Date / /

→ Cryptography ⟶ Network Security

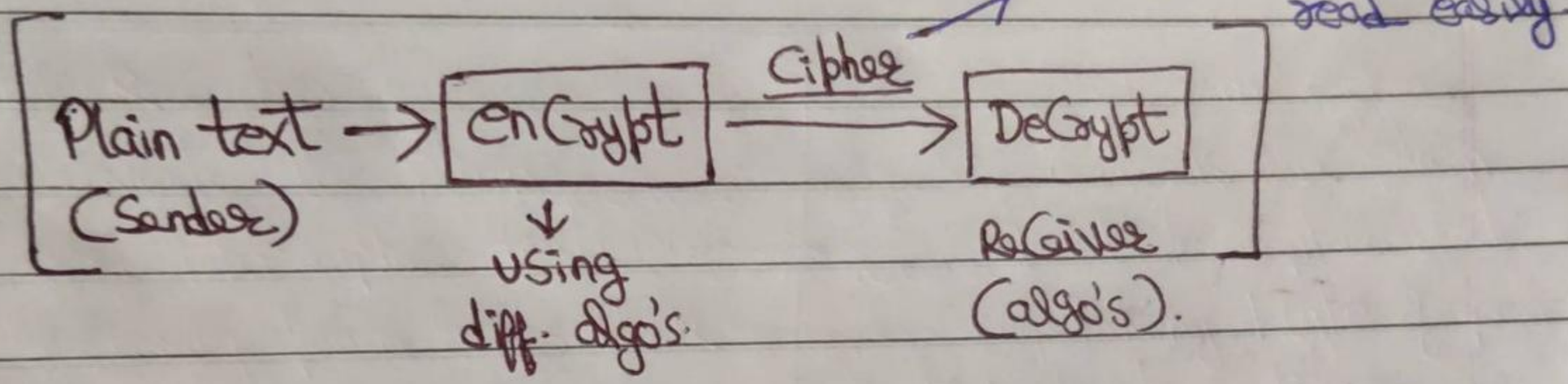
→ Types of Cryptography ↗ Symmetric
↘ Asymmetric

→ Matrix

→ CIA

→ Attacks ↗ Passive
↘ Active

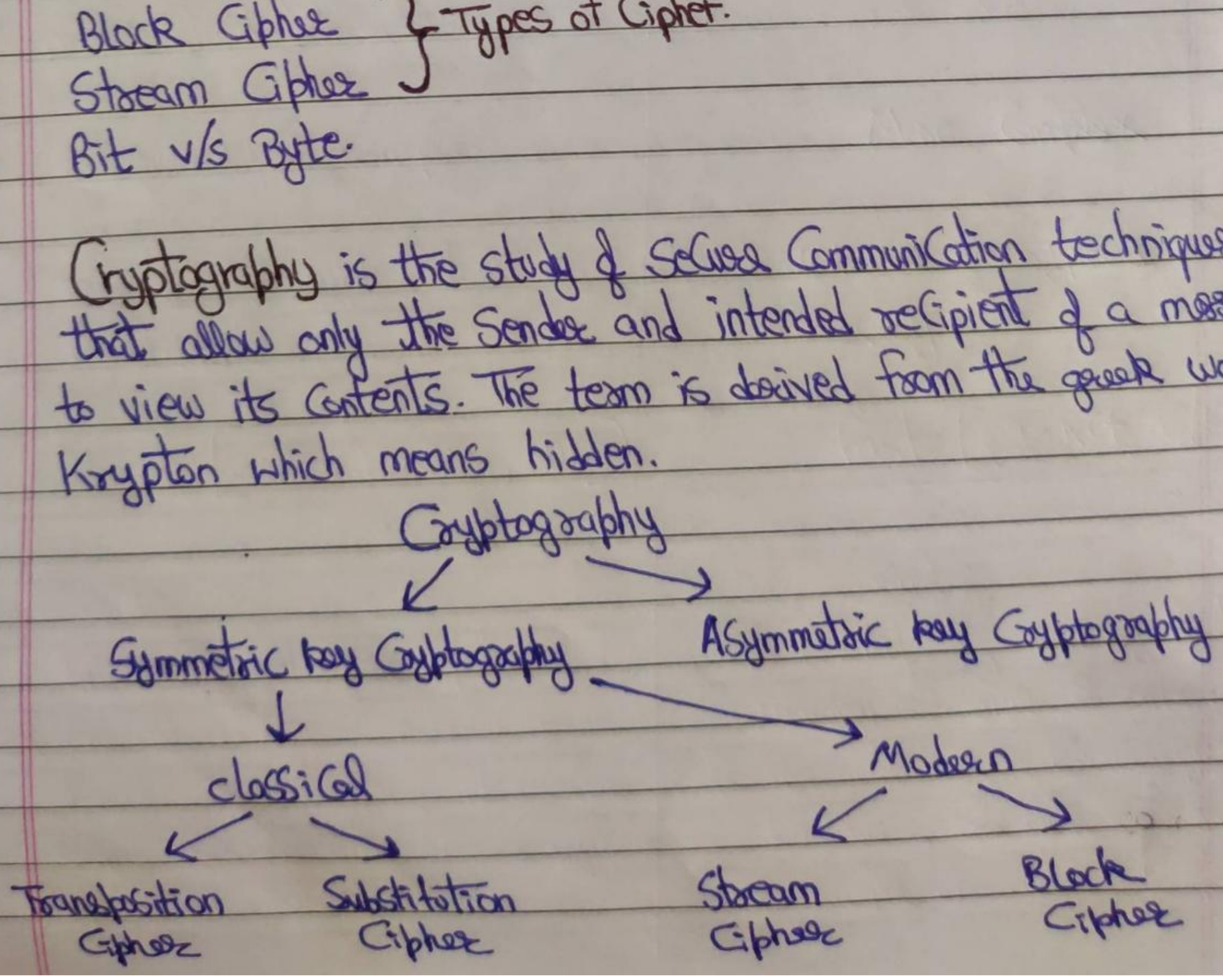
→ EnCrypt. deCrypt. Cipher.

→ 

Block Diagram

→ Block Cipher } Types of Cipher.
→ Stream Cipher
→ Bit v/s Byte.

Cryptography is the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the greek word Krypton which means hidden.



Date / /

Public Key Cryptography / asymmetric Cryptography is a Cryptograph System that uses pairs of keys. The generation of such key pairs depend on Cryptographic algorithms which are based on mathematical problems termed one-way functions.

Symmetric Cryptography / Secret Key Cryptography is the use of a single based shared secret to share encrypted data between parties - Ciphers in this category are called Symmetric because you can use the same key to encrypt and to decrypt the data.

CIA Triad - Confidentiality, Integrity, Availability.
Confidentiality ensures that data is accessible to only those th have authorized access.
Integrity ensures that data is maintained and that no unauthorize changes have been made to the data.
Availability ensures that systems that store and process data are accessible to authorized users when needed.

Attacks is a method for circumventing the security of a Cryptographic system by finding a weakness in a code, cipher, Cryptographic protocol or key management scheme. Attacks are typically categorized based on the action performed by the attacker. An attackers, thus can be passive or active.

In an active attack, an attacker tries to modify the content of the messages.
In a passive attack, an attacker observes the messages and copies them.

Decryption is the process of converting cipher text back to plain text.

Date / /

EnCryption is the process of translating plain text data (plain text) into something that appears to be random and meaningless (Cipher text).

Cipher is an algorithm for performing enCryption or deCryption - a series of well defined steps that can be followed as a procedure.
A Cipher converts the original message, called plain text into Cipher text using a Key to determine how it is done.

Block Cipher	Stream Cipher
Converts the plain text into Cipher text by taking plain text's block at a time	Converts the plain text to Cipher text by taking 1 byte of plain text at a time.
Uses either 64 bits or more than 64 bits.	Uses 8 bits.
Complexity is simple.	More Complex.
reverse enCrypted text is hard.	reverse enCrypted text is easy.
Slow. [E.g- AES, DES, 3DES)	fast. [E.g- RC4, A5/1, FISH, etc

Bit	Byte
Smallest unit of Computer Information. It's essentially a single binary data point; either yes or no, on or off, up or down.	unit of memory that usually contains 8 bits. This is because historically, 8 bits are needed to encode a single character of text.

Date / /

Plain text (Sender) → EnCryption algorithm i.e. Key → Cipher (unSecure channel) → DeCryption 'Key' → Plain text (Receiver)

* Cryptography is the Science of writting in SeCret Code so that no other person except the intent receipient Could read.

* Crypto means hidden SeCret and graphic means to write or study

* Cryptography is the Practice and Study of technique for SeCure Communication in the presence of third party.

* More generally it is about Constructing and analyzing protocols tha overCome the influence of attacker or outside people and which are related to various aspect in information SeCurity. Such a data Confidentiality, data integrity, authentiCation.

Applications of Cryptography

It includes ATM Cards, Computer passwords, etc.

* It is the Science of using mathematic to enCrypt or deCrypt the data. It enables you to store Sensitive information or transmit it aCCross inSeCure channel (network).

Types of Cryptography -

1. Symmetric Key Cryptography (Same Key) / Private / SeCret Key Cryptograph

Key methods - DES, 3DES, AES.

Date / /

Plain text → Sender → EnCryption (we use various algorithms) → unsecure channel → DeCryption → Receiver → plain text

$C[K1[M]] \xrightarrow{\text{Cipher text}} M=[K1[C]]$

C = Cipher Text
K1 = Key
M = Message (Plain text)

2. Asymmetric Key Cryptography or (Public Key Cryptography)

Plain Text → Sender (enCryption) → unsecure channel → Receiver (DeCryption) → Plain Text

A: 'A' Public Key, 'A' Private Key
B: 'B' Public Key, 'B' Private Key

Steganography

Case –

1. A = E ['A' Public Key [M]] Send to B.
2. A = E ['B' Private Key [M]] Send to B.
3. A = E ['A' Private Key [M]] Send to B.

(Confidentiality not achieved)

4. A = E ['B' Public Key [M]] Send to B. ✓ right

Note: Always use Receiver Public Key to encrypt the message.

Date / /

Symmetric Key Cryptography-

Also Known as private Key / Secret Key Cryptography.

In Symmetric Key Cryptography, a Single Key is used for both enCryption and deCryption.

⇒ AES (Advanced EnCryption System) - most widely used Symmetric Key Cryptography.
(DES, 2DES, 3DES)

→ The Symmetric Key System has one major drawback that two parties must exchange the Key in a Secure way. As there is only one Single Key for enCryption as well as deCryption.
i.e. $P = [D[K, E(P)]$

Where, K = Key for both (enCryption & deCryption)
M/P = plain Text
D = DeCryption
E(P) = EnCryption for plain Text.

Steganography-

The action or Process of writting in shorthand and transcribing the shorthand on a typewriter.

Advantages of Symmetric-

* It is faster.

* EnCrypted data Can be transfered on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being deCrypted are null.

* A Symmetric uses Password authentication to Prove the receiver's Identity.

* A system only which possesses the Secret Key can decrypt a message.

Disadvantages of Symmetric-

* Have a Problem of Key transportation. The Secret Key is to be transmitted to the receiving System before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging Keys would be exchanging them personally.

* Cannot Provide digital Signatures that cannot be repudiated.

Advantages of Asymmetric-

* In Asymmetric or public Key Cryptography, there is no need for exchanging Keys, thus eliminating the Key distribution Problem.

* The primary advantage of public Key Cryptography is increased security; the private Keys do not ever need to be transmitted or revealed to anyone.

* Can Provide digital Signatures that Can be repudiated.

Disadvantages of Asymmetric-
for encrypting is speed; there are popular secured-Key

Date / /

encryption methods which are significantly faster than any presently available public-key encryption method.

→ Security Service-

1. Confidentiality
2. integrity
3. Authentication → (Password).
4. Non-repudation → (Proof of access)
5. Access Control

Asymmetric Key Cryptography-

Asymmetric Key also known as public Key Cryptography or Conventional Cryptography.

In this, two Keys are used for encryption and decryption.

$$P = D(K_d, E(K_e, P))$$

Crypto System (Cryptography)-

A System which Convert plain text to Cipher text by the application of encryption or decryption algorithms.

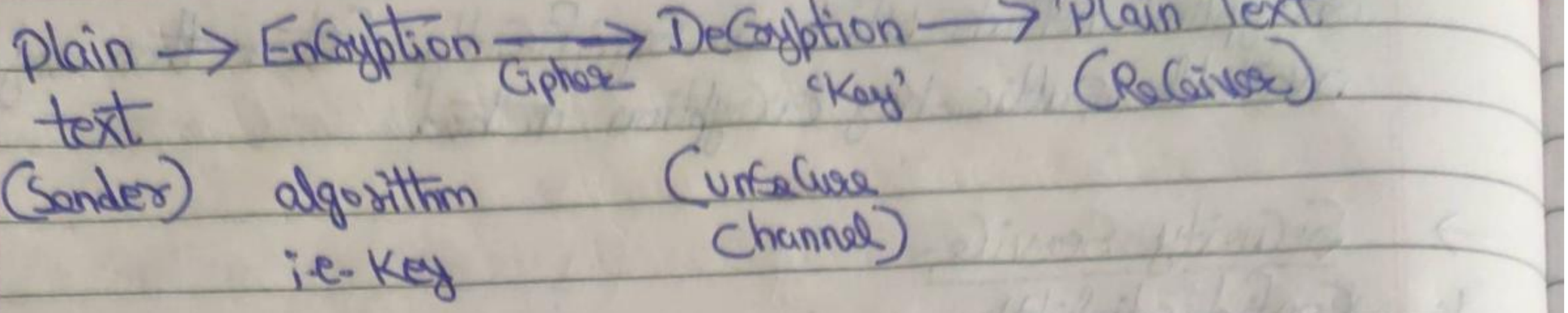
The Key generation for encryption and decryption algorithm is also a part of a CryptoSystem.

OR

A CryptoSystem is an implementation of Cryptographic techniques.

Diagram Same as CryptoSystem.

Date / /



Plain Text -
This is the data that needs to be protected.

EnCryption Algorithm -
This is the mathematical algorithms that takes plain text as the input and return Cipher text.
It also Produce the unique enCryption Key for the text.

Cipher Text -
This is the enCrypted or unreadable form of the plain text.

DeCryption Algorithm -
This is the mathematical algorithm that takes Cipher text as the input and deCode it into plain text or original text.
It also use the unique deCryption Key for the text.

EnCryption Key -
This is the value known to the Sender that is used to Compute the Cipher text for the given plain text.

DeCryption Key -
This is the Key known to the receiver that is used to deCode the given Cipher text to plain text.

Note - challenges of Symmetric Key Cryptosystem.

Date / /

1. **Key Establishment -**
Before any Communication, both the Sender and receiver needs to agree on a Secret Symmetric Key.

2. **Trust Issue -**
Since the Sender and the receiver use the Same Symmetric Key, there is an implicit requirement that the Sender and the receiver trust each other.

Security Goals - (CIA Triads in Cryptography)

Confidentiality (Privacy) -

* It is the most Common aspect of Information Security.

* It allow authorised user to access Sensitive and protected data. The data Sent over the network should not be accessed by unauthorized user.

* Attackers will try to Capture the data. So to avoid this, various encryption techniques are used. To Save our data So that even if attacker gain access, he or she will not be able to decrypt it.

Integrity -
means that changes need to be done by the authorized entity and through authorized mechanisms. and nobody else Should modify our data.

Date / /

Availability -

Data must be available to the authorized user.
Information is useless if we cannot access it.

What would happen if we cannot access our bank account for transaction?

Cryptographic Attack

- Cryptanalytic attack
  - by absorbing Info
  - Bruteforce Attack (on short Period)
  - Dictionary Attack (on long Period)
- Non-Cryptanalytic attack
  - Security attack
    - Passive
    - Active
  - Security mechanism
  - Security Service

Threat of Confidentiality

- Spoofing (absorb plain message)
- Traffic (analytic absorb Cipher)

Threat of Integrity

- Modification attack (by change in message)
- Masquerading attack (fake account)
- Reputation attack (clearly No) / (without proof)
- Replay attack (misuse of message in future)

Threat of Availability

- Denial of Service

Date / /

Attack

Attack is any attempt to explore, alter, destroy, steal or gain information through unauthorized access.

Bruteforce Attack - It uses trial and error to guess login info, encryption key or find hidden web page.
e.g → Crack, Hydra, rainbow Crack, etc } → Tools

Security Attack - OST Security model focus on 3 basic aspect of Network Security.
→ Security Attack
→ Security Mechanism
→ Security Service

3 goals of Security (CIA) can be threaten by security attacks.

Security Attack

Threat of Confidentiality	Threat of Integrity	Threat of Availability
→ Traffic Analysis → Snooping: It is unauthorized access to data or information	→ Modification → Masquerading → Repatation → Replay attack	→ Denial of Services

⇒ Threat of Confidentiality
Traffic analysis → we encrypt the information so that the attacker even if captures the message, could not extract any information from the message. e.g → Netflow analyzer, Microsoft message analyzer.

Date / /

⇒ Threat of Integrity

Threat of Modification → After accessing the info, the attack alter the message or that message could be delayed or delete clone by unauthorized user.

Masquerading attack (Spoofing) → It happen when the attacker (Pretend) impersonate somebody else i.e. one entity pretend to be a different entity.
eg. → A user try to contact a bank but another site pretend it is the bank & obtain information.

Replay (Play back attack) → The attacker obtain a copy of a message send by a user and later try to replay or resend/delay it.
eg. → Text dependent speaker verification.

Reputation → It can be done by the sender or receiver. The sender of the message might later denied that he has send the message, the receiver of the message might later denied that he has received the message.

⇒ Threat of Availability

Denial of Services → An attempt to make a server/machine or network resources unavailable to inext user.

Passive Attack → In passive attack, it attempt to learn or make use of the information from the system but does not affect the system resources that is the attacker will only see the data. he will not modify it.
we can prevent it using better encryption techniques.

Date / /

Types of Passive attacks:

1. Release of message Content (Bruteforce Attack) → The Attacker will easily able to understand the data or information.

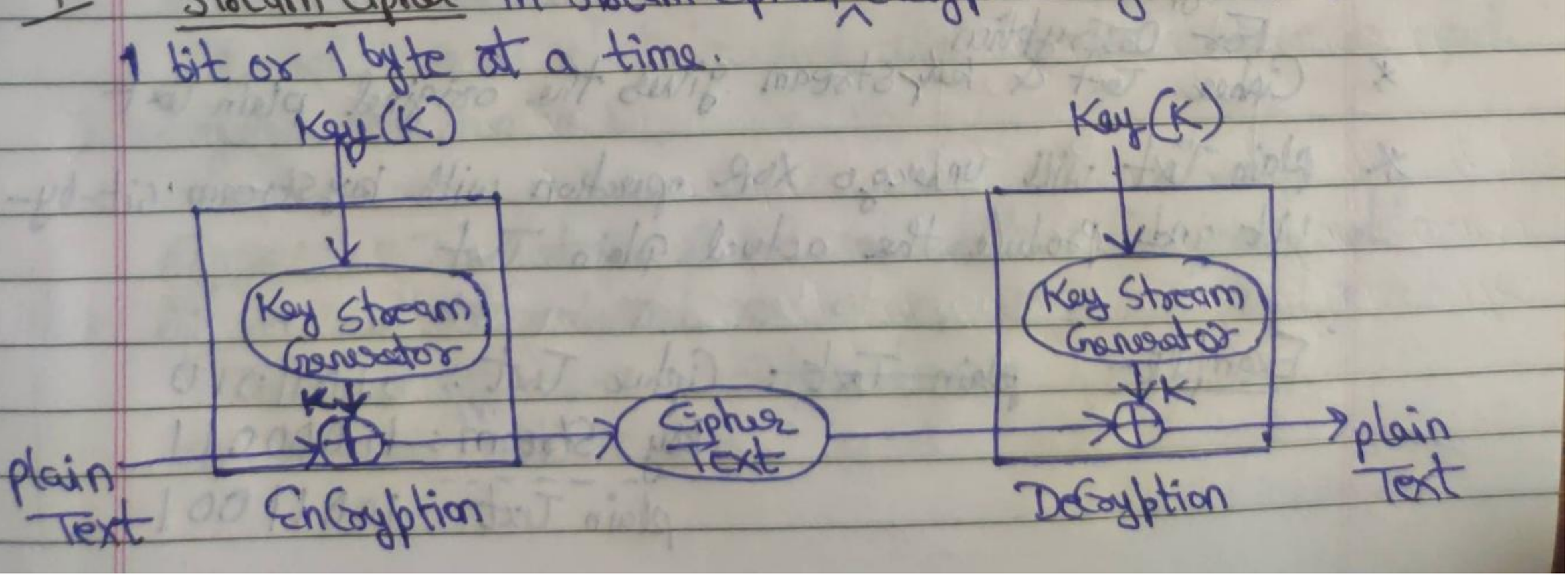
2. Traffic Analysis - If we have Encryption Protection, and attacker might still be able to see the patter & the messages. The attacker could determine the location and identity of communicating host and could observe the frequency and length of the message being exchanged.

Active Attack → It attempt to alter system resource and information.

Symmetric Key Cipher-
In a Symmetric Key Cipher, both sender and receiver during communication share the same Key.
e.g → AES (Advanced Encryption standard), DES (Data Encryption Standard), IDEA (International data Encryption Algorithm)

There are two kinds of Symmetric key Ciphers -
① Stream Cipher
② Block Cipher

1. Stream Cipher - In stream Cipher, encrypt a digital data stream in 1 bit or 1 byte at a time.



Date / /

Stream Cipher Example

```
01000001101001010010010 Plain text
10100101001101011101101 Cipher Stream
-----------------------
11100100100100001111111 Cipher Text
```

Bits are different so result is 1

Bits are same so result is 0.

Plain text = Key stream ⊕ Cipher

Encryption:

For Encryption,

* plain text and Key Stream produces Ciphar Text (same Keystream will be used for decryption.)
* The plain text will undergo XOR operation with Key stream bit-by-bit and Produces the Cipher Text.

