic Confidentiality

1) In packet-switching Network, the packet header cannot be encrypted.
2) Monitoring of communications flows b/w parties.
3) Link encryption obscures header details.
4) Traffic padding can further obscure flows
5) Traffic analysis reveals -
   (i) identities of partners
   (ii) How frequently the partners are communicating
   (iii) message pattern, message length, quantity of message etc.

Key Distribution

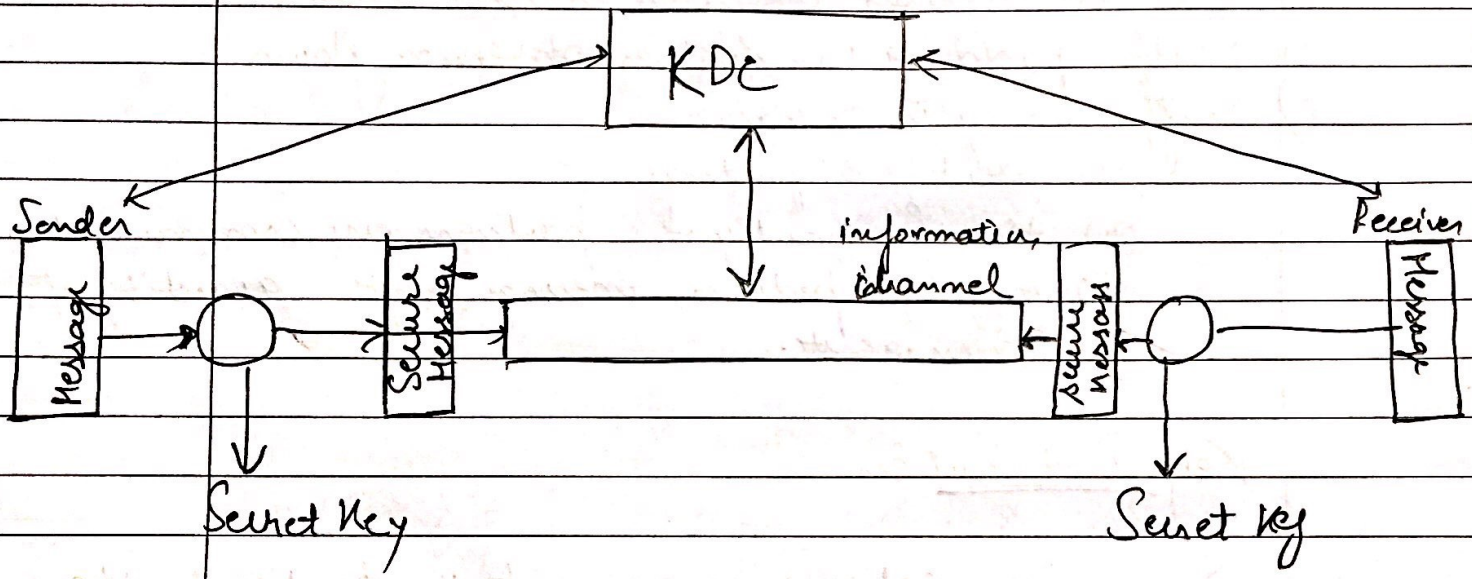
(i) Symmetric schemes require both parties to share a common secret key.
(ii) But the issue is how to securely distribute this key. Here are some alternatives of Key distribution b/w the given parties A & B.

a) A can select key & physically deliver to B
b) Third party can select & deliver key to A & B.
c) If A & B have communicated previously can use previous key to encrypt a new key.
d) If A & B have secure communications with a third party C, C can relay b/w A & B.