Example- plain Text : 10011001
Key stream: 11000011
Cipher Text : 01011010

Decryption:

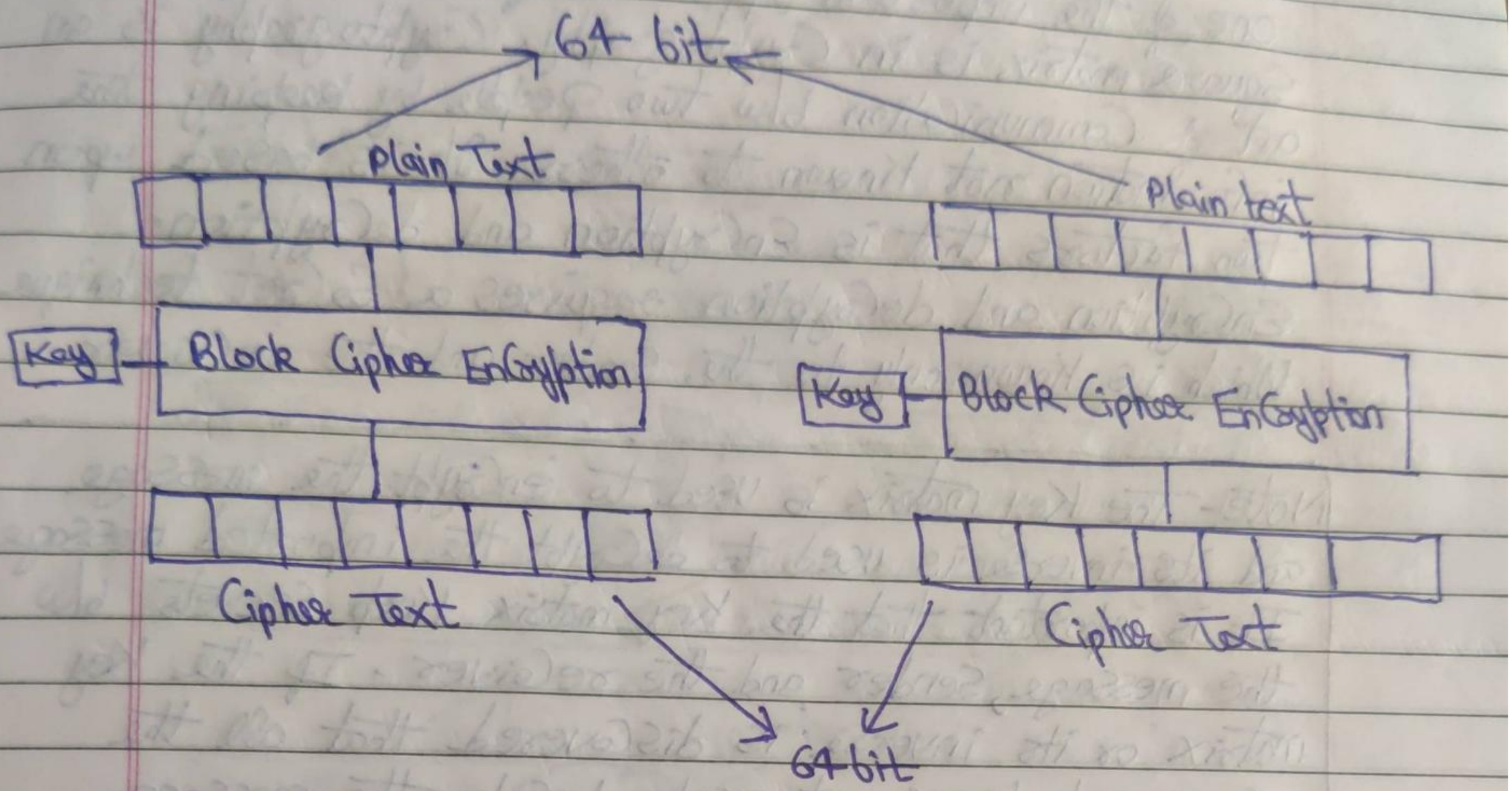
For Decryption

* Cipher Text & key stream gives the original plain text
* plain Text will undergo XOR operation with keystream bit-by-bit and produce the actual plain Text.

Example- ~~plain Text~~: Cipher Text : 01011010
Key Stream : 11000011
plain Text : 10011001

Date / /

Block Ciphers:



Q. Diff b/w stream and Block Cipher.

Q. $-50 \bmod 10$

How to find modulus of Congruent numbers-

e.g. → $n \bmod m$

method → $n = q \times m + r$

n or m is given, n or m are Integer nos.

r = remainder

q = we have to choose 'q' such that we get a more or equal negative no. than n

Congruent - Two Integers A & B are said to be Congruent modulo n if $a \bmod n = b \bmod n$

This is written as → $a \equiv b \bmod n$

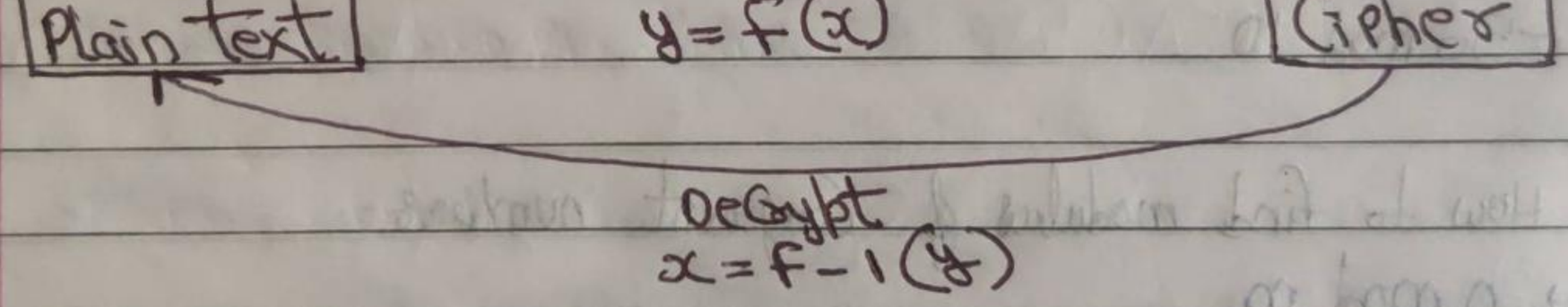
or $b \equiv a \bmod n$

Date / /

Matrix in Cryptography

One of the important application of inverse of the Square matrix is in Cryptography. Cryptography is an art of Communication b/w two people by keeping the information not known to others. It is based upon two factors that is Encryption and decryption. Encryption and decryption requires a secret technique which is known only to the sender and the receiver.

Note- The Key matrix is used to encrypt the message and its inverse is used to decrypt the imported message. It is important that the Key matrix keep secrets b/w the message, Sender and the receiver. If the Key matrix or its inverse is discovered that all the users or hackers get easily decode the message.



Example:

Let the encoding matrix be:

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

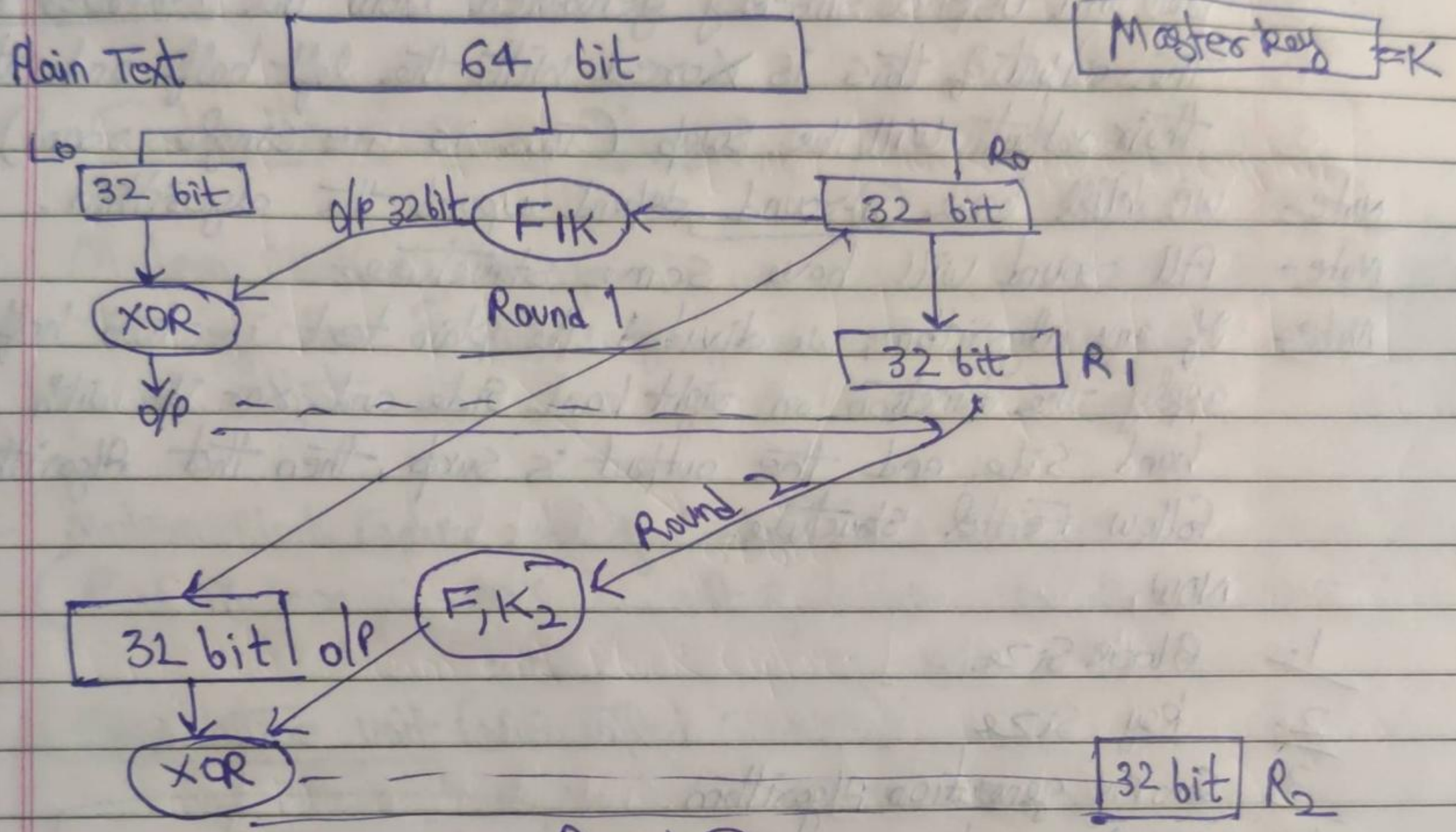
Let the message to be sent by the Sender the Welcome

Q. Encrypt the message COVID using the Encryption matrix:

Date / /

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$. Hence decode the received message using the corresponding message.

Feistel Cipher Structure



1. Feistel Cypher is not a specific scheme of Block Cipher. It is a designed model from which many different Block Ciphers are derived.

2. DES is just one example of Feistel Cipher
3. A Cryptographic System based on Feistel Cipher structure uses the same algorithm for both Encryption and decryption.
4. In the Feistel Block Cipher, each Block has to undergo many rounds whose each round has the same function.

Functions of Feistel structure

Date / /

1. The plain text is divided into two equal halfs - L_0 & R_0.
2. The two half of the data pass through n-round of Processing and then Combine to produce the Cipher text. Block.
3. on the Right half, we apply a function and in the function we will use a Sub-key generated from the Master Key. The output of this is Xored with the left half and then their output will be Swap (This is one Single round).

Note- we Will have (n)-round, depend upond the algorithm.

Note- All round will have Same Structure.

Note- If any algorithm, we divided the plain text in two half and apply the function on right hand Side and xor it with left hand Side and the output is Swap, then that Algorithm follow Feistel structure.

Now,

1. Block Size
2. Key Size
3. Sub-key generation Algorithm
4. No. of rounds
5. Round function

1. Block Size - Longer Block Size means more Security.
2. Key Size - Longer Key Size means more Security. (But It may decrease the processing of Encryption & decryption.)
3. No. of rounds - More rounds, more Secure.
4. Sub-key generation - More Complex algorithm, difficult for attacker to store data.
5. Round function - More Complex function, harder for the Crypt analysis to attack.

Date / /

EXAMPLE:

Let the encoding matrix be:

PREPARE TO NEGOTIATE

and the encoding matrix be:

$$\begin{bmatrix} 3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

Components of Block Cipher

1. Modern Block Cipher normally are Key Substitution Cipher in which the Key allow Partial mapping from the possible input to the possible output.

2. Modern Block Cipher made of Combination of Transposition (Permutation) (P-BOX or D-BOX). unit & diffusion (Called D-Box).

Substitution unit (Also Called S-BOX)

* **Types of Transposition**

3. A Symmetric Key modern Block Cipher Encrypt n-bit block of plain text or decrypt n-bit of Ciphee text.

4. The Encryption or decryption algorithm use a n-bit key (will be same for both)

Substitution and Transposition Cycle

1. A Modern Block Cipher Can be design to either act as a Substitution Cipher or Transposition Cipher.
2. Traditional Ciphee unlike the Symbol to be Substituted or Transposed bit insted of character.

Date / /

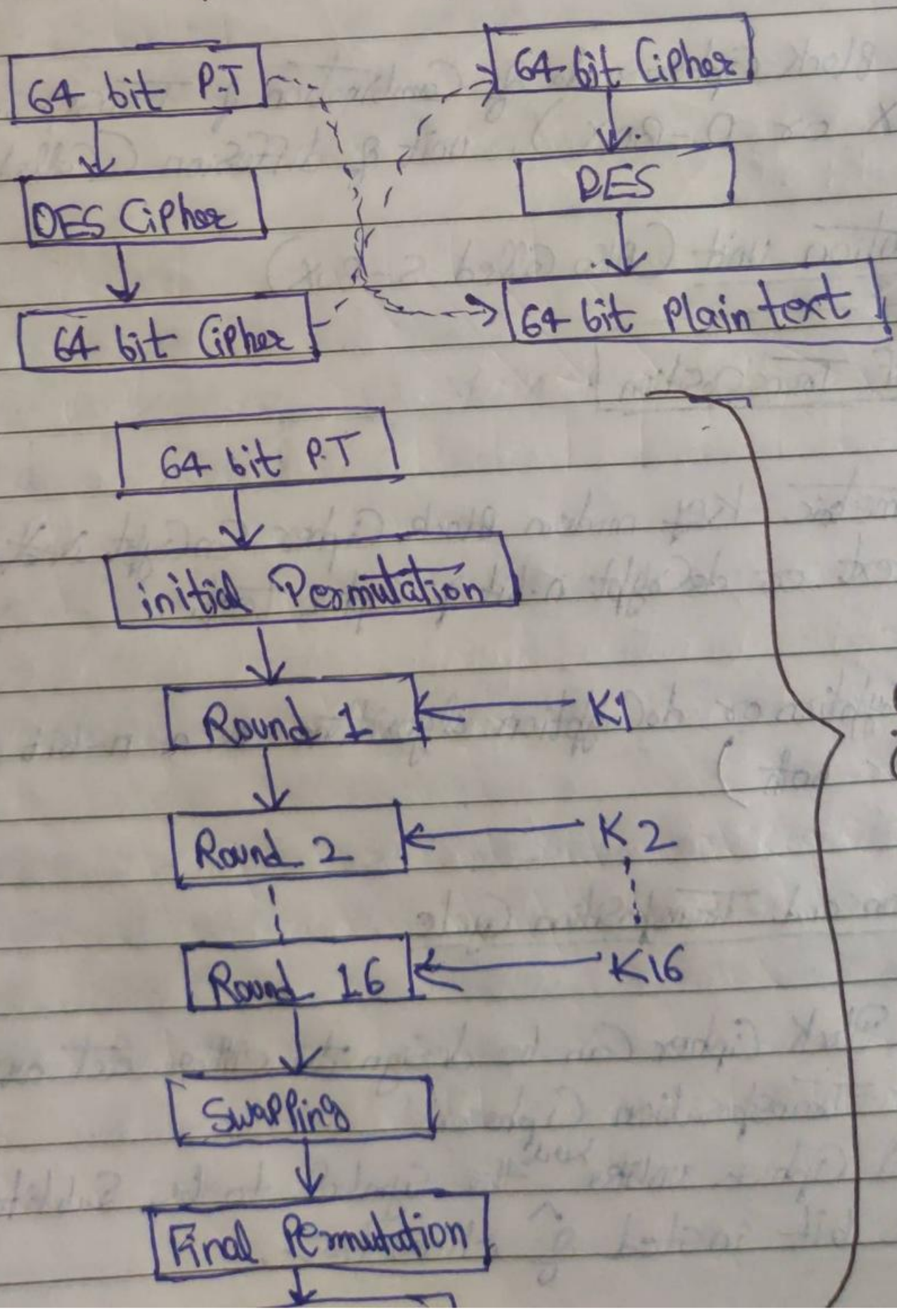
Note: Modern Block Cipher are designed as Substitution Cipher.

Note: Substitution Techniques:

1. Caesar Cipher
2. Monoalphabetic Cipher
3. playfair Cipher
4. Hill Cipher
5. Polyalphabetic Cipher
6. one-Time pad

Task → Playfair Cipher & Hill Cipher

Simple Block diagram of DES

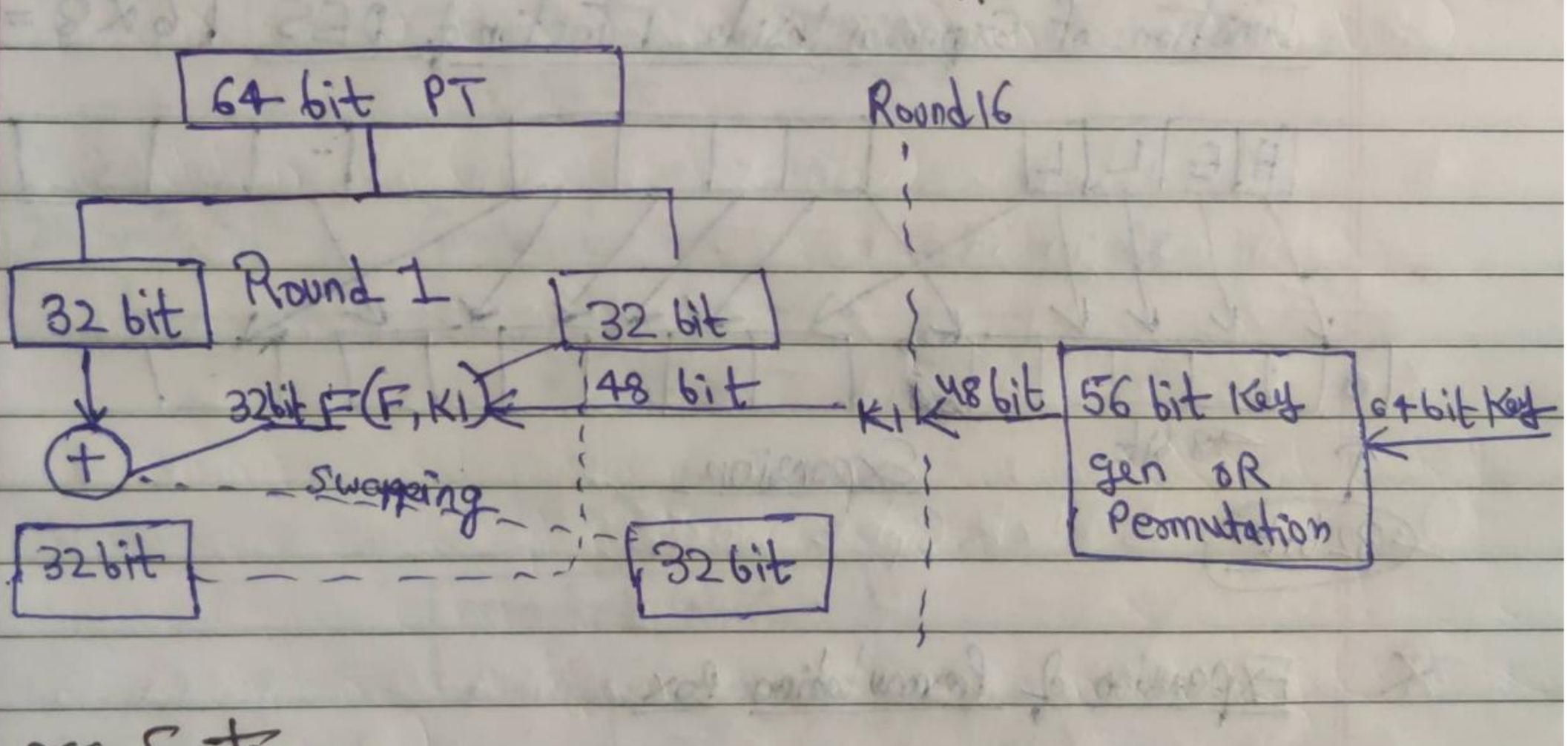


Date / /

1. DES i.e, Data EnCryption standard. It is a symmetric key Block Cipher.
2. published by (NIST) National Institude & Standard and Technology.
3. DES EnCrypt 64-bit plain Text to 64-bit Cipher Text.
4. 16 round in DES Provide Strengthness the algorithm.....?

5. DES is an implementation of a Fiestel Cipher. It use 16 round Fiestel structure.
6. Each round has the Same function which involve Key transformation expension, Permutation, S-box, P-box, X-OR function and Swapping.

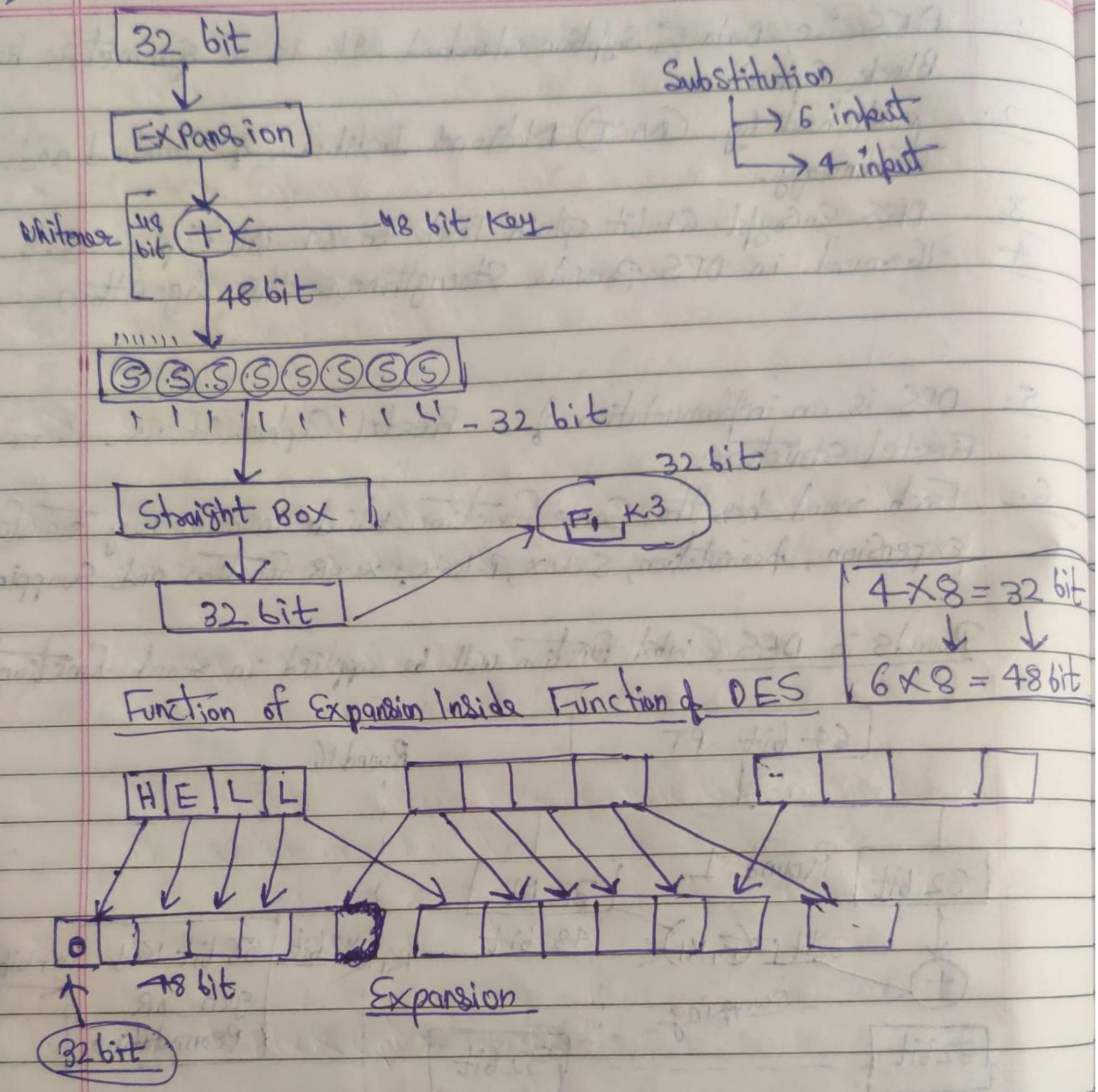
Rounds in DES (what function will be applied in round function)



DES function

1. The heart of the Cipher is the DES function 'F' (which is already defined in DES function).
2. It applies 48 bit Key to the right most 32-bit to produce 32-bit output.
3. Expansion P-box, whitener, Substitution (S-box) straight box
   (group of substitution box)

Date / /

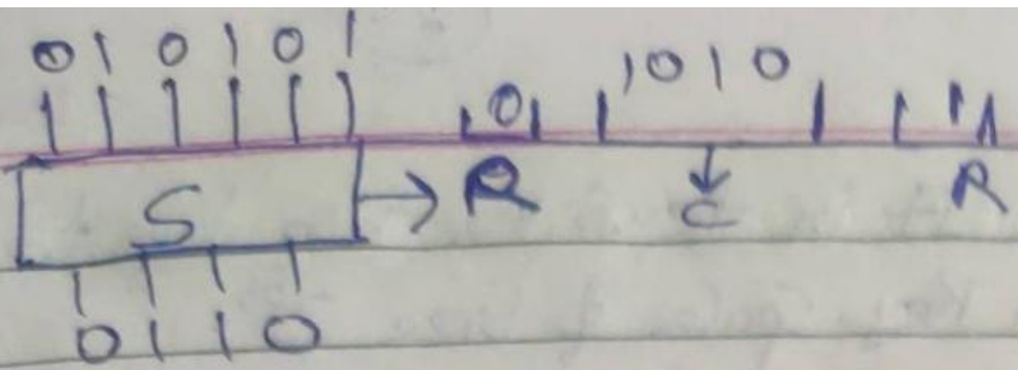


Function of Expansion Inside Function of DES

* Expansion of Permutation Box

Since, right input is 32-bit and round Key is a 48-bit. We must need to Expand right input to 48-bit.

Note- Whitener Key :
XOR operation b/w 48 bit Key and 48 bit output from Expansion Box.



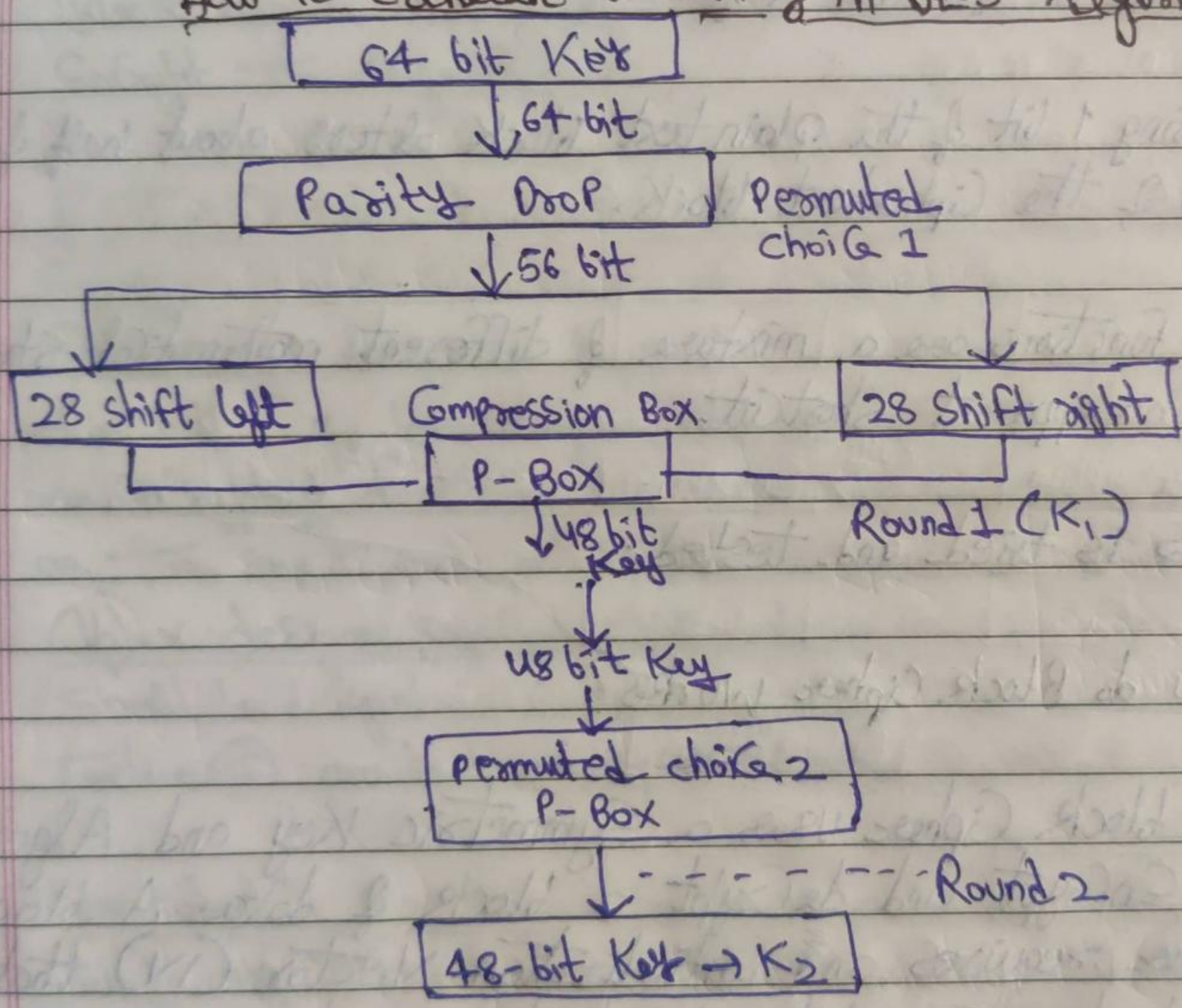
Date / /

Substitution Box

The S-boxes carry out the real mixing (Confusion). DES use 8 S-boxes Each with a 6-bit Input and a 4-bit Output.

	0	1	2	. . .	15
0	16	28	19	- - -	- - -
1	2	3	(45)	- - -	- - -
2	1	1	1	- - -	- - -
3	1	1	1	- - -	- - -

How to Generate 16 Sub Key in DES Algorithm



Q. Find out weakness and strength of DES Algorithm.

→ Weaknesses of DES

* Although Secure When it was designed in 1977, the Key Size of 56

Date / /

bits is now too small. It is feasible these days to exhaustively search a Key Space of Size 2^{56}.

* Linear and differential Cryptanalysis can be used to improve the search time.

* Nobody can prove that DES is secure.

→ Strengths of DES

* Even if you have the plaintext and Ciphertext, it seems difficult to get the Key.

* Altering 1 bit of the plaintext block alters about half of the bits of the Ciphertext block.

* The functions are a mixture of different mathematical structures with no apparent shortcut.

* DES is tried and tested.

Q. How do Block Cipher works?

→ A block Cipher uses a Symmetric Key and Algorithm to encrypt and decrypt a block of data. A block Cipher requires an initialisation Vector (IV) that is added to the input plaintext in order to increase the KeySpace of the Cipher and makes it more difficult to use brute force to break the Key.

Date / /

Principles of Block Cipher

Block Cipher is designed on the following 3 principles-

1. No. of Rounds
2. Function (F) design
3. Key schedule Algorithm

1. **No. of Rounds** ⟶ This Block Cipher principle indicates the overall strength of the Cipher algorithms. In short, the more the no. of rounds, the greater is the strength of the Block Cipher making it more difficult to break into or Encrypt the Algorithm.

2. **Function (F)** → Based on the Fiestel structure, the entire Encryption Process Consists of multiple rounds of plain text Processing where the Input Block of each round is denoted by two half i.e, left half and Right half. Function (F) is essentially an Encrypting function that take the Encrypting Key, 'K' and 'R' as the Input and reduce the Encrypted output. It is the Block Cipher designed principle that determines security. Function (F) should be designed in such a way that it Can not be Substituted. Function (F) provide the strength to the algorithms.

3. **Key schedule Algorithm** → The Key schedule algorithms Calculates the round Key. This Algorithm differ acco. to the Block scheme or Block Cipher or Block method. For example, the Key schedule algorithm in the DES Scheme divide the 56-bit Key into two half of 28 bit each.

Date / /

Examples → DES, 2DES, 3DES, AES, IDEA, etc.

Mode of Operation in Block Cipher

The Block Cipher Operation mode are divided into 5 parts and these modes of operation help in provide Security to the Algorithms.

These modes are:

1. Electronic Code Book mode
2. Cipher Block chaining mode
3. Cipher Feedback mode
4. output Feed back mode
5. Counter mode

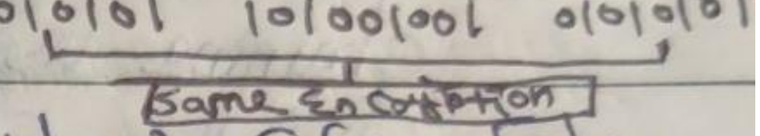
1. Electronic Code Book (ECB) Mode

Date / /

1. In ECB mode, the given plain text message is divided into blocks of 64 bit each and each 64 bit block get EnCrypted.

2. The plain text Box produce Cipher text of same size and EnCrypt and DeCrypt the message using same Key.

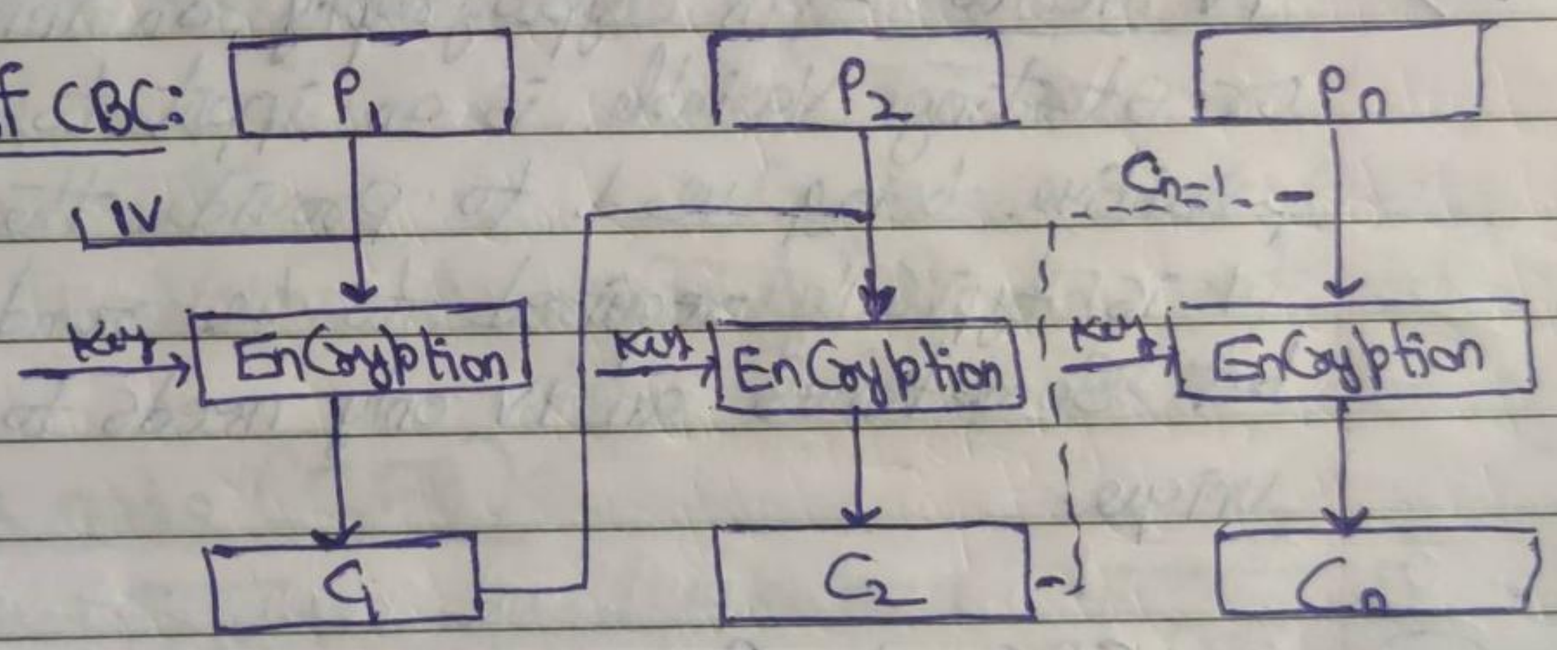
3. The Drawback of ECB mode is that occurance of more than one plain text Block in the Input generate the same Cipher text Block in the output which gives clue to the attacker.
For Example, Hellow everyone Hellow



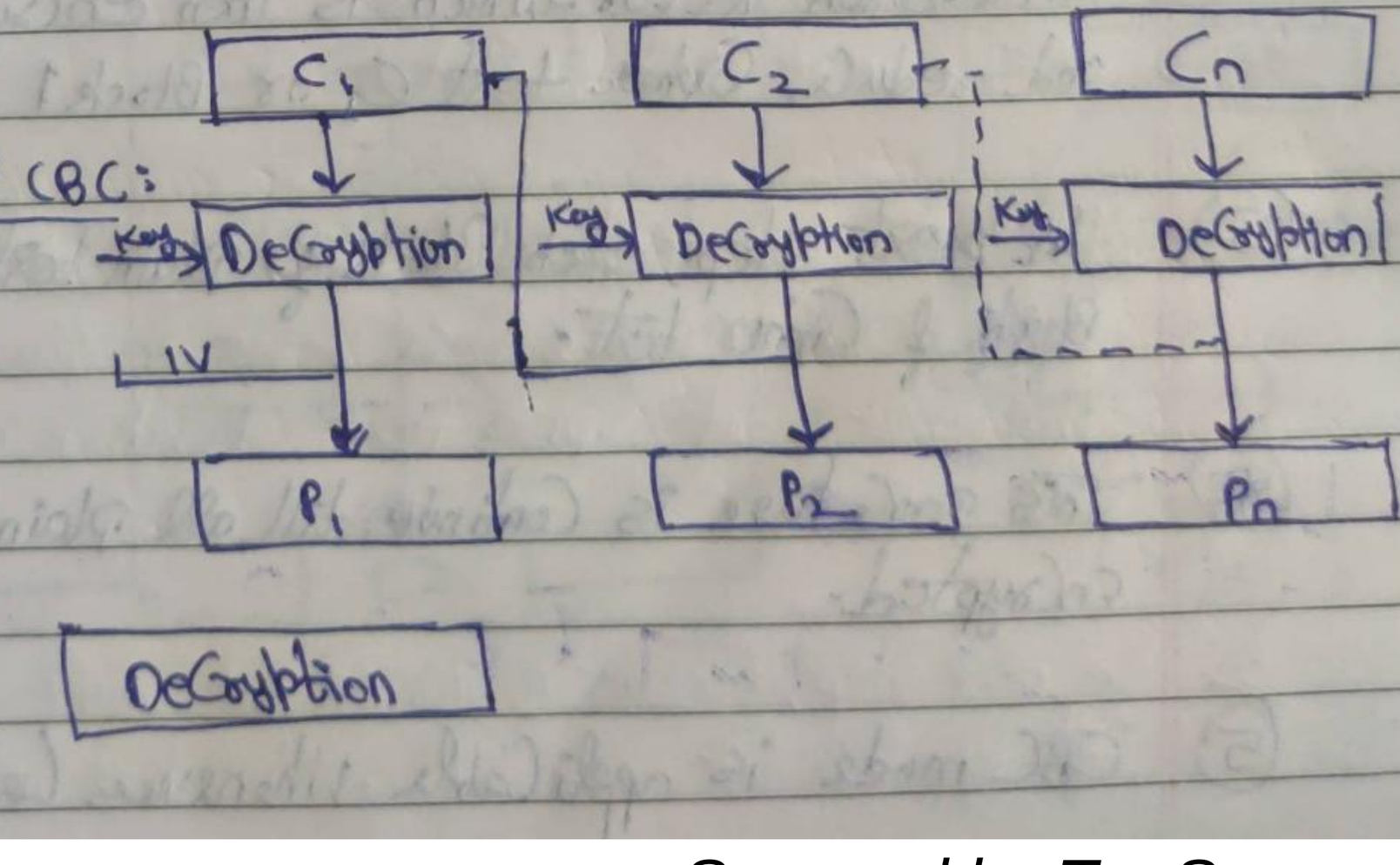
Mostly ECB mode used transmitting a single value in secure fashion.
Example - Password.

2. Cipher Block chaining (CBC) Mode

△ EnCryption Steps of CBC:



△ DeCryption Steps of CBC:



Date / /

Q- what is the role of IV vector in CBC mode?

Cipher Block Chaining mode

(1) To overcome the problem of ECB mode, the Cipher Block chaining mode is used.

Q. Define IV vector.

→ Role of IV vector in CBC mode - Cipher block chaining uses what is known as an initialization Vector (IV) of a certain length. By using this along with a single encryption key, organizations and individuals can safely encrypt and decrypt large amounts of plaintext.

→ IV vector - In Cryptography, an initialization vector (IV) or starting variable is an input to a cryptographic primitive being used to provide the initial state. The IV is typically required to be random or pseudorandom, but sometimes an IV only needs to be unpredictable or unique.

(2) In CBC mode, first Block of plain text is xor with an initialization vector which is then encrypted using Key (K) and reduce Cipher text C_1 or Block 1.

(3) In next step, each Block of plain text xored with previous Block of Cipher text.

(4) This procedure is continue till all plain text Block gets encrypted.

(5) CBC mode is applicable whenever large amount of data

Date / /

needs to be send Securely. Examples → E-mail, FTP, Web, etc.

Disadvantages of CBC mode

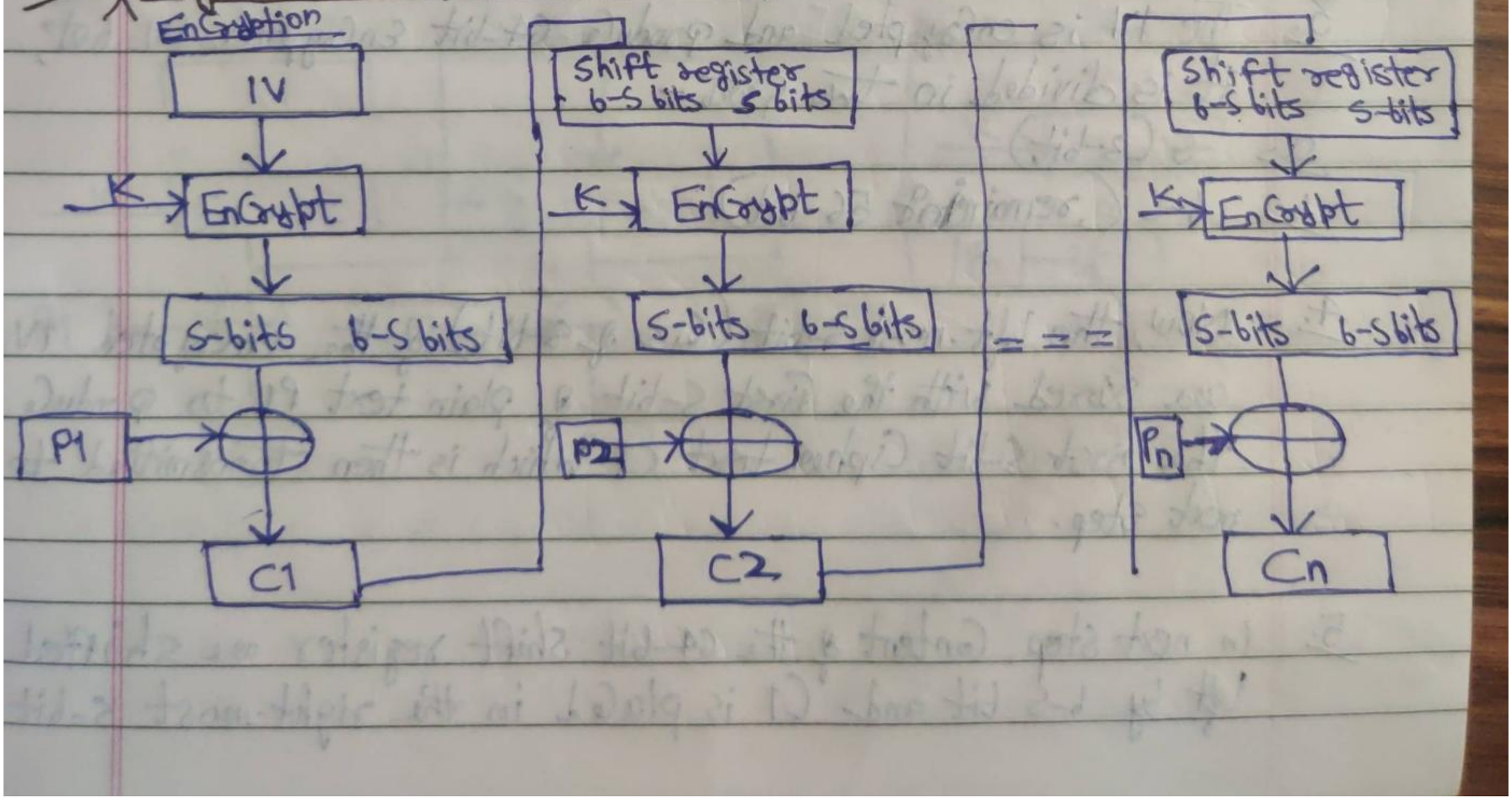
* Parallel encryption is not possible since every encryption requires a previous Cipher.

* While distinct Ciphertext blocks are extremely useful in terms of encryption strength, they can be a detriment in terms of decryption reliability. If one or more of the Ciphertext Blocks becomes lost, damaged or Corrupted, a user won't be able to perform a Complete decryption. While this can be a minimal inconvenience and rarely happens, it does force agencies to employ Secure Storage Systems to retain all Ciphertext data.

* Due to recursive nature of CBC's encryption process it is impossible to Simultaneously encrypt all plaintext inputs using Cipher Block chaining.