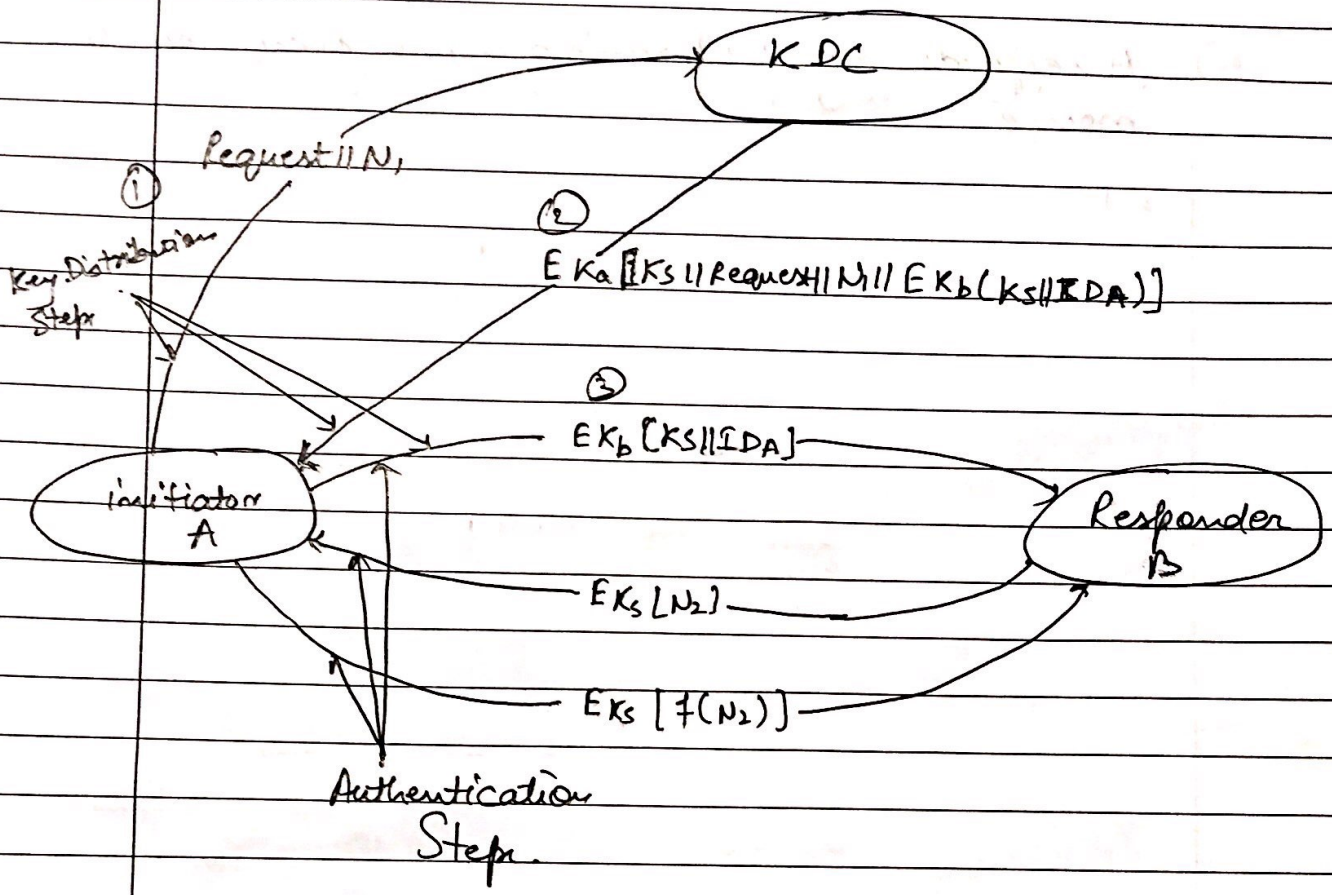
__/__/____

Key Distribution Centre (KDC)

KDC share a unique key i.e. master key with each user to distribut ~~session~~ secret key (session key) b/w ~~a~~ a pair of users.



Key Distribution Scenario



1) A issues a request to the KDC for a session key.
   (i) Nonce is also sent
   (ii) Nonce includes identities of communicating parties and a unique value.

2) KDC sends a response encrypted with A's secret key K_A.
   (i) It encludes one time session key Ks
   (ii) Original request message, include the nonce
   (iii) Message also included Ks and ID of A encrypted with ~~secret~~ with K_B intended for B.