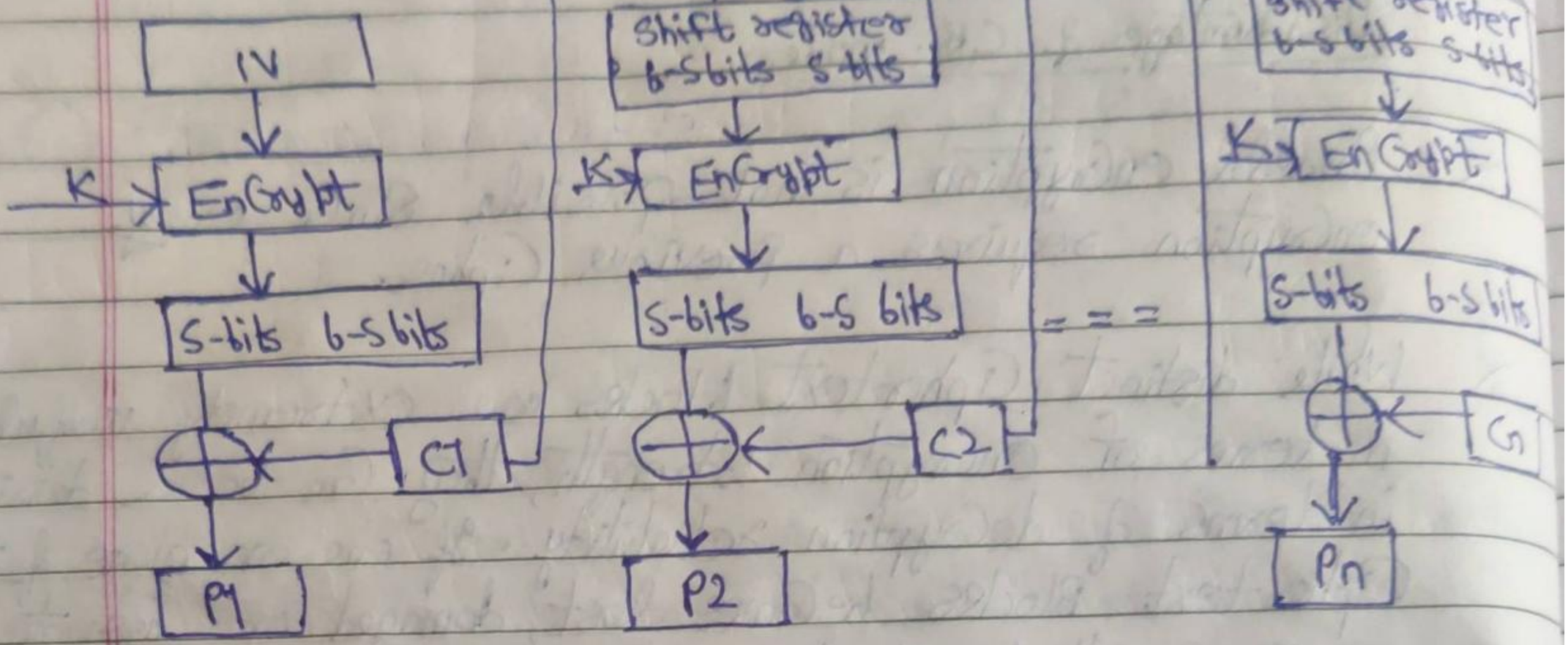
Cipher

3: Cyber Feedback mode (CFB)



Date / /

DeCryption



1. CFB mode use block Cipher but act as stream Cipher. It means that data is enCrypted in small unit of block 8-bits rather than predefined size of 64 bit.

2. In CFB EnCryption process, 64-bit IV is used which keep in 64 bit of shift register.

3. The IV is enCrypted and produce 64-bit EnCrypted IV but, it is divided in two part -
   a. S (8-bit)
   b. 6-S (remaining 56-bit)

4. Now, the left-most S-bit (size of 8-bit) of the EnCrypted IV are Xored with the first S-bit of plain text P1 to produce the first S-bit Cipher text C1. which is then transmitted to next step.

5. In next step, Content of the 64-bit shift register are shifted left by 6-S bit and C1 is placed in the right-most S-bit

Date / /

of the shift register and which again undergoes to Encryption process shown in figure.

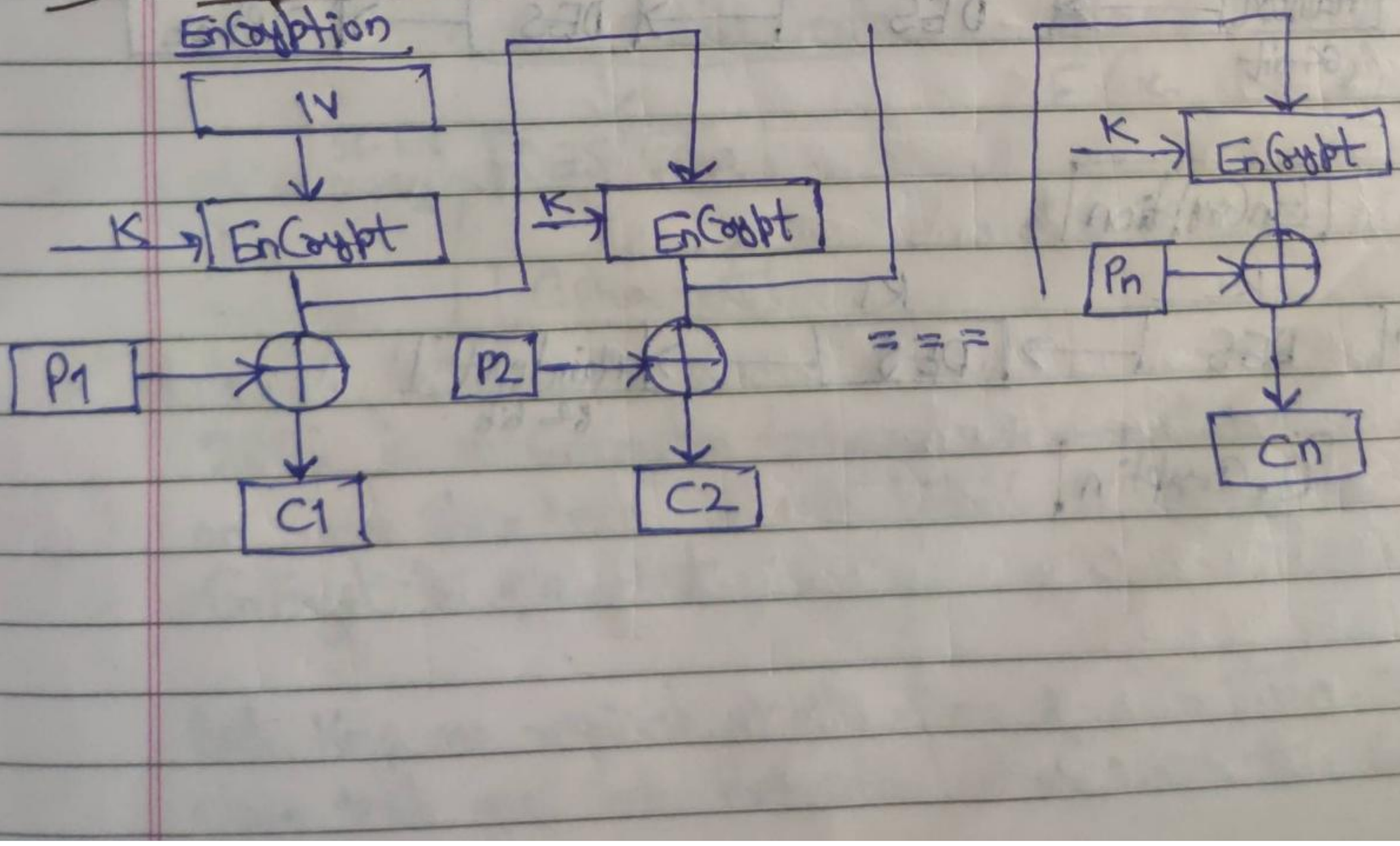
Note → CFB mode is Converting up Block Ciphes into a type of Stream Ciphes. This algorithm mostly use to key stream generator to produce Key stream.

Drawbacks of CFB mode

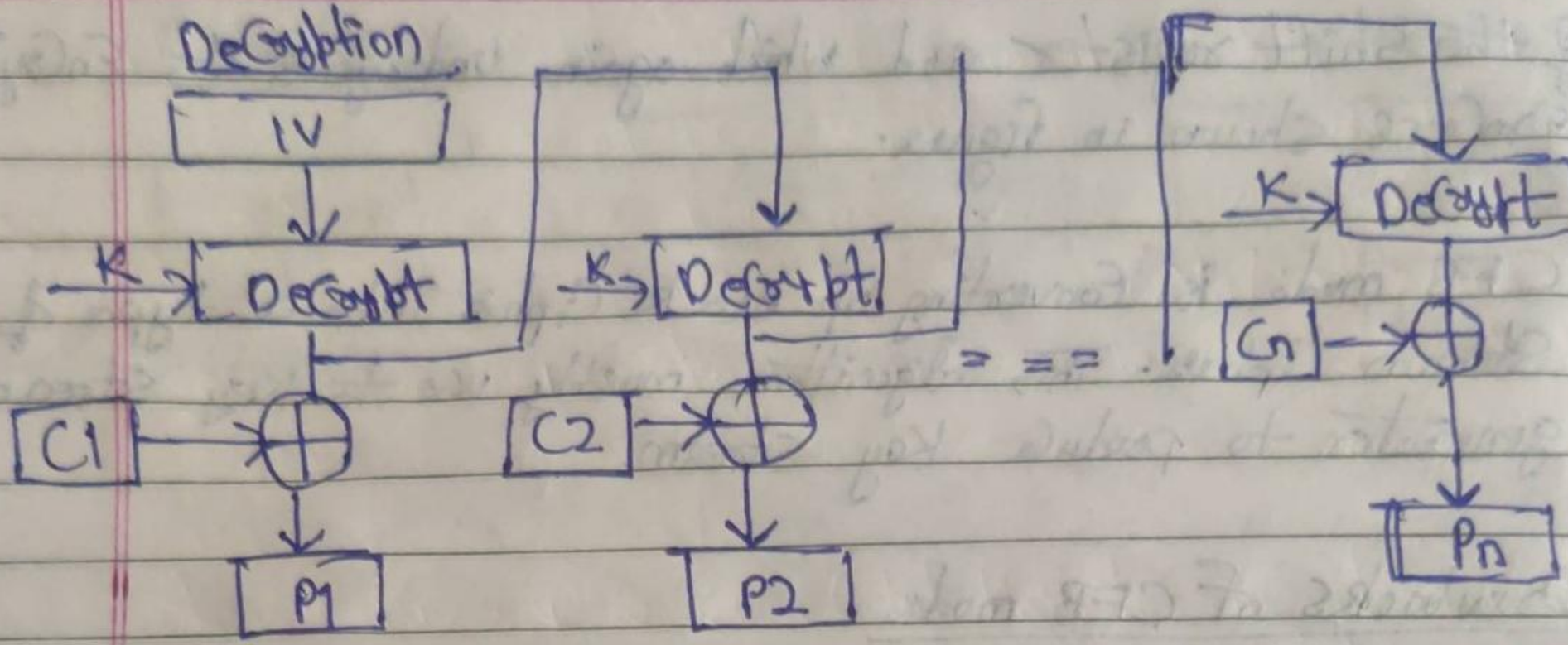
1. Message Blocks Cannot be decrypted from any part or re-encrypted after modification
2. Encryption Speed is Significantly slower.
3. CPU is not free during the whole process of the Ciphes text.
4. It is time Containing Process.

4. output Feedback (OFB) Mode

Encryption



Date / /

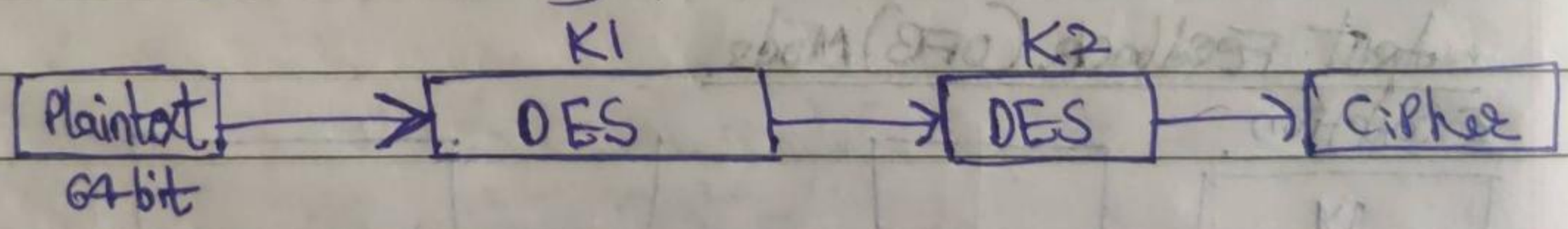


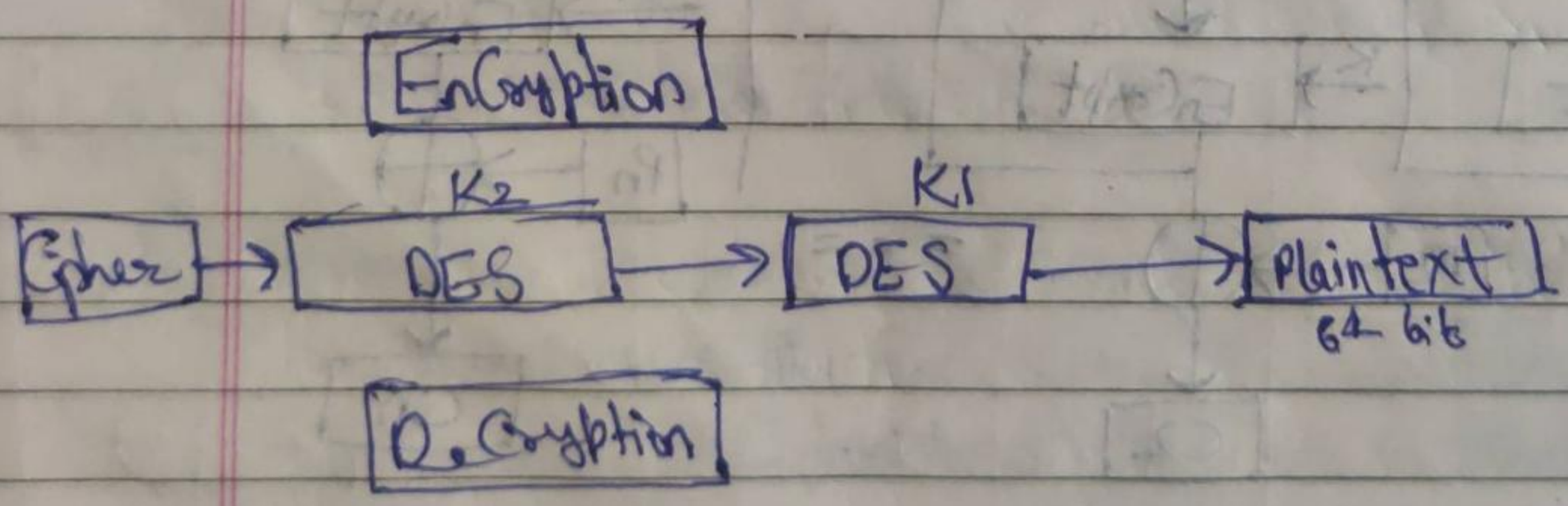
1. The output Feedback mode is similar as CFB mode - In CFB, the Cipher text unit is Feedback to the shift register.

2. In Case of OFB, difference is that output of Encryption process generating text C1 is directly placed in next stage of shift register which Perform XOR operation.

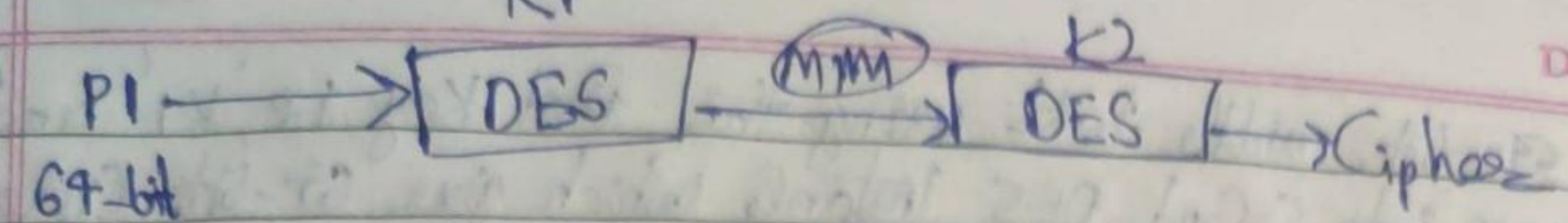
2 DES

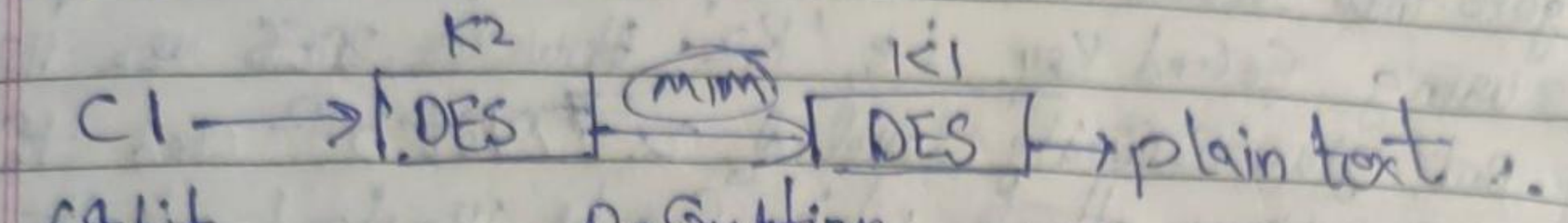
2 DES used to different Keys i.e 56+56 = 112 Key (both are use 56-bit Key).





EnCryption





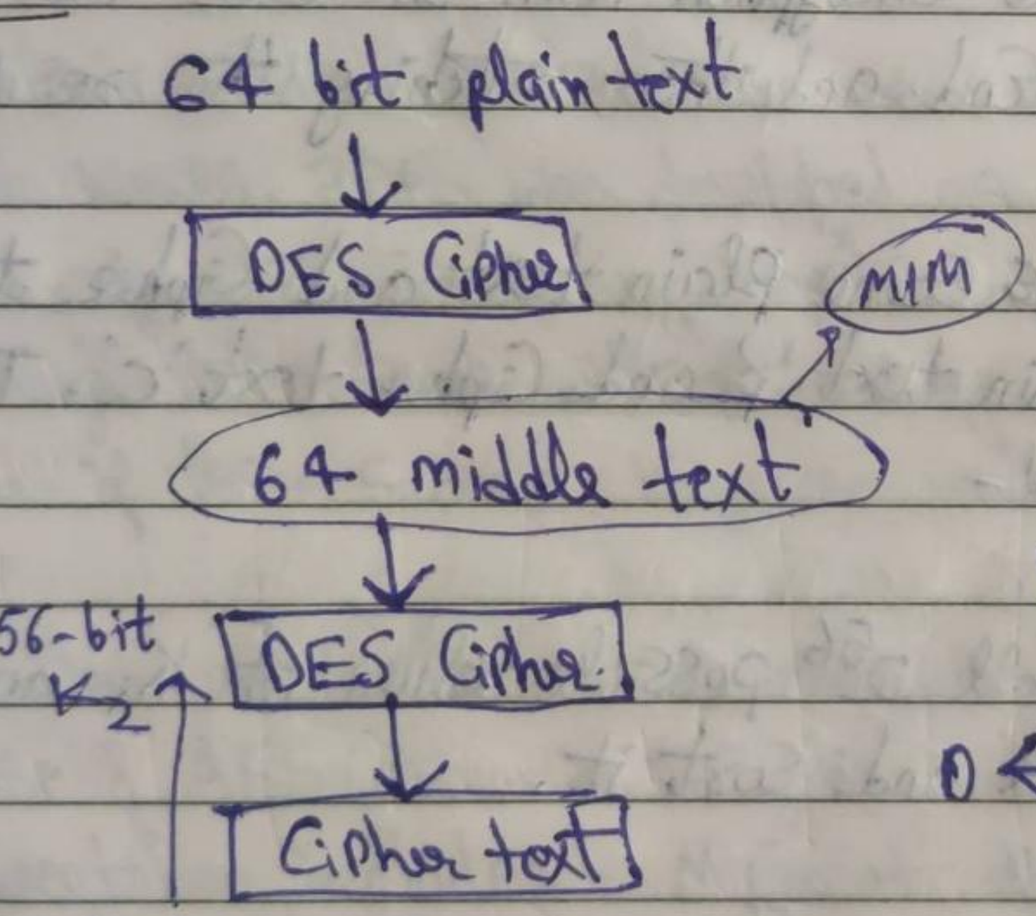
DeCryption

$P \rightarrow E(K_1, P)$
$E(K_2, (K_2, P))$

$P \leftarrow (K_1 (K_2, C_1))$

Note = First deCryption using Key K_2 which produces Single-EnCrypted Cipher text. This 64-bit middle text is then deCrypting using the Key K_1 to get plain text.

2DES



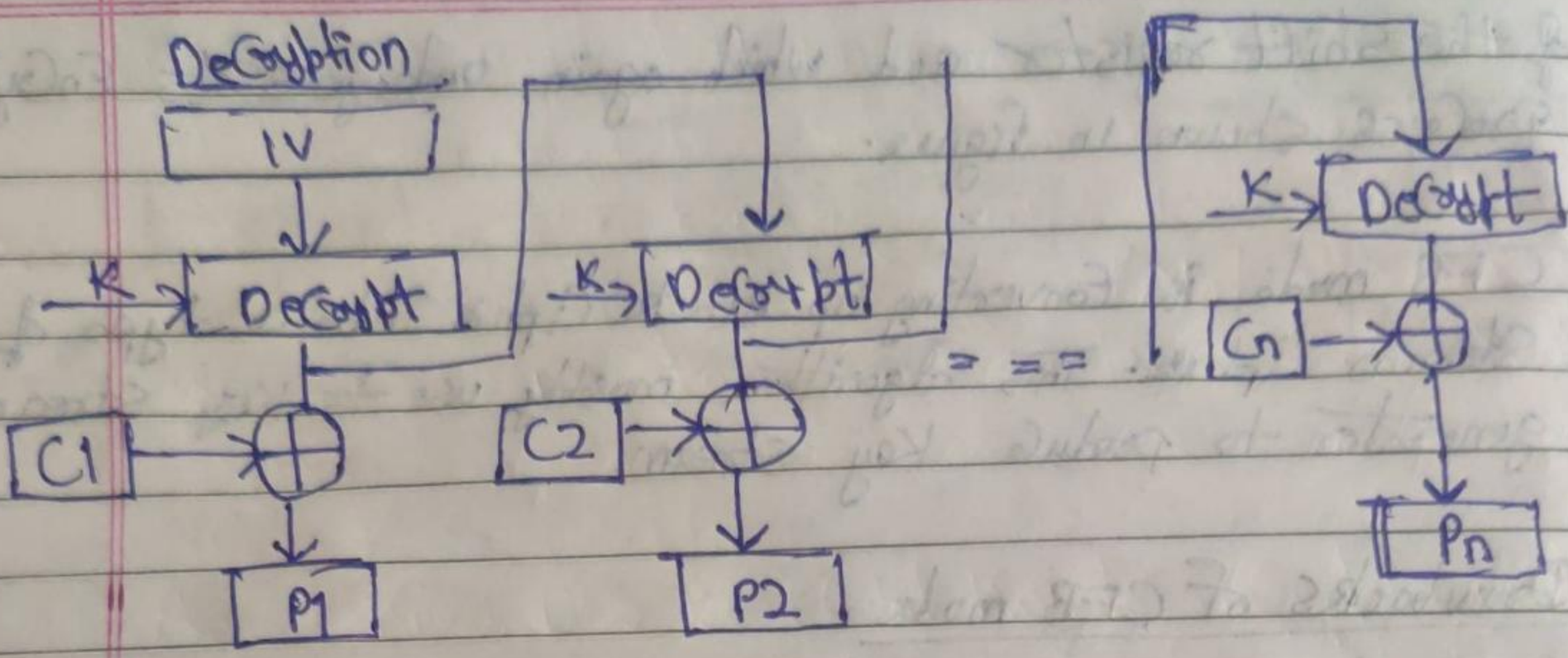
$P \rightarrow E(K_1, P)$
$E(K_2, (K_1, P))$

$P \leftarrow (K_1, D(K_2, C))$

2DES is an EnCryption technique which uses two Instance of DES on Same plain text. In both Instance, it use different Keys to EnCrypt the plain text.

Both Keys are required at the time of deCryption. The 64-bit plain text goes into first DES Instance which then Converted into

Date / /

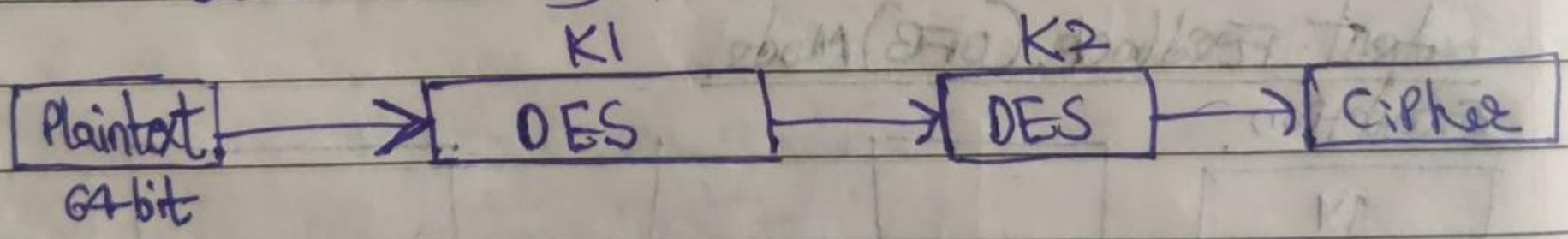


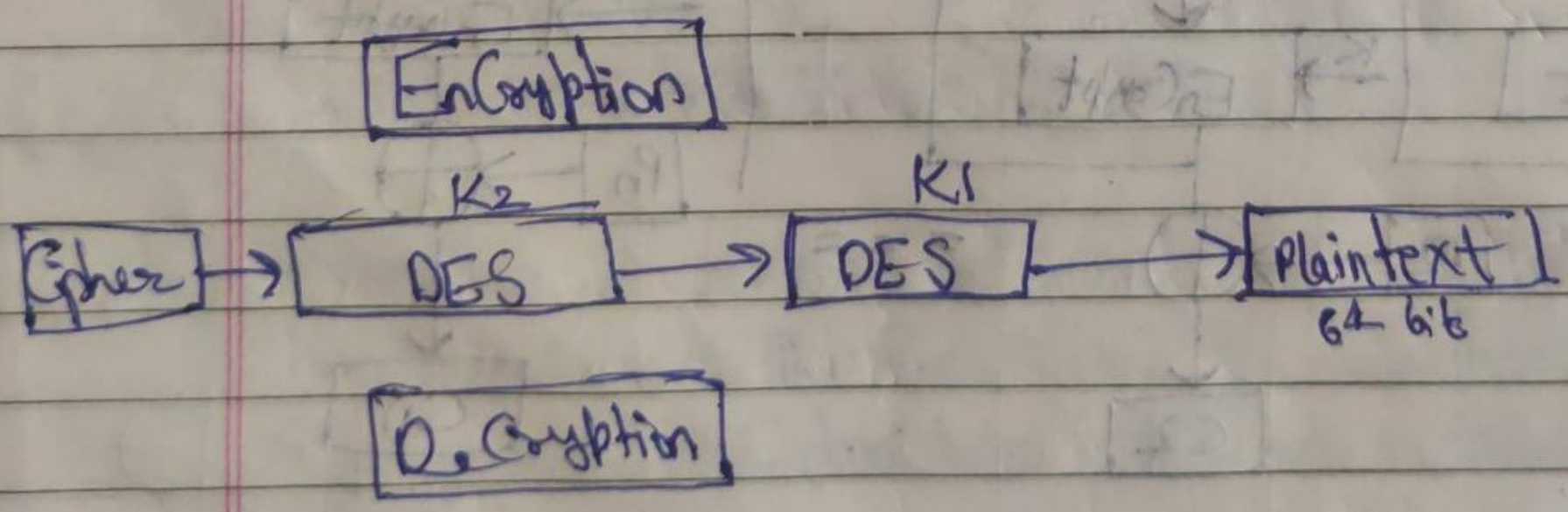
1. The output Feedback mode is similar as CFB mode - In CFB, the Cipher text unit is Feedback to the shift register.

2. In Case of OFB, difference is that output of Encryption process generating text C1 is directly placed in next stage of shift register which Perform XOR operation.

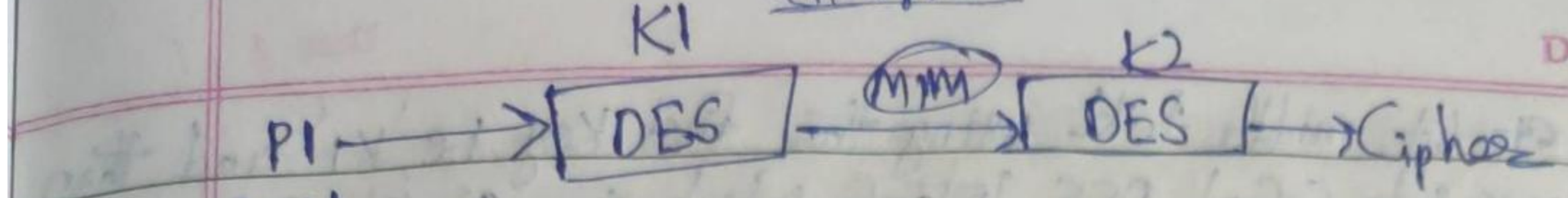
2 DES

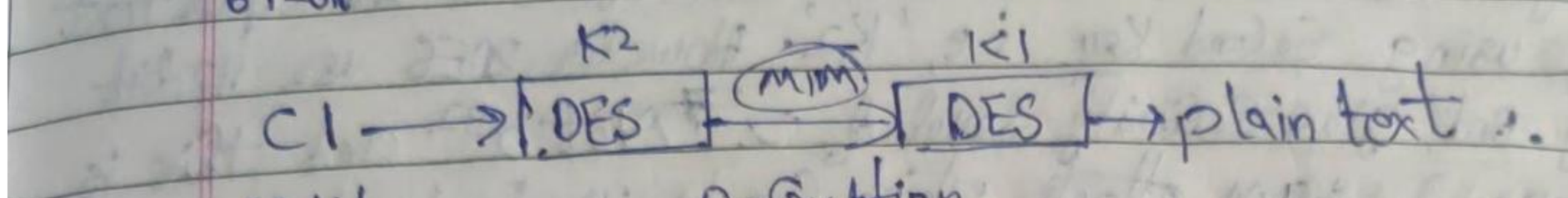
2 DES used to different Keys i.e 56+56 = 112 Key (both one use 56-bit Key).





EnCryption





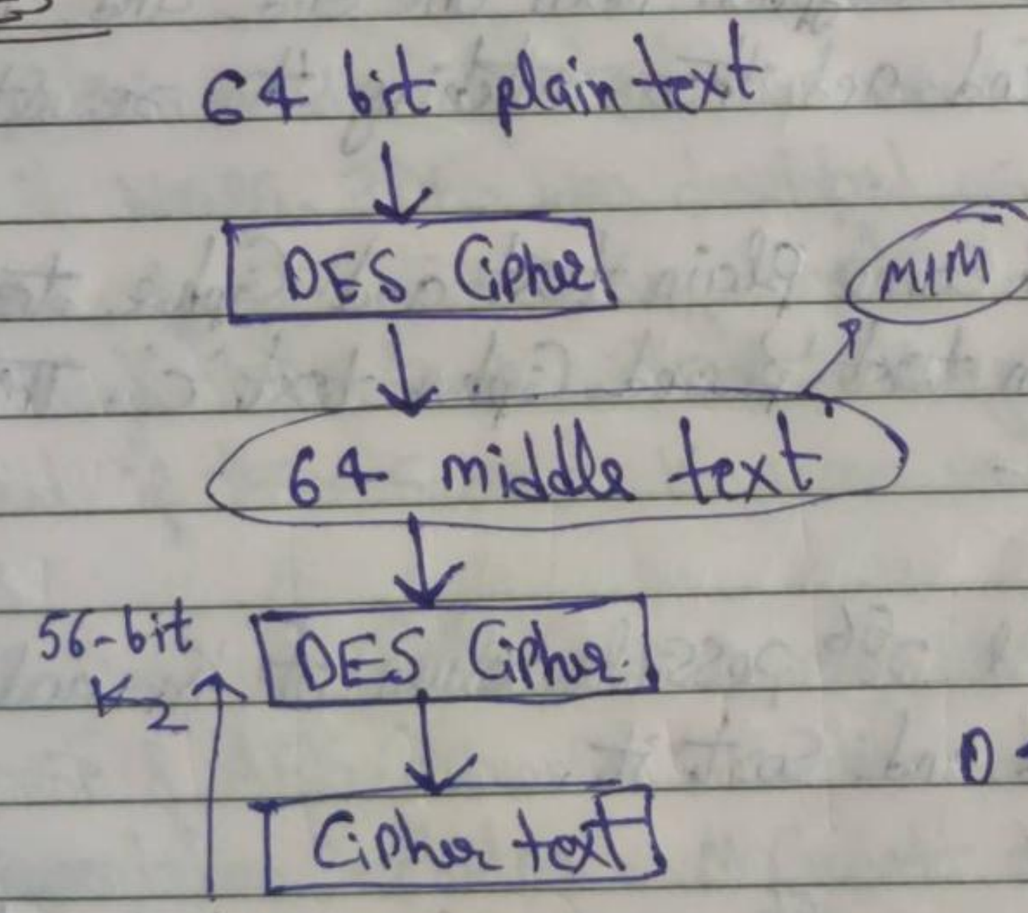
DeCryption

$P \rightarrow E(K_1, P)$
$E(K_2, (K_2, P))$

$P \leftarrow (K_1 (K_2, C_1))$

Note - First deCryption using Key K_2 which Produces Single-EnCrypted Cipher text. This 64-bit middle text is then deCrypting using the Key K_1 to get plain text.

2DES



$P \rightarrow E(K_1, P)$
$E(K_2, (K_1, P))$

$D \leftarrow (K_1, D(K_2, C))$

2DES is an EnCryption technique which uses two Instance of DES on Same plain text. In both Instance, it use different Keys to EnCrypt the plain text.

Both Keys are required at the time of deCryption. The 64-bit plain text goes into first DES Instance which then Converted into

Date / /

a 64-bit middle text using the first key i.e, 'K1' and then it goes into Second DES Instance which give 64-bit Ciphertext by using Second Key i.e, 'K2'. However, 2DES use 112-bit Key. But, give Security level of 2^{57} Not 2^{112} and this is because of MIM attack which can be use to break through 2DES.

As we Know, DES use 56-bit Key to Encrypt any plain text which can be easily Crack by using modern Technology. To prevent this from happening, 2DES and 3DES were introduced which are much more Secured than the original DES Because, it uses 112 and 168-bit Key. 2DES and 3DES offer much Security than DES.

Meet In the Middle attack (MIM)

① This attack Involves Encryption from one end and Decryption from the other End. and then, matching the result in the middle.

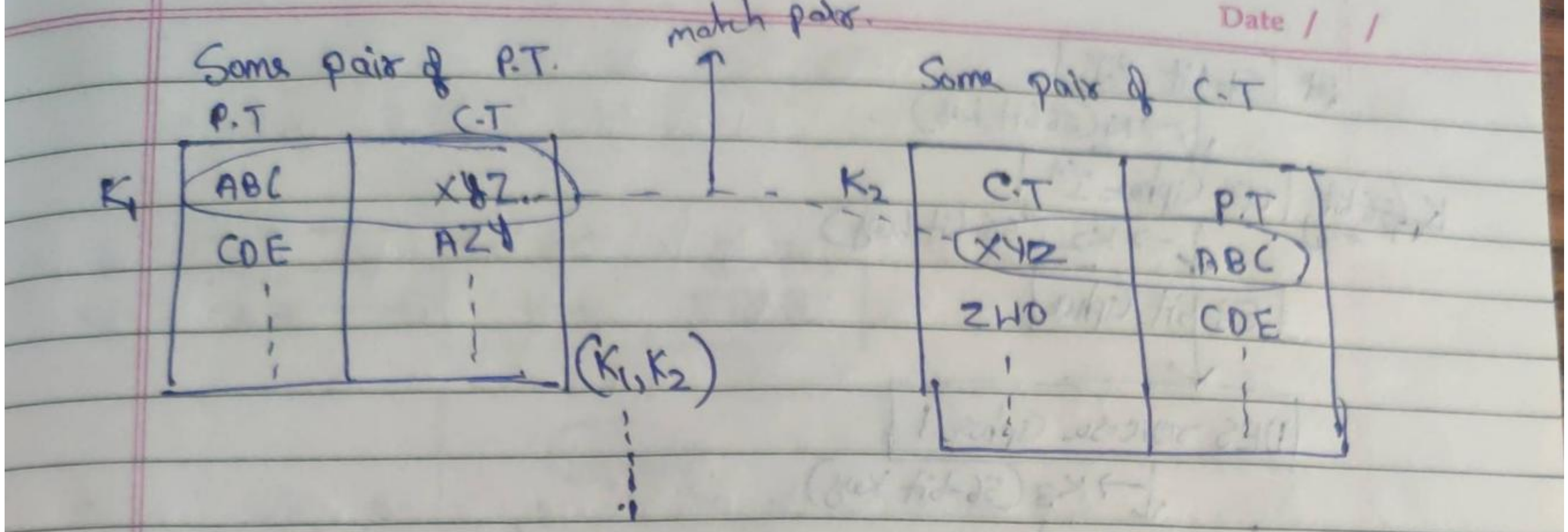
② This attack requires Some plain text and Ciphere text pair. Let us assume, plain text 'p' and Ciphere text 'c'. This attack Proceed as follow -

a. Encrypt 'p' for all 2^{56} possible values of 'K_1' and store the result in a table and Sort it.

b. Now, Decrypt 'c' using 2^{56} possible values of 'K_2'. After check the table for a match.

③ When there is a match, we have located a possible correct pair of Keys.

Date / /



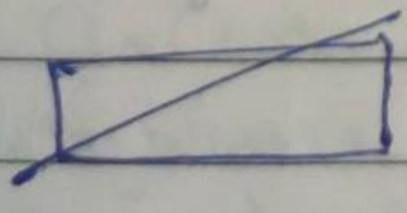
3DES

3DES is a type of Computerized Cryptography where Block Cipher algorithm are applied three time to Each data Block. The Key Size is inCreased in 3DES to EnSure additional SeCurity through EnCryption Capabilities. Each Block Contain 64-bit of data. Three Keys are collected to as Bundle Key with 56-bit/Key. (i.e, 'K1', K2', 'K3').

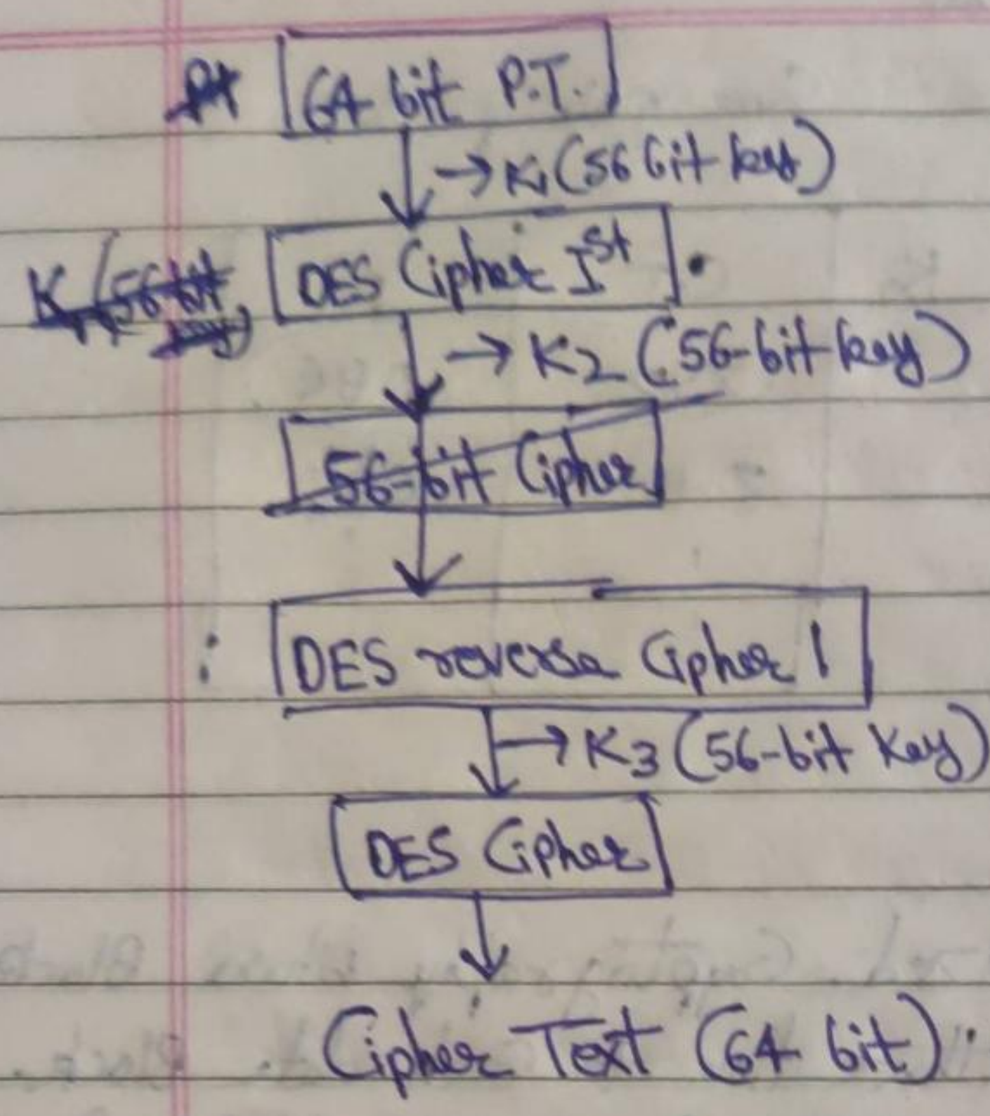
Note- DES, it is Still important to learn about what 3DES is and how it WorkS. 3DES Was developed as a more SeCure Alternative beCause of DES Small Key Length. In 3DES, the DES algorithm is run through three times with three Keys. However, it is only ConSidered SeCured if three Seperate Keys are used.

Note- 3DES Was one of the more Commonly used EnCryption Scheme before the rise of AES (Advanced EnCryption Scheme). Some Example of its Implementation includes - MiCroSoft offiCe, FireFox, etc. But, Now many of these platform no longer use 3DES BeCauSe, there are better alternatives.

Block diagram of AES using 3DES



Date / /



* AES (AdvanCed EnCryption Standard)

1. AdvanCed EnCryption Standard is a Symmetric Key Cryptography algorithm published by NIST.

2. This Algorithm is the replaCement of DES.

3. AES Work on Block Cipher Technique. Size of plaintext and Ciphertext must be Same.

4. In AES, the data length (plaintext length) of 128, 192, 256 bit. And Supporting 3 different Key length.

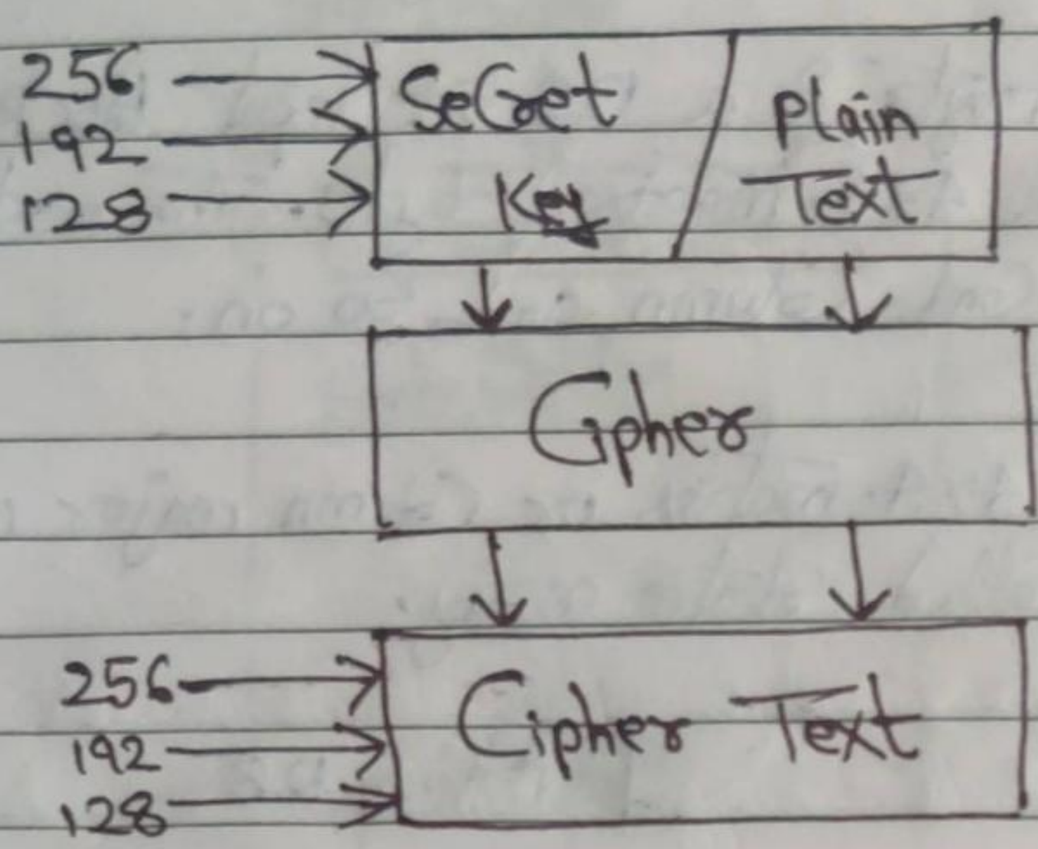
P.T	Key length
128	128
192	192
256	256

5. AES Consist of multiple Rounds of processing different Keys pick like -

P.T	K.L	Round
128	128	10

Date / /

192 192 12
256 256 14



Characteristics

1. AES has Key of three length – 128, 192, 256.
2. It is flexible and has implementation for Software and hardware.
3. It Provide high Security and Can prevent from many attack.
4. It doesn't have any Copyright. So, it Can be easily used globally. (Tool – "Devglan").
5. It Consist of 10 rounds of Processing for 128 bit Key, 12 rounds for 192 bit Key and 14 rounds for 256 bit Key.