3) A stores Ks and forwards ~~the~~ information for B i.e. $E K_b [K_s || I D_A]$

4) B sends a nonce to A encrypted with Ks

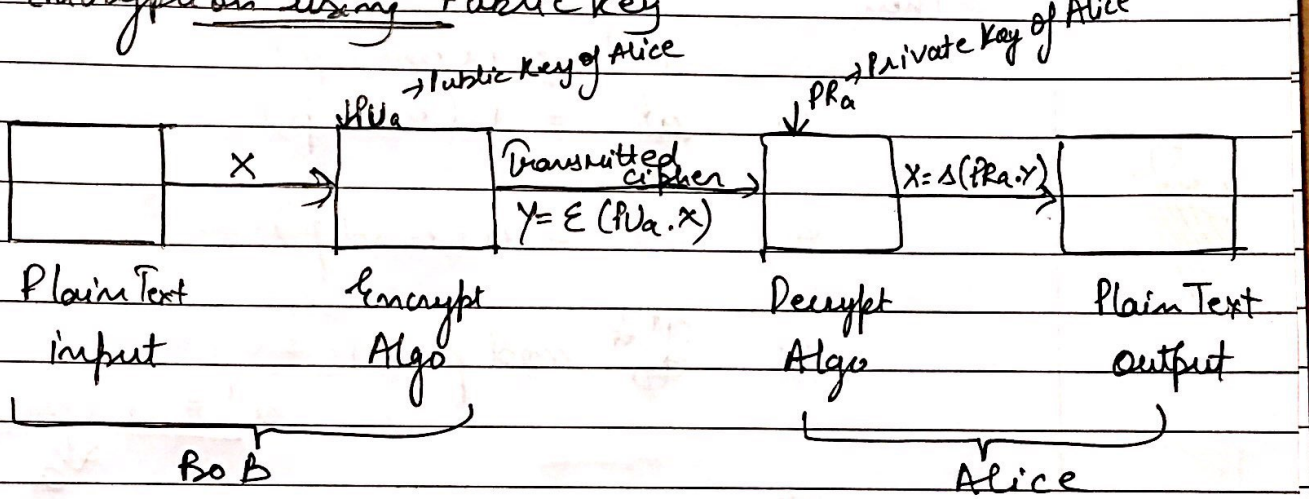
5) A responds by performing some function on nonce.

__/__/____

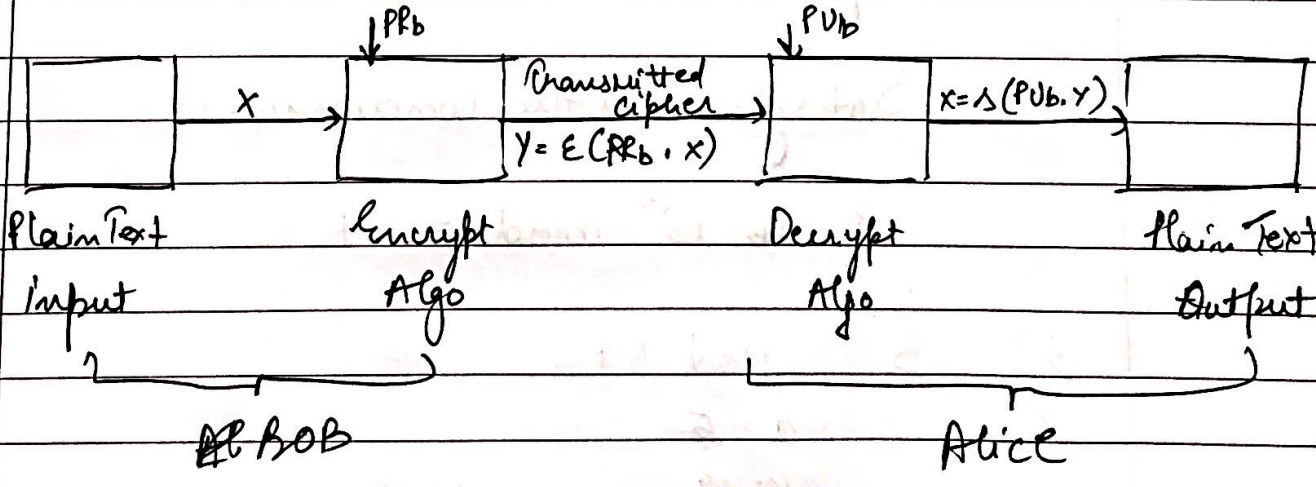
Assymetric Encryption or Public Key Cryptography

- Plaintext
- Encrypt Algo
- Public & Private Key
- Cipher text
- Decrypt algo.