Examples-

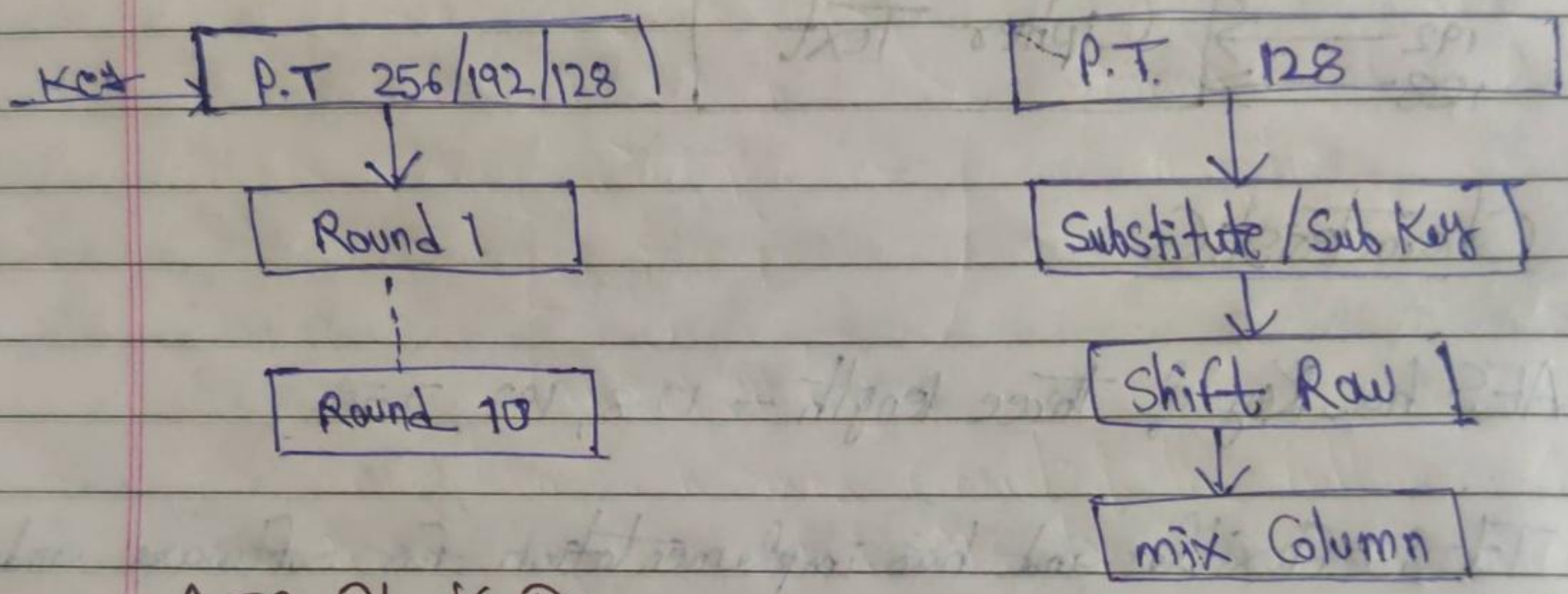
1. when you store personal Information on a website – facebook, twitter, etc or even when you use your VISA or Pan Card to make a Purchase AES algorithm. AES algorithm Provide Security Everywhere.
online govt. site, Passport application, driving license, etc.

Date / /

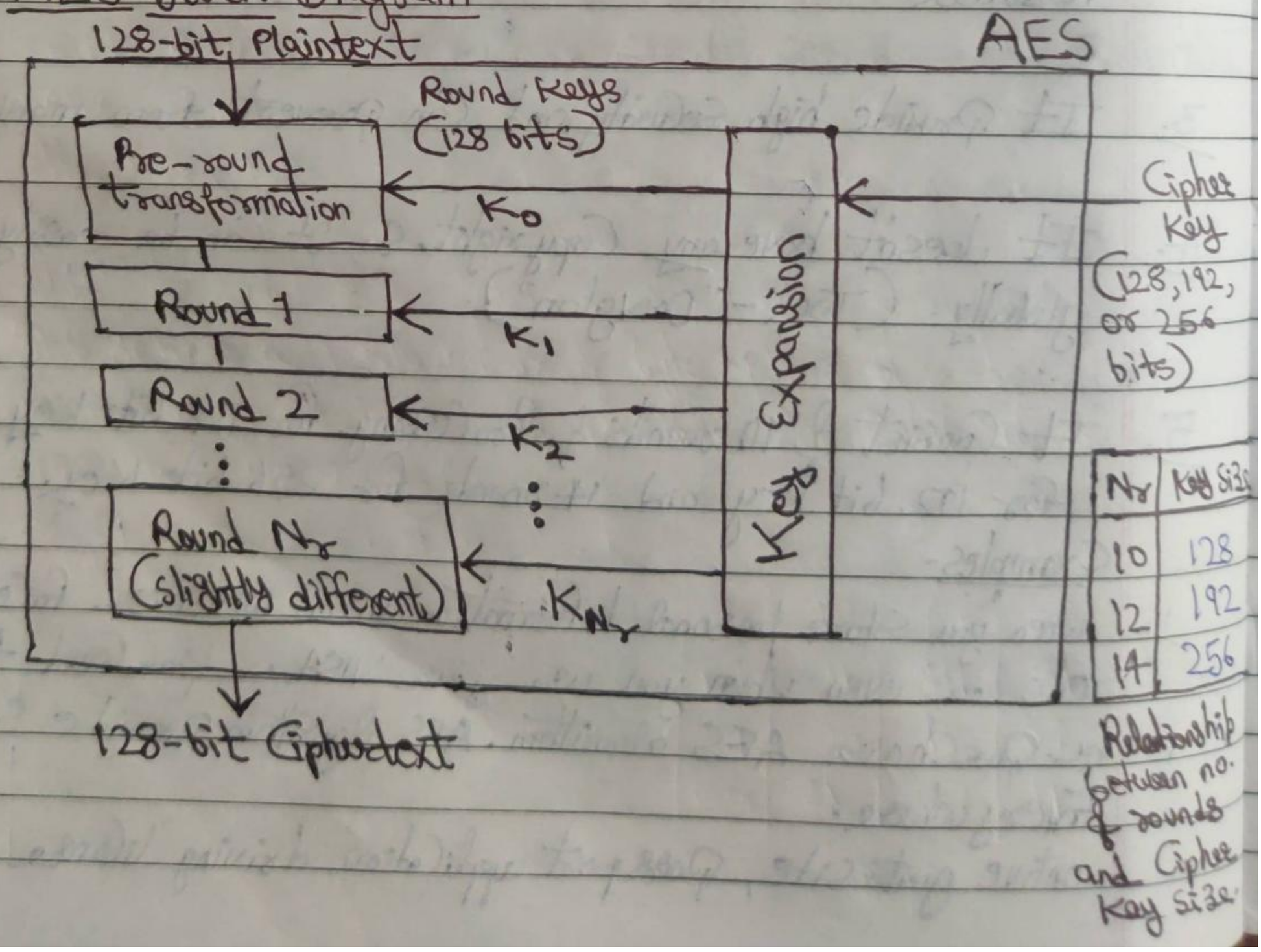
6. plaintext for e.g "AES is used"
plaintext (128 bit) Convert into 4×4 matrix byte.

7. Therefore, the first 4 byte of a 128 bit Input block occupy First Column In the 4×4 matrix of byte. The next 4 byte occupy the Second Column and so on.

8. AES operate on a 4×4 matrix or Column major order matrix of byte is called state array.



AES Block Diagram



Date / /

AES Function Block Diagram

Fig (B)

Plain Text :-

"AES is a Symmetric algo"

↳ Hex

Hexa:- 01 01 02 03 01 A0 C0 20 ----

01	01	03	11
01	A0	EF	21
02	C0	S0	23
03	20	16	24

Initial state array

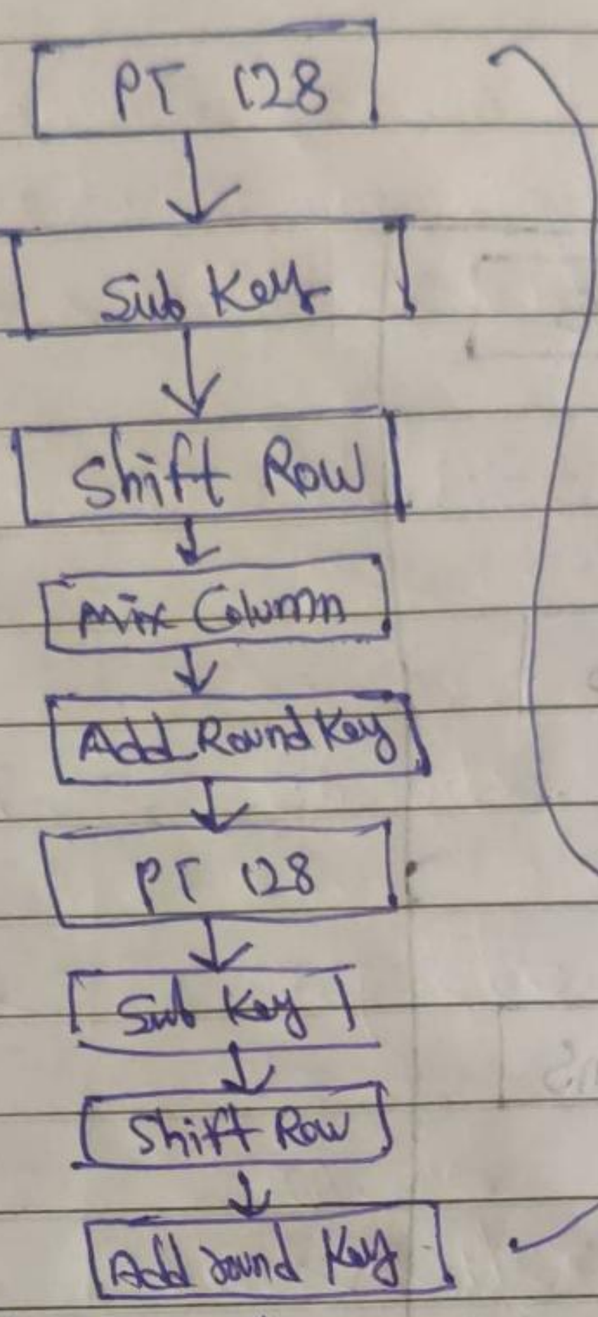
S-Box 16X16

4X4

Final state array

Date / /

1. Overall structure of AES Encryption process show in Fig(B).



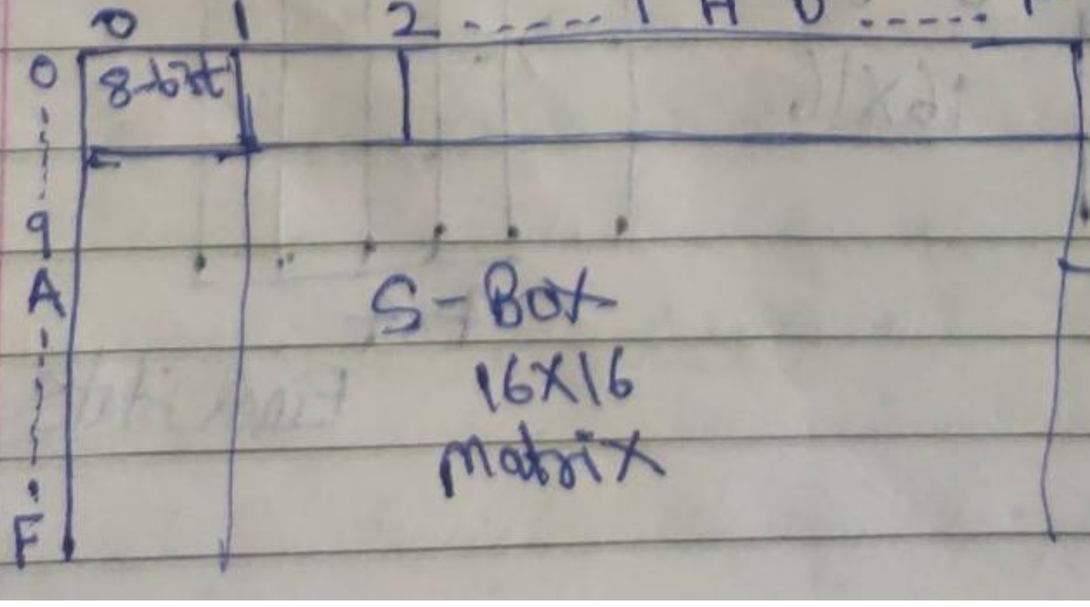
Final round of AES Encryption

2. For Encryption, Each round Consist of the following 4 step and these step also called AES transformation function

a. Substitute/Sub byte
b. Shift Row
c. Mix Column
d. Add Round Key

a. Substitute/Sub byte:

1. AES defines a 16X16 matrix of byte values at S-box that Contains a Permutation of all possible 256 8-bit values. (Similarly for 192 & 128 values)



1A	12	AF	23
GF	11	H1	81
01	05	12	07
FG	21	22	11

4X4

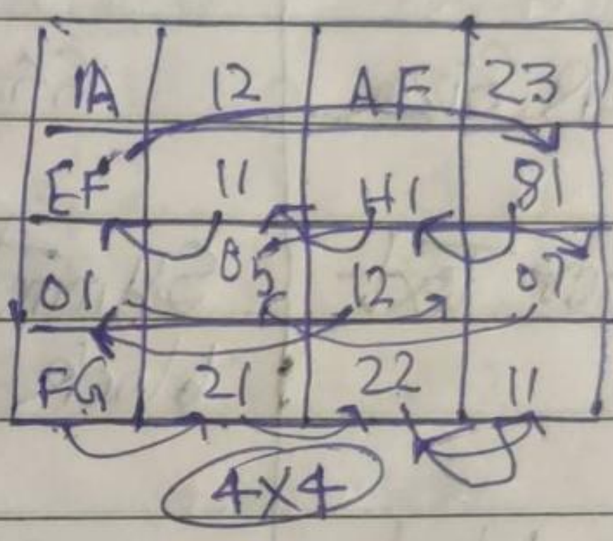
Date / /

2. Each individual byte of State is map into a new byte in the following way -
The left most 4 bit of the byte are used as a row value and the right most 4 bit are used as a Column Value.

3. The row and Column Values serve as index into the S-Box to Select a unique 8-bit output Value

b. Shift row transformation :

1. The shift row transformation is called shift row.
2. rules of shifting rows:
   a. Row 1 → No shifting
   Row 2 → 1 byte left shift
   Row 3 → 2 byte left shift
   Row 4 → 3 byte left shift



c. Mix Column transformation :

1. The mix Column Transformation ~~Colum~~ Called mixed Columns, operates on Each Column Individually.

2. Each byte of a Column is map into a new value that is a function of all 4 bytes in that Column.

01	01	03	11
A1	A0	EF	21
02	C0	50	23
03	20	1d	24

initial State array

×

1A	12	AF	23
EF	11	H1	81
01	05	12	07
FG	21	22	11

Pre-defined array

=

Mixed Column

F1			

01 × A1 + 01 × EF + 03 × 01 + 11 × FG = F1

d. Add round Key :

1. In the ~~first~~ forward and round Key transformation called Add round Key, the 128 bit ~~key~~ of State array with bitwise XOR

Date / /

with 128 bit round Key.

2. In this Columnwise operation blw the 4 byte of a State Column and ~~In this~~ Column~~wit~~ one word/bit of the round Key, It Can also be ~~four~~ viewed as a ~~bihite~~ byte level operations.

Q. Comparison blw DES Vs AES.

→

Factors	DES	AES
Key length	56 bits	128, 192, 256 bits
Block Size	64 bits	128, 192, 256 bits
Cipher Text	Symmetric block Cipher	Symmetric block Cipher
Developed	1977	2000
Security	Proven inadequate	Considered Secure
Cryptanalysis resistance	Vulnerable to differential and linear Cryptanalysis.	Strong against differential and linear Cryptanalysis.
Possible Keys	2^{56}	2^{128}, 2^{192}, 2^{256}

Date / /

Questions

Q.1 $(17+20) \bmod 7$

Q.2. $-15 \bmod 7$

Q.3. $-37 \bmod 5$

Q.4. $2 \equiv -3 \pmod 5$, check it is valid or not.

Q.5. $123 \times 62 \bmod 12$

Q.6. $3 \equiv -3 \bmod 17$, check whether it is valid or not.

Q.7. $7 \bmod 4 \equiv 3$

Q.8 $-51 \equiv 9 \bmod 10$

Q.9. SeCrets → message
10|2|13|20 → Key

SECRETS — message

Key- $\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 0 \end{bmatrix}$

A.1. $37 \bmod 7 \Rightarrow 2$

A.2. $-15 \bmod 7 \Rightarrow 6$

$n = -15$

$m = 7$

$a = q \times m + r$

$-15 = q \times 7 + r$

$-15 = -1 \times 7 + r$

$-15 + 7 = r \Rightarrow r = -8$

$-15 = -3 \times 7 + R$

$-15 = -21 + R$

$-15 + 21 = R$

$R = 6$

A.3 - $-37 \bmod 5$

$-37 = q \times 5 + r$

$-37 = -8 \times 5 + r$

$-37 + 40 = r$

$r = 3$

A.4. $2 \equiv (-3 \bmod 5)$

$2 \bmod 5 = -3 \bmod 5$

$N = q(m) + R$

$-3 = -1 \times 5 + R$

$-3 + 5 = +R$ Yes, it is valid

Date / /

A.5. $123 \times 62 \bmod 12$

$= 7626 \bmod 12$

$= 635.50 - 635$

$= 0.50 \times 12$

$= 6$

Q.10. $73 \cong 4 \bmod 23$, check whether it is valid or not.

→ $73 \bmod 23 = 4 \bmod 23$

$73 \div 23$ $\quad$ $4 \div 23$

$= 3.17 - 3$ $\quad$ $= 0.17 - 0$

$= 0.17 \times 23$ $\quad$ $= 0.17 \times 23$

$= 3.91$ $\quad$ $= 4$

$= 4$ $\quad$ $\therefore$ It is valid

A.6. $3 \cong -3 \bmod 17$

$3 \bmod 17 = -3 \bmod 17$

$3 \div 17$ $\quad$ ~~$3 = \cdot \times 17 + r$~~ $\quad$ $-3 \div 17$

$= 0.18 - 0$ $\quad$ ~~$3 = -17 + r$~~ $\quad$ $= -0.18 + 0$

$= 0.18 \times 17$ $\quad$ $= -0.18 \times 17$

$= 3.06$ $\quad$ $= -3$

$= 3$ $\quad$ $\therefore$ not valid.

A.7. $7 \bmod 4 \cong 3$

$7 \div 4$

$= 1.75 - 1$

$= 0.75 \times 4$

$= 3 \cong 3$

$\therefore$ It is valid.

A-8. $-51 \equiv 9 \bmod 10$

Date / /

$9 \div 10$ $\quad -51 \bmod 10 = 9 \bmod 10$

$= 0.9 - 0$ $\quad -51 \div 10 \quad = 0.9 \times 10$

$= 0.9 \times 10$ $\quad 9 \quad = 9$

$= 9$ $\quad \therefore$ It is valid

A-9. message — SECRETS

Key- $\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 0 \end{bmatrix}$

Step 1- Let the encoding matrix be

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 0 \end{bmatrix}$$

Let the message to be sent by the Sender be "SECRETS".

S E C R E T S

19 5 3 18 5 20 19

[19 5 3], [18 5 20], [19 0 0]

Step 2-

UnCoded row matrix		Encoding Matrix		Coded row Matrix
[19 5 3]		$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 0 \end{bmatrix}$	=	[32 11 34]
[18 5 20]		$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 0 \end{bmatrix}$	=	[48 45 33]

$$\begin{bmatrix}19 & 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 1\\ 2 & 1 & 3\\ 1 & 2 & 0\end{bmatrix} = \begin{bmatrix}19 & 0 & 19\end{bmatrix}$$

So, the encoded message is $[32\ 11\ 34]\ [48\ 45\ 33]\ [19\ 0\ 19]$

Step 3- The receiver will decode the message by the reverse Key, post-multiplying by the inverse of A.
So, the decoding matrix is

$$A^{-1} = \frac{1}{|A|}\,adj.A = \begin{bmatrix}0 & 2 & 1\\ 3 & 1 & 2\\ 1 & 0 & 1\end{bmatrix}$$

Step 4- The receiver decodes the coded message as follows:

Coded row matrix	Decoding matrix	Decoded row Matrix

$$\begin{bmatrix}32 & 11 & 34\end{bmatrix}\begin{bmatrix}0 & 2 & 1\\ 3 & 1 & 2\\ 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}67 & 75 & 88\end{bmatrix}$$

$$\begin{bmatrix}48 & 45 & 33\end{bmatrix}\begin{bmatrix}0 & 2 & 1\\ 3 & 1 & 2\\ 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}168 & 141 & 171\end{bmatrix}$$

$$\begin{bmatrix}19 & 0 & 19\end{bmatrix}\begin{bmatrix}0 & 2 & 1\\ 3 & 1 & 2\\ 1 & 0 & 1\end{bmatrix} = \begin{bmatrix}19 & 38 & 38\end{bmatrix}$$

So, the Sequence of decoded row matrices is $[67\ 75\ 88]$, $[168\ 141\ 171]$, $[19\ 38\ 38]$
Thus, the receiver reads the message as "SECRETS".

UNIT-3

Date / /

Random Number

* Random Numbers play an Important role in the use of EnCryption for various Network SeCurity Application

* In Cryptography, the randomness (entrophy) play a very Important role. In many Algorithms, we need random numbers. i.e, unpredictable numbers. If these numbers are not unpredictable, the algorithms will be Compromised. for.e.g- assume we need a SeCret Key that will protect our financial asset. This SeCret Key should be randomly generated in a way that nobody else should be able to generate or have the Same Key. If we generate the Key From a SeCure random generator then it will be unpredictable. and the System will be SeCure. Therefore, SeCure random means unpredictable random number.

* Random numbers are Important in TCP/IP SequenCe number, password, In domain name System, SourCe Code number or are depend on random numbers. In Cryptography, randomness is found everywhere from the generation of Key to enCryption System, Even the way in which CryptoSystem are attached. without randomness, all Crypto operation would be predictable and henCe inSeCure.

* When Computer algorithms are feed with the Same Input, they Should always give Same output. So, they are easily predictable and therefore it is not a good SourCe of random numbers. A good random numbers generator Consists of two part. A SourCe of

1. Entrophy
2. Cryptographic algorithms

Date / /

Types of Random Number Generators

1. **PRNG (PSeudo Random Number Generator)** - PSeudo numbers are numbers that appears random but are obtained in a deterministic, repeatable and predictable manner.

A pSeudo number generator i.e, PRNG also known as deterministic bit generators i.e 'DRBG' is an algorithm for generating a sequence of numbers whose property approximate the sequence of random numbers.

The PRNG generated sequence is not truely random because it is completely determined by a relatively small set of initial values called the PRNG seed (fixed length of input).

PRNG are used Everywhere in Cryptography that is random numbers are in Session Key, public Key generation and many other places.

PRNG is a Single point of failure for many real world Crypto System. If random numbers are insecure, then the Entire application is insecure.

Some algorithm depend upon PRNG. mainly there are two types of PRNG algorithms. i.e, LCG (Linear Congruential generator) PBS (Plum Blum Shub).

1. **LCG** → a = multiplier, c = increment, m = modulus, x_0 / x_n = initial value, $x_{n+1} = (ax_n + c) \bmod m$

E.g- a = 7, c = 0, m = 32, x_0 / x_n = 1

$x_1 = (7 \times 1 + 0) \bmod 32$

$= 7 \bmod 32$

$= 7$

Types of Random Number Generators

1. PRNG (PSeudo Random Number Generator) - PSeudo numbers are numbers that appears random but are obtained in a deterministic, repeatable and predictable manner.

A pSeudo number generator i.e, PRNG also known as deterministic bit generators i.e 'DRBG' is an algorithm for generating a sequence of numbers whose property approximate the sequence of random numbers.

The PRNG generated sequence is not truely random because it is completely determined by a relatively small set of initial values called the PRNG seed (fixed length of input).

PRNG are used Everywhere in Cryptography that is random numbers are in Session Key, public Key generation and many other places.

PRNG is a Single point of failure for many real world Crypto System. If random numbers are insecure, then the Entire application is insecure.

Some algorithm depend upon PRNG. mainly there are two types of PRNG algorithms. i.e, LCG (Linear Congruential generator) PBS (Plum Blum Shub).

1. LCG → a = multiplier, c = increment, m = modulus, x_0/x_n = initial value, $x_{n+1} = (ax_n + c) \bmod m$

   E.g - a=7, c=0, m=32, x_0/x_n=1

   $x_1 = (7 \times 1 + 0) \bmod 32$

   $= 7 \bmod 32$

   $= 7$

Date / /

$x_2 = (7X7+0) \bmod 32$
$= 49 \bmod 32$
$= 17$
$x_3 = (7X17+0) \bmod 32$
$= 119 \bmod 32$
$= 23$
$x_4 = (7X23+0) \bmod 32$
$= 161 \bmod 32$
$= 1$
$x_5 = \underline{\underline{1}}$

Q. $a=5, C=0, m=32$
→ $x_1 = (5X1+0) \bmod 32$
$= 5 \bmod 32$
$= 5$
$x_2 = (5X5+0) \bmod 32$
$= 25 \bmod 32$
$= 25$
$x_3 = (5X25+0) \bmod 32$
$= 125 \bmod 32$
$= 29$
$x_4 = (5X29+0) \bmod 32$
$= 145 \bmod 32$
$= 17$
$x_5 = (5X17+0) \bmod 32$
$= 85 \bmod 32$
$= 21$
$x_6 = (5X21+0) \bmod 32$
$= 105 \bmod 32$
$= 9$
$x_7 = (5X9+0) \bmod 32$
$= 45 \bmod 32 = 13$

Q. $x_0/x_n = 27, a=17, C=43, m=100$
→ $x_1 = (17X27+43) \bmod 100$
$= (459+43) \bmod 100$
$= 502 \bmod 100$
$= 2$
$x_2 = (17X2+43) \bmod 100$
$= 97 \bmod 100$
$= 77$
$x_3 = (17X77+43) \bmod 100$
$= 1352 \bmod 100 = 52$
$x_4 = (17X52+43) \bmod 100$
$= 927 \bmod 100 = 27$
$x_5 = (17X27+43) \bmod 100$
$= (459+43) \bmod 100$
$= 502 \bmod 100$
$= \underline{\underline{2}}$

Q. $a = 13, C = 0, x_n = 4, m = 64$

→ $x_1 = (13 \times 4 + 0) \bmod 64$

$= 52 \bmod 64$

$= 52$

$x_2 = (13 \times 52 + 0) \bmod 64$

$= 676 \bmod 64$

$= 36$

$x_3 = (13 \times 36 + 0) \bmod 64$

$= 468 \bmod 64$

$= 20$

$x_4 = (13 \times 20 + 0) \bmod 64$

$= 260 \bmod 64$

$= 4$

$x_5 = (13 \times 4 + 0) \bmod 64$

$= 52 \bmod 64$

$= \underline{\underline{52}}$

→ Difference b/w PRNG and TRNG

The difference between PRNG and TRNG is deterministic. PRNG is a deterministic random number generator and TRNG is a non-deterministic random number generator.

PRNG generates a long-length random number using algorithms based on a short initial value.

Date / /

2. TRNG (True random number generators) - TRNG is non deterministic, they are not predictable, not repeatable.

Q. Differentiate b/w TRNG and PRNG.

Note- Applications of Random Numbers (Cryptography, Gaming)

1. IT Security application
* Session Key in a web browser
* Encryption key in RSA algorithm and for generate Symmetric Key and many others.
* lottery numbers
* Key generation for govt. purpose. e.g- ID card, passport.

Note- Gaming - The behaviour of a Computer Controlled Characters.

Note- Almost all Network Security protocols rely on the randomness of Certain parameters.

Q.1 ~~Blowfish~~ Why is Randomness important in Cryptography?
Q.2 characteristic of good PRNG.

A-1. In Cryptography, randomness is important because it removes any reasoning and therefore any predictability. An attacker is usually trying to attain information on a System, When this information is randomly generated there are no clues as to what it maybe and therefore no open opportunities to attack the System.

Date / /

A-2. Characteristics of a Good PRNG:

1. Efficient:

PRNG can produce many numbers in a short time and is advantageous for applications that need many numbers.

2. Deterministic:

A given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known. Determinism is handy if you need to replay the same sequence of numbers again at a later stage.

3. Periodic:

PRNGs are periodic, which means that the sequence will eventually repeat itself. While periodicity is hardly ever a desirable characteristic, modern PRNGs have a period that is so long that it can be ignored for most practical purposes.

Date / /

	Characteristic	PRNG	TRNG
1.	Efficiency	Excellent	Poor
2.	Deterministic	Deterministic	Non-Deterministic
3.	Periodicity	Periodic	Non-periodic

Application

1. Lottery - TRNG
2. Security or Simulation - PRNG

Blowfish Algorithm:

Blowfish is a Symmetric Cryptographic Block Cipher. It was designed by Bruce Schneier in 1993. The first Implementation of the Blowfish algorithm in Labview.

Features of Blowfish Algorithm:

1. It is a symmetric Cryptographic Block Cipher.
2. Block Cipher.
3. It Can be replacement of DES.
4. Blowfish is unpatented and Strong Algorithm.

Objectives:

1. It is fast.
2. It is Compact. (It takes very less memory to execute) i.e, 5Kb.
3. It is very Simple. (It use very Simple operations such as additions, XOR)
4. It is Secure. (because it is use Variable Key length)

Date / /

Note- **Block Size:**

Block Size = 64 bits

Key Size:

Key Size = 32 bit to 448 bit (variable key size)

Round:

Round = 16

Sub Key:

Sub Key = 18 [Array] 0,1 0,2 17

No. of Substitution Box:

S-box = 4 S-box

Size:

Size of s-box = 256 bit

32 bit

Note- Sub Keys is the combination of Integers and hexa decimal

5- There are 3 main step in Blowfish Algorithm :

a- generation of Sub-Key. (18 Sub-Key)

b- initialization of Substitution Boxes (S-boxes) i.e, 4 S-box.

c- EnCryption - In EnCryption function, there are two post-

(1) Round.

(2) Post-processing or undo Swap.

1. **generation of Sub-Key:**

1. There are 18 Sub-Key - P_0 to P_{17} (P[0] ..... P[17]) or (P[1] ..... P[18]) are used for Encryption as well as for deCryption. These 18 Sub-Key are stored in a "P-array" with each array element being 32 bit Entry i.e,

P[0], P[1] ..... P[17]

↓

32 bit Store

2: The Hexadecimal i.e, 0-9 or A-F representation of each Sub-Key.

P[0] = "0 1 9 a 7 6 e 3", (8 data = 32 bit

P[1] = "0 2 8 6 7 a e 4" 8 × 4 bit = 32 bit

Now, Each of the Sub-Key is changed with respect to the Input key

[P0]
[P1]
.
.
.
[P17]

32 — 448

32 32 32

14 × 32 = 448

Total No. of Sub-Keys = 14.

32-bit → XOR with 32 bit Key

P[0] = P[0] XOR K1
P[1] = P[1] XOR K2
P[2] = P[2] XOR K3
.
.
.
P[13] = P[13] XOR K14
P[14] = P[14] XOR K1
.
.
.
P[17] = P[17] XOR K4

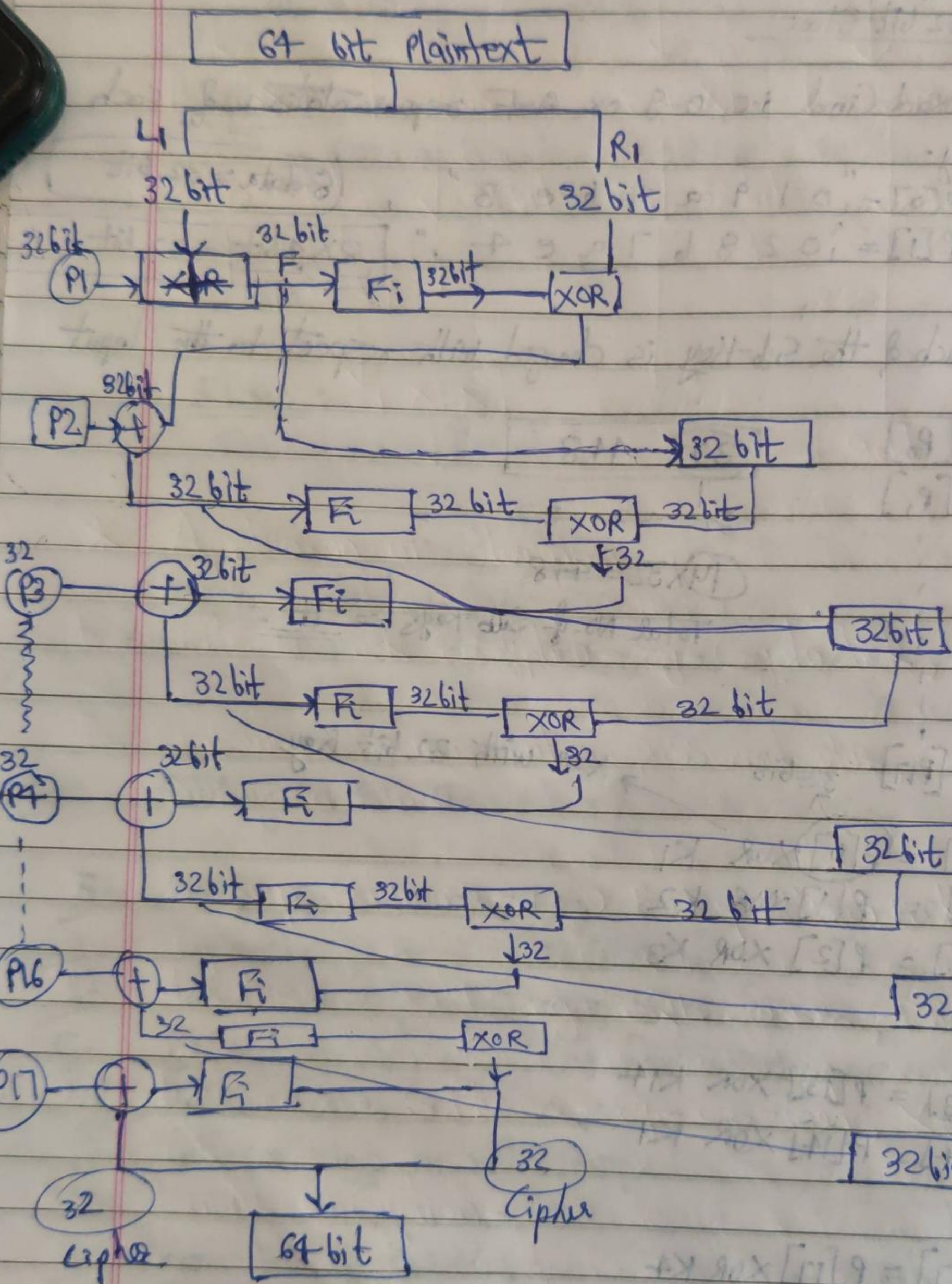
of

2: Initialization Substitution Boxes:

4 S-boxes i.e, S[0], S[1], ... S[3] used for Encryption & for decryption. (256 Entries - 32 bit each)

Date / /

3. EnCryption:



Algorithm for EnCryption for 64 bit Block

1. Divide plain text into two block left and right of Equal Size (32 bit each).

Date / /

2. for i=0 to i=15
OR
for i=1 to i=16.
Left Side
$L_1 = L_1 \oplus R_1$ [P - array derive from generation of Key]

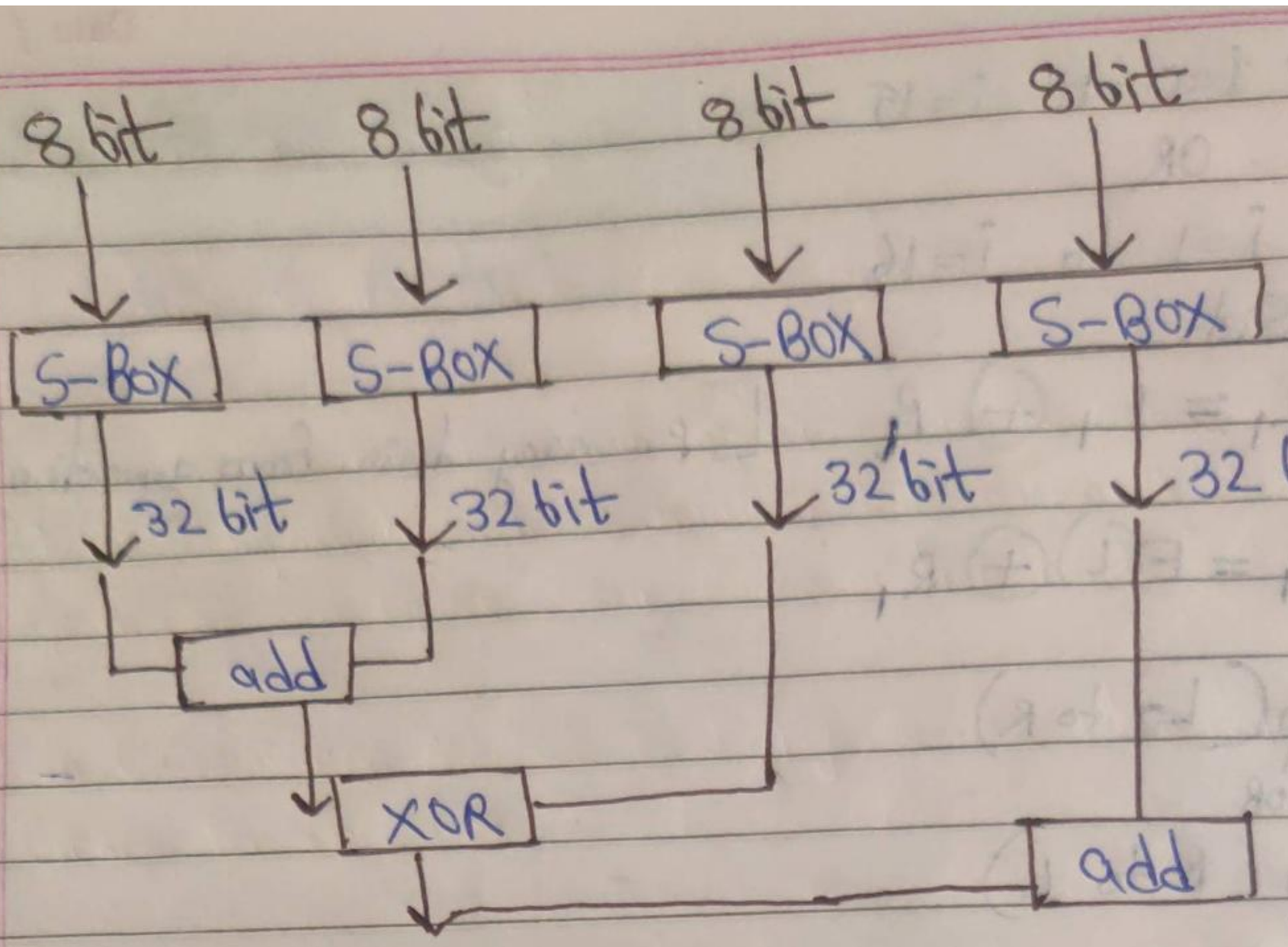
3. $R_1 = F(L) \oplus R_1$

4. Swap (L_2 to R)
OR
Swap (R to L)

5. Undo last Swap :
R = R + P[17] OR R+P[18]
L = L + P[18] OR L+P[17]
~~OR~~ OR
L = L + P[17] + F(R)
After this, Concatenate left and right side to get 64 bit Cipher text.

Function of F

* Function F Split the 32 bit input into 4 parts, 8 bit Each, 8 bit is given as input to Each S-box.
* Each S-box produce 32 bit output. Hence, the function Add [Addition], XOR is perform inside the function.



* Application of Blowfish

1. File of disk Encryption - Eg - Crypto disk, Blowtorch, etc

2. Password management - password plus, Password wallet, password store.

3. Backup Software - LEO Backup, Hoardi Backup

4. Database Security - Eg - SQL Server, DBA toolkit.

5. E-Commerce Software - Eg - CS-Cart, X-Cart.

6. Email Encryption -

* placement of Encryption

1. End to End Encryption - End to End Encryption refers to the process in which Encryption of data are being done at the end host. It is an implementation

hence ensures Date / /

of Asymmetric Encryption and ~~his~~ ~~transfers~~ a secure way of data Communication. It is the most secure way to Communicate privately and securely as data can be read only by the Sender and the receiver. No one else can Encrypt the data including government or even by the Server through which data is passing.

⇒ Working of End to End Encryption

1. It uses asymmetric encryption technique for data Communication between Sender and receiver.

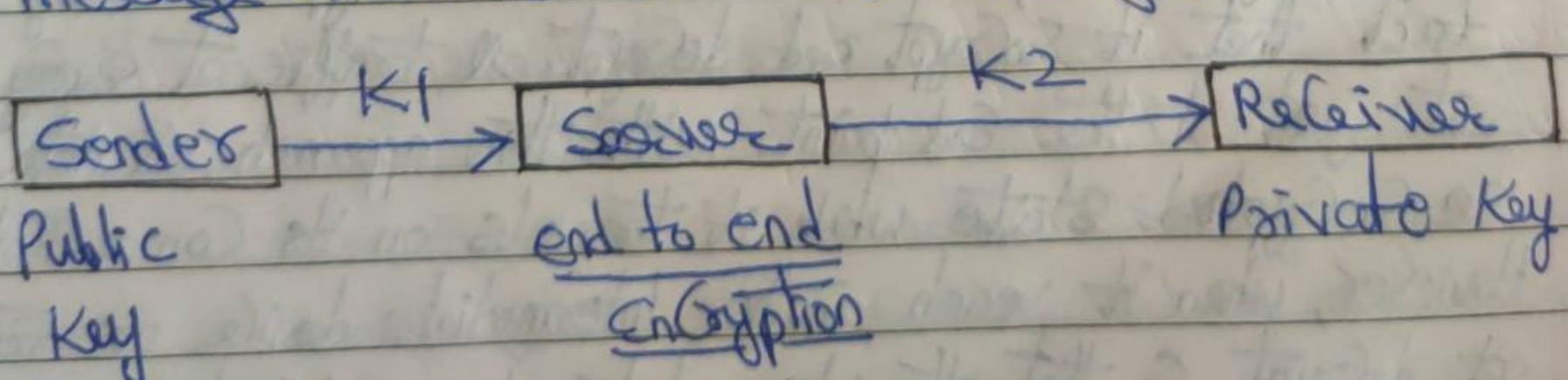
2. Sender use receiver's public Key for Encrypting the message.

3. Sender, then Encrypt the message to be sent using the public Key of receiver.

4. Sender, then Send the encrypted message to the Server.

5. Receiver, then receive the Encrypted message from the Server.

6. Receiver, then using its private Key to decrypt the message and then read the message.



Date / /

~~Link to Link~~ EnCryption

Applications for End to End EnCryption

1. This Method has very high Importance in the case where privacy is Very Important Such as military Information that needs to be protected and where Every Communication need Security.

Note: a) ~~th~~ Communication method is highly Secure when data travel from Sender to receiver

b) It provide greater flexibility to the user as it allow to them to decide which data to Encrypt. It also allow user to decide who has authority to read this message.

c) End-to-End Encryption process can use less resources and time and file size is generally small.

Link-to-Link EnCryption (It happen at lower layer in OSI model)

1. Link Encryption is a technique in which a Communication travelling along a network is Encrypt and decrypt at Every stage or node. It is use to prevent traffic analysis and avoid human Error.

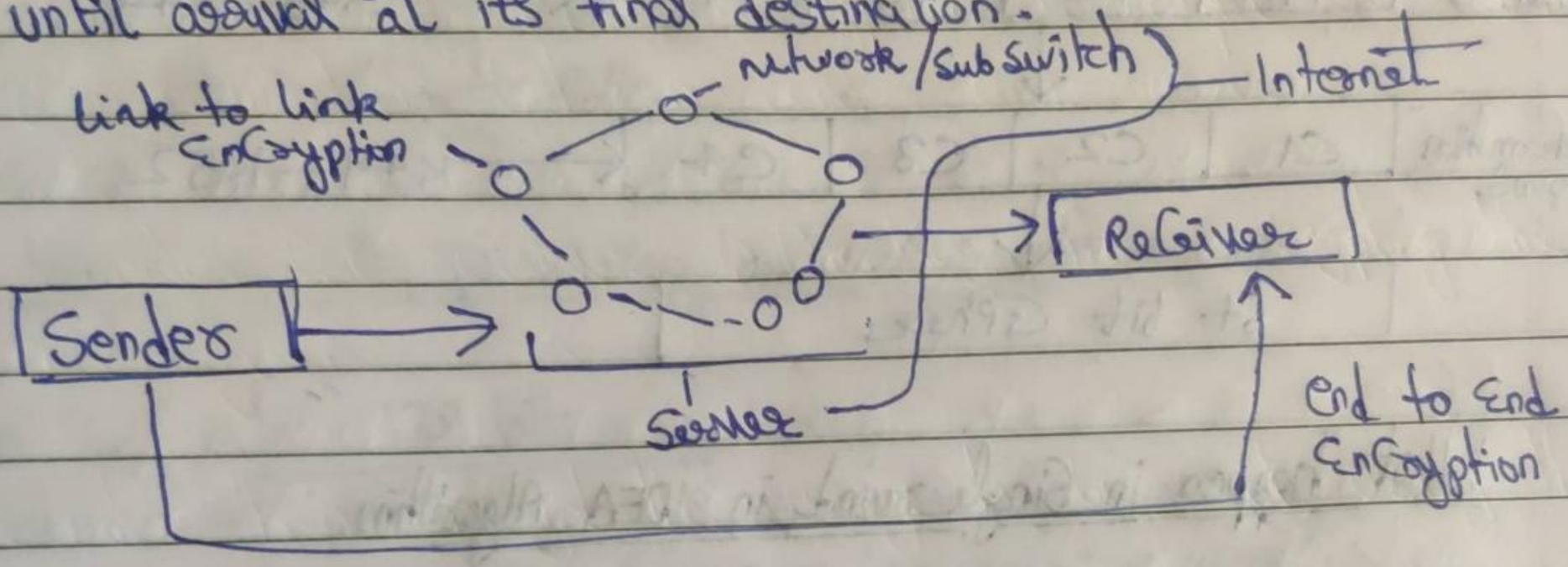
2. Link Encryption differ from End-to-End Encryption mainly in the fact that it Encrypt and decrypt all traffic at Every point, not just at the End point. With this approach, all data is in an Encrypted state while it travels on its Communication path. However, when it reach another Intermediate device or router, it get decrypt so that the intermediater knows which way to send it next.