Encryption using Public key



Encryption using Private Key



Number theory

★ Fermat's theorem

- p is prime
- 'a' is a +ve integer not divisible by p
  i.e. (gcd (a, p) = 1)

then

$$a^{p-1} \equiv 1 \pmod{p}$$

or $$\frac{a^p}{p} \equiv 1 \pmod{p}$$

or $$a^p \equiv a \pmod{p}$$

or $$a^{p-1} \bmod p = 1$$

$$a^p = a \pmod{p}$$
$$\frac{}{a}$$

eg. i) $13^{16} \bmod 17$

$a = 13$

$p = 17$

Satisfies all the conditions.

$\therefore 13^{16} \bmod 17 = 1$

2) 5^{18} Mod 19

$a = 5$

$p = 19$, $p - 1 = 18$

5^{18} Mod $19 = 1$

3) $5^{20} \mod 19$

$5^{19 \times 1 + 1} \mod 19$

$\Rightarrow 5^{19} \cdot 5^{1} \mod 19$

$\Rightarrow 5^{19} \mod 19 \cdot 5 \mod 19$

$\Rightarrow 5 \cdot 5$

$\Rightarrow 25$

$a^p \mod p = a$

1) left hand side is smaller than right hand side then the left hand side is the answer

3) $13^{15} \mod 15$

$\Rightarrow 13$

4) $13^{15} \mod 17$

$p = 17$

$a = 13$

prime but $17 - 1 \neq 15$

Soln: Fermat's theorem will not be applied.

Ans

Euler's theorem

a & n are relatively prime

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Where $\phi(n)$ is Euler Totient function.

Eg. $\phi(10)$ Factors (10)

~~2, 5~~

~~1~~ (1)
~~2~~
~~3~~ (2)
~~4~~
~~5~~
~~6~~
~~7~~ (3)
~~8~~
~~9~~ (4)
~~10~~

$\therefore \phi(n) = 4$

Case I

if n is prime

$$\phi(n) = n-1$$

Eg. if $\phi(7) = 6$

Case II

If n is the product of two prive No.s i.e. p, q
Then,

$$\phi(n) = \phi(p) \times \phi(q)$$
$$= (p-1) \times (q-1)$$

Eg. $\phi(21) = \phi(7) \times \phi(3)$
$= 6 \times 2$
$\phi(21) = 12$

Case III

If $n = p^e$
where p is prime

Then $\phi(n) = p^e - p^{e-1}$

Eg. $\phi(8) = \phi(2^3)$
$= 2^3 - 2^2$
$= 8 - 4$
$\phi(8) = 4$

RSA Algorithm

Most popular public key name after three scientists i.e. Rivest, Shamir, Adleman.

Algo:-

Key Generation process

- Consider two large prime nos. p, q
- Calculate $n = p \times q$
- Euler's Totient Function:-
$$\phi(n) = (p-1) * (q-1)$$
- Assume 'e' (public key used for encryption)

  e is such that $gcd(e, \phi(n)) \equiv 1$
- Assume 'd' (private key used for decryption)

  d is such that
$$d \equiv e^{-1} \bmod \phi(n)$$
i.e.
$$d \times e = 1 \bmod \phi(n)$$
$$d \times e \bmod \phi(n) = 1$$

- Public key = $\{e, n\}$
- Private key = $\{d, n\}$

Encryption

$M < n$ (M = Original message)

cipher text, $c = M^e \bmod n$

__/__/__

Decryption

$M = c^d \text{ Mod } n$

Q. consider $p = 7$ and $q = 3$

$n = p \times q$

$n = 21$

$\phi n = (p-1) \times (q-1)$

$= 6 \times 2$

$\phi(n) = 12$

Now, assume $e = 5$

i.e. e, $\gcd(e, \phi(n)) = 1$

$\gcd(5, 12) = 1$

Now d,

$d \times e \text{ Mod } \phi(n) = 1$

$d \times 5 \text{ mod } 12 = 1$

$5 \times 5 \text{ Mod } 12 = 1$

$25 \text{ Mod } 12 = 1$

152380

public Key = {5, 21}

private Key = {5, 21}

Encryption

$M = 20$

$C = M^e \text{ Mod } n$

$= 20^5 \text{ mod } 21$

$= 3200000 \text{ mod } 21$

$\boxed{C = 20}$

Decryption

$M = C^d \bmod n$

$= 20^3 \bmod 21$

$= 32000 \bmod 21$

$M = 20$

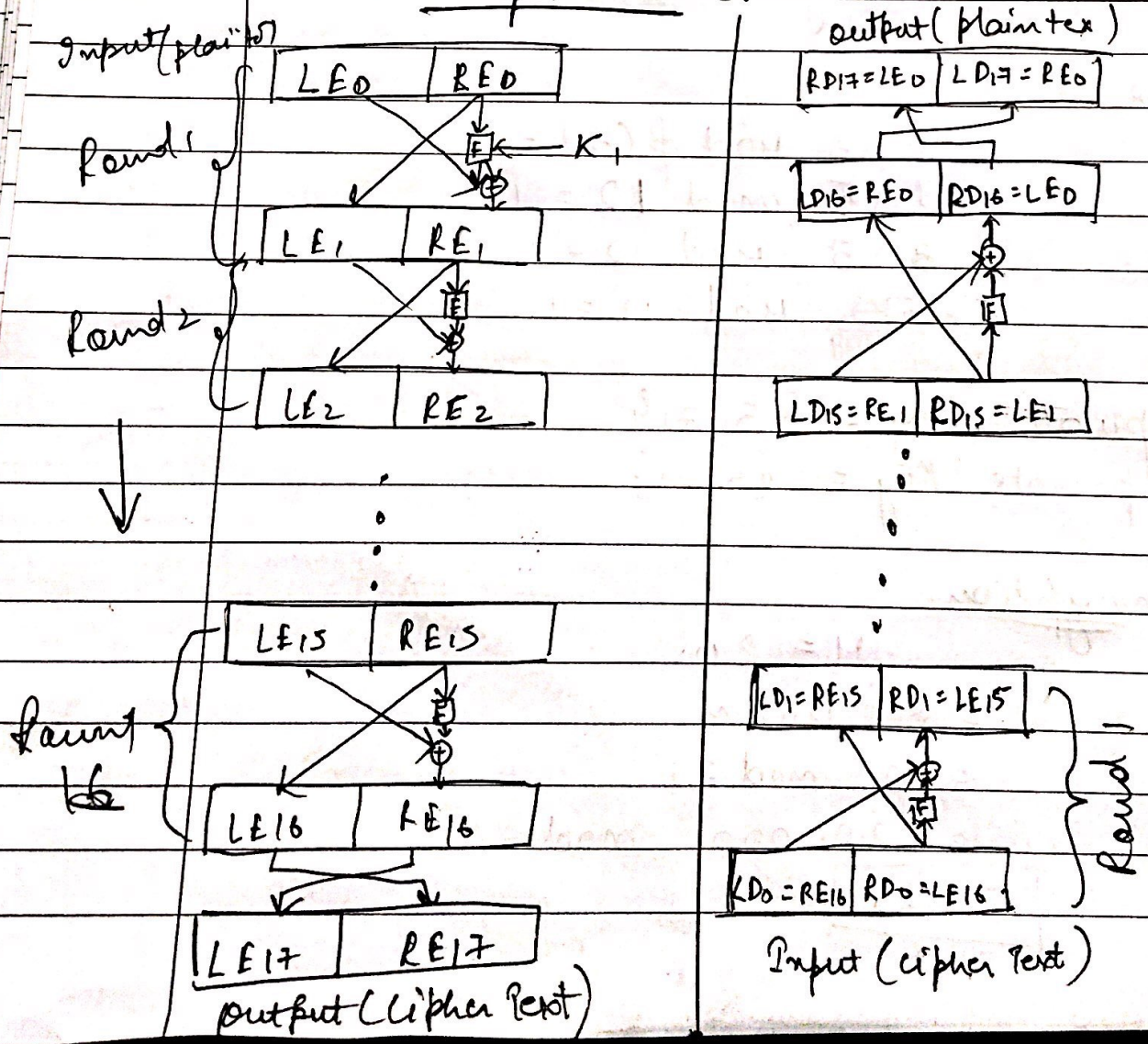
for calculating mod.

Eg. ~~b mod a x mod b~~

(i) ~~divide b/a b = a~~

(ii) ~~subtract the~~

Feistel Cipher Structure



Cryptanalysis

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.

Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximation to the actions of the cipher. Attacks have been developed for block ciphers & stream ciphers.

Differential cryptanalysis is the study of how differences in information input can affect the resultant difference at the output.