Date / /

3. Sometime, link-to-link EnCryption called online EnCryption. usually it is used in Network ProtoCols.

Note: a) Link EnCryption is less secure as compared to End to End EnCryption.

b) Link EnCryption is an approach to Communication Securely that EnCrypt and deCrypt all traffic at each network routing point. E.g → Network Switch or nodes through which it passes until arrival at its final destination.



IDEA Algorithm (International data EnCryption Algorithm)

1. International data EnCryption Algorithm is a Symmetric key EnCryption or block Cipher designed by James Massey and Xuezia Lia in 1992.

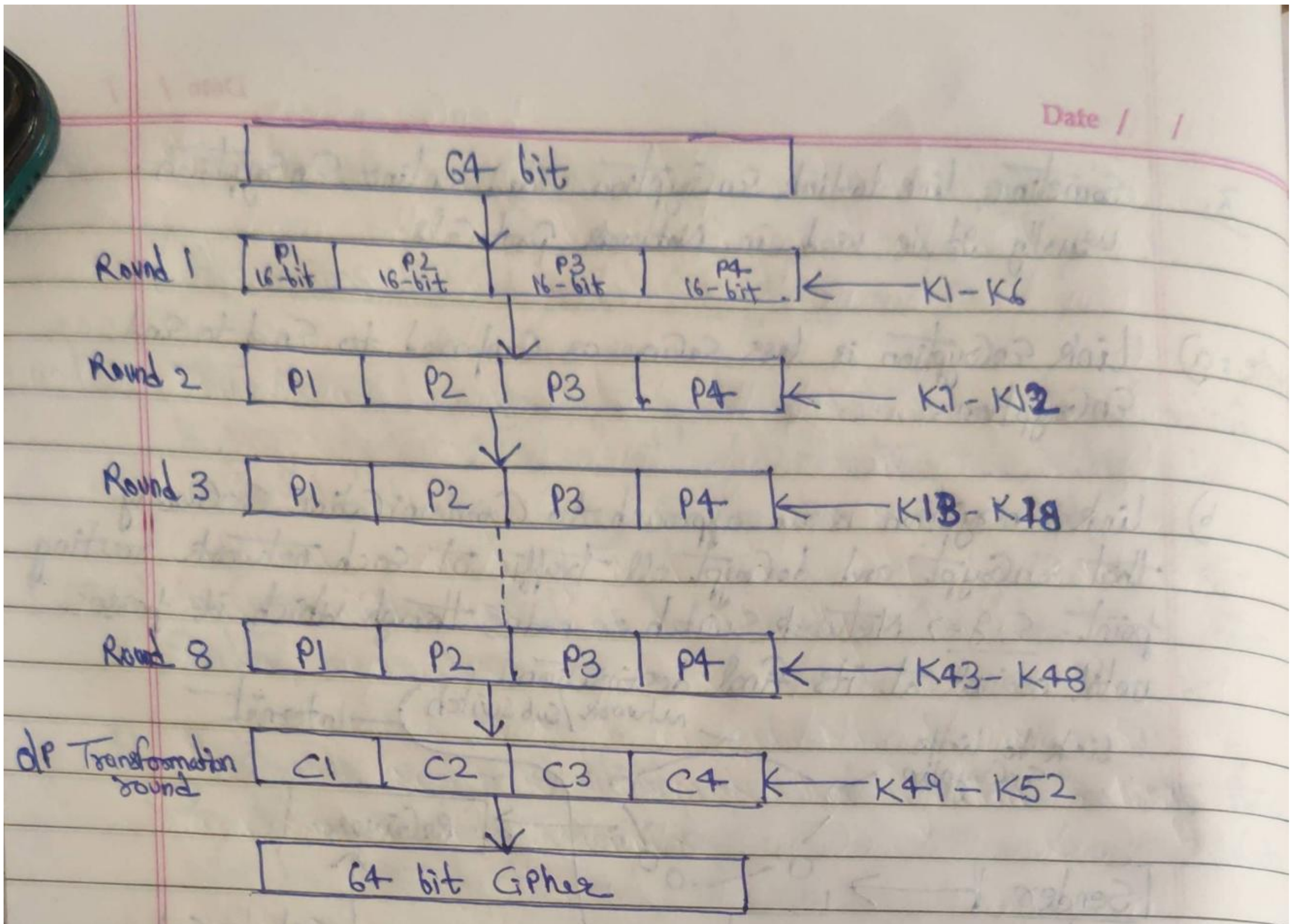
2. It is a reversible like DES.

a: Key Size - 128 bit, from which 52 Sub-Key are generated and Each Sub-Key divided into 16-bit.

b: In Each round, Block divided into 4 parts (16-bit Each)

c: There is total 8 round. (In Each round, 6 Sub-Key are used that is $8 \times 6 = 48$ Sub-Key. So, left 4 Sub-Key used in output transformation or one half round.)

d. In last round, i.e, output transformation produce the Cipher text and



What happen in Single round in IDEA Algorithm

Note:- There is total 14 steps to Perform function in Each round.

$S_1 = P1 \times K1$
$S_2 = P2 + K2$
$S_3 = P3 + K3$
$S_4 = P4 \times K4$

$S_5 = S1 \oplus S3$
$S_6 = S2 \oplus S4$

$S_7 = S5 \times K5$
$S_8 = S6 + S7$

$S_9 = S8 \times K6$
$S_{10} = S7 + S9$

$S_{11} = S1 \oplus S9$ — P1
$S_{12} = S3 \oplus S9$ — P2

Date / /

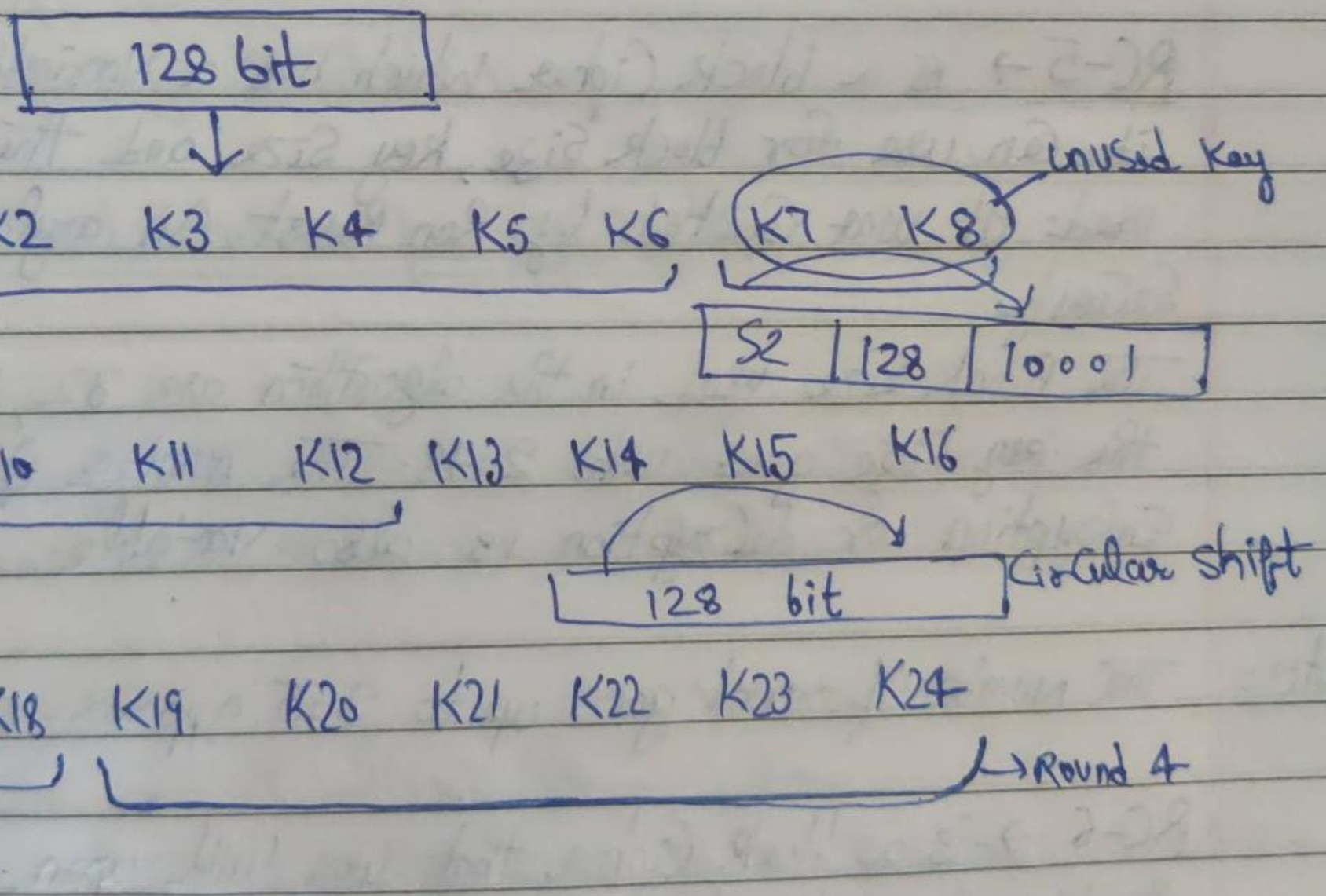
$S_{13} = S2 \oplus S10 - P3$
$S_{14} = S4 \oplus S10 - P4$ } → Ciphor

Output Transformation

Note- It take plaCe at the End of 8th round. Input to this Block is a 64 bit Value divided into 4 Sub-block that is P1, P2, P3, P4.

P1 x K49 — C1
P2 + K50 — C2
P3 + K51 — C3
P4 x K52 — C4

How to genrate 52 Sub-Key In IDEA Algorithm



Q. Write a breif note on How to generate Sub-Key In IDEA Algorithm.

Date / /

RC-4 → is one of the most commonly implemented Stream Cipher. It has a variable Key Size, is used in the SSL protocol (Secure Socket layer)

Note: SSL is a Connection b/w web browser and the particular server

* RC-4 was developed in 1987 by Ron Rivest and was considered a secret of RSA data Security. The Source Code of this algorithm was posted Publically.
Since, the Source Code was RC-4 was released then it makes some changes on RC-4 and published at ARE4 because the titled RC-4 is trademark. This algorithm is very fast and simple and efficient.

RC-5 → is a block Cipher which has a variety of parameter it can use for block size, key size and the number of round used. It was created by Ron Rivest. An argolas by RSA data Security.
The Block Size used in the algorithm are 32, 64, 128 bit and the key size goes upto 2048. The number of round used in Encryption or decryption is also variable.

Note: The number of rand goes up to 255 approx.

RC-6 → is a block Cipher that was build upon RC-5. So, it has all the same attribute as RC-5. The algorithm was developed mainly to be submitted as AES. by Rijndael was chosen instead. There were some modification of the RC5 algorithm to increase to over all speed, the result of which is RC-6

Note: Strength and weakness of Symmetric Encryption.

Date / /

Strengths:

1. Symmetric Encryption must faster than Asymmetric system.
2. Difficult to break to large key size.

Weakness:

1. Requires a secure mechanism to deliver key Properly.
2. Each pair of users need a unique key so, as the no of individual increases, so thus the no. of key possible making Key management.
3. It provides Confidentiality but not authenticity.

e.g → DES, 2DES, 3DES, AES, Blowfish.

Limitations of Symmetric Encryption:

1. Security service
2. Security key distribution

Strength and Weakness of Cryptosystem

Strengths:

1. Better Key distribution than Symmetric System.
2. It Can provide authentication.

Weakness:

1. Uses much more slowly Symmetric System.
2. Difficult mathematic Concept is used in Asymmetric algorithm.

RSA Algorithm (Rivest, Shamir, Adleman) developed in 1978
It is an asymmetric Cryptographic algorithm i.e, is public and private Key.

* public Key - This Key is known to all users in the network.

* Private Key - Not shareable to all. It is kept secret.

If public key of user A is used for Encryption, we have to use the private key for same user decryption.
The RSA schemes the block cipher in which the plaintext and Cipher text. An Integer b/w 0 & n-1 for some value n.

Algorithm:

Key generation:

Select 2 large prime number 'P' and 'Q'.

Calculate $\boxed{n = P \times Q}$

Now Calculate $\phi(n) = (P-1) \times (Q-1)$

choose value of (e)

$$1 < e < \phi(n)$$

i.e,

$GCD = (e, \phi(n)) = 1$

↓

(Co-prime)

Calculate d

↓

$\boxed{e \times d \bmod \phi(n) = 1}$

OR

$\boxed{ed = 1 \bmod \phi(n)}$

OR — integer value

$$\boxed{d = \frac{1 + (K) \times \phi(n)}{e}} \Rightarrow (K \leq 0)$$

Easy

public Key - $\{e, n\}$

Private Key - $\{d, n\}$

Encryption $\rightarrow$ $C = m^e \bmod n$ | $m = C^e \bmod n$

OR

$C = pe \bmod n$

$m \$ P \Rightarrow$ It is a plaintext indicate

Decryption $\rightarrow \boxed{m = cd \bmod n}$

By using algorithm, we Encryption and decryption point $m = 3,5$ and plain text of or message is 8.

Q. $P=3, q=5$

Find Encryption and decryption using RSA Algorithm where Msg is 8. Also find e, d ?

$\rightarrow$ $n = P \times q = 3 \times 5 = 15$

$n = 15$

$\phi(n) = (P-1)(q-1) = (3-1)(5-1) = (2)(4) = 8$

$\phi(n) = 8$

e	$\phi(n)$
2	3
3	
4	5
5	
6	7
7	

$e = \{3, 15\}$

$d = \frac{1 + K \times 8}{3} \Rightarrow \frac{1+15\times8}{3} = \frac{1+120}{3} = \frac{121}{3} = 4033$

$ed = 1 \bmod \phi(n) \Rightarrow ed \bmod \phi(n) = 1 \bmod \phi(n)$

~~$3d = 1 \bmod 8$~~ $3 \times d \bmod 8 = 1$

OR

$d = \frac{1 + K(\phi n)}{e} \Rightarrow \frac{1 + \phi(n)}{e} = \frac{1 + 1 \times 8}{3}$

$= \frac{9}{3} = 3$

$d = \{3, 15\}$

Date / /

Encryption → $C = m^e \bmod n$

$C \bmod n = m^e \bmod n$

$8 \bmod 15 = x^3 \bmod 15$

$7 = 0 \times 3 \bmod 15$

$8 = C^3 \bmod 15$

$8 = 8^3 \bmod 15$

$512 \bmod 15$

decryption → $m = c^d \bmod n$

$8 = 9 \times 3 \bmod 15$

$8 =$

Q. In RSA CryptoSystem, a ~~plaintext~~ participant A use two prime numbers i.e, 3, 11 to generate her public and Private Key. If the public key i.e, 'e' is 3. then, find out private key of A. also find Encryption and decryption value. Msg = 2.

→ $p = 3, q = 11$

$n = 3 \times 11 = 33$

$\phi(n) = (11-1)(3-1) = 10 \times 2 = 20$

$e = 3$

$d = \frac{1 + K(\phi(n))}{e}$

$= \frac{1 + 4 \times 20}{3} = \frac{81}{3} = 27$

$d = \frac{1 + 1 \times 20}{7} = \frac{21}{7} = 3$

Date / /

Encryption ~~et~~

Q- P=3, q=11, e=17, m=13. find out public and private key and Encryption and deCryption by using RSA Algorithm.

→ $n = P \times q = 3 \times 11 = 33$

$\phi(n) = (3-1)(11-1) = 2 \times 10 = 20$

$e = 17$

$d = \frac{1 + x20}{17}$

Q: Encrypt plaintext 9 using RSA public key Encryption Algorithm where prime number 7 and 11 to generate the public and private key. And also find message and Cipher Text. Note, e = 7, 13.

→ $n = P \times q$

$n = 7 \times 11 = 77$

$e = 7$

$d = \frac{1 + K(\phi(n))}{7}$

$d = \frac{1 + 2(60)}{7}$

$d = \frac{121}{7}$

$d = \frac{1 + 5(60)}{7}$

$d = \frac{301}{7}$

$\boxed{d = 43}$

$\phi(n) = (7-1) * (11-1)$

$= 6 * 10$

$= 60$

$d = \frac{1 + 3(60)}{7} = \frac{181}{7}$

$d = \frac{1 + 4(60)}{7} = \frac{241}{7}$

Euler's Totient function

1. It is represent using "Phi" i.e, ϕ as. $\phi(n)$. and may also be called Eulers phi function.

2. Euler Totient Function is defined as the number of positive integers less than 'n' that are Co-prime to 'n'. e.g → $\phi(5)$ and $\phi(6)$.

$\phi(5) = 1, 2, 3, 4 = (4)$

$\phi(6) = 1, 2, 3, 4, 5 = (2)$

$\boxed{\phi(n) = n-1}$

Note- Two Integers A, B are said to be Relatively prime, mutually prime or Co-prime. If the only positive Integer, factor that divides both of them is one.

3. When n is equal to prime number, then $\boxed{\phi(n) = n-1}$

If $\phi(a * b) = \phi(a) * \phi(b)$,

If 'a' and 'b' is always be a prime number.

e.g → 1. $\phi(35) = \phi(7) * \phi(5)$

$= 6 \times 4 = (24)$

2. $\phi(15) = \phi(5) * \phi(3)$

$= 4 \times 2 = (8)$

Euler's Theorem

1. It is also called Format Euler theorem or Euler's totient Theorem.

2. Euler's theorem states that if 'x' and 'n' or 'p' and 'q' are Co-prime Positive Integers. then $x^{\phi(n)} \equiv 1 \bmod n$ or

$x^{\phi(n)} \bmod n = 1 \bmod n$

or

$p^{\phi(q)} \equiv 1 \bmod q = p^{\phi(q)} \bmod q = 1 \bmod q$

or $\phi(q)$

where, $\phi(n)$ denotes Euler's Totient function.

Example- Assume $x=11$ or $p=11$, $n=10$ or $q=10$. find out Represent by using both the value it satisfies Euler's theorem or not.

→ ~~$\phi(n) = (11-1)\times(10-1) = 10\times 9 = 90$~~

By using Euler's theorem,

$x^{\phi(n)} \equiv 1 \bmod n \Rightarrow x^{\phi(n)} \bmod n = 1 \bmod n$

~~$\phi(11) = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 = 10$~~

$\phi(10) = 1, 2, 3, 4, 5, 6, 7, 8, 9 = 4$

$11^4 \bmod 10 = 1 \bmod 10$

$14641 \bmod 10 = 1 \bmod 10$

$1 = 1$

Q. Verify Euler Theorem $p=3$, $q=10$.

→ $x=3$, $n=10$

$\phi(10) = 4$ using Euler's theorem,

$x^{\phi(n)} \equiv 1 \bmod n$

$x^{\phi(n)} \bmod n = 1 \bmod n$

$3^4 \bmod 10 = 1 \bmod 10$

$81 \bmod 10 = 1 \bmod 10$

$1 = 1$

Format Theorem

1. If 'n' is prime and 'x' is a positive Integer not divisible by 'n' then;

1st form: $x^{n-1} \equiv 1 \bmod n$

or (use any form)

Another form of Fermat theorem 2nd form: $x^n \equiv x \mod n$

or, $a^p \equiv a \pmod p$

Note- where: n prime number

x is not divisible by n also x, n should be Co-prime.

Example- $x=3, n=5$

using Fermat's theorem 1st form:

$$x^{n-1} \equiv 1 \mod n$$

$$3^{5-1} \equiv 1 \mod 5$$

$$3^{5-1} = 81$$

Therefore 81 is Congruent to 1 mod 5 i.e, $81 \equiv 1 \mod 5$ means

$81 \mod 5 = 1$

$5 = 1$

Solve Same Example using 2nd form of Fermat's theorem:

$X = 3, n = 5$

$X^n \equiv X \mod n$

$3^5 = 243$

$243 \equiv 3 \mod 5$

means $243 \mod 5 = 3 \mod 5$

$243 \mod 5 = 3$

$3 \mod 5 = 3$

That is both LHS and RHS ~~are equal~~ = 3 remainder

Q: Verify Format Theorem for $x=2, n=17$

→ using Format's theorem 1st form:

$$x^{n-1} \equiv 1 \mod n$$

$$2^{17-1} \equiv 1 \mod 17$$

$$2^{16} \equiv 1 \mod 17$$

$2^{16} \mod 17 = 1 \mod 17$

$65536 \mod 17 = 1 \mod 17$

$1 = 1$

Date / /

Rabin Cryptosystem

1. Rabin Cryptosystem is a public key Cryptosystem invented by Michael Rabin. It uses asymmetric key Encryption for Communicating between two parties and Encrypting the message.

2. Rabin Cryptosystem is based on quadratic Congruency.

3. The Rabin Cryptosystem Can be taught of same as or similar as RSA Cryptosystem in which the value of 'e' and 'd' are fixed. The Encryption is $C \equiv P^2 \pmod{n}$. The decryption is:
$P \equiv C^{1/2} \pmod{n}$.
In Rabin Cryptosystem, public key is 'n' and private key is 'p' and 'q'.

Step in Rabin CryptoSystem

1. Key generation
2. Encryption
3. Decryption

1. Key generation:

1. Generate two very large prime numbers, p and q, which satisfies the condition:
$p \neq q \rightarrow p \equiv q \equiv 3 \pmod 4$ or $4K+3$ & $p \neq q$
For Example:
$p = 139$ and $q = 191$
2. Calculate the value of n
$n = p.q$
3. publish n as public key and save p and q as private key.

2. Encryption:

1. Get the public key n.

Date / /

2. Convert the message to ASCII value. Then convert it to binary and extend the binary value with itself, and change the binary value back to decimal m.

3. EnCrypt with the Formula:
$C = p^2 \bmod n$

4. Send C to recipient.

3. DeCryption:

$a_1 \leftarrow +\left(C^{(p+1)/4}\right) \bmod p$

$a_2 \leftarrow -\left(C^{(p+1)/4}\right) \bmod p$

$b_1 \leftarrow +\left(C^{(q+1)/4}\right) \bmod q$

$b_2 \leftarrow -\left(C^{(q+1)/4}\right) \bmod q$

Note: The Rabin CryptoSystem is not deterministic: DeCryption Creates four plaintexts.

Example:

1. ~~Both~~ Bob selects $p = 23$ and $q = 7$. Note that Both are Congruent to 3 mod 4.

2. Bob Calculates $n = p * q = 161$.

3. Bob announces n publicly; he keeps p and q private.

4. Alice wants to send the plaintext $p = 24$. Note that 161 and 24 are relatively prime; 24 is in Z_{161}^*.

She Calculates $C = 24^2 = 93 \bmod 161$, and sends the Ciphertext 93 to Bob.

5. Bob receives 93 and Calculates four values:

$a_1 = +\left(93^{(23+1)/4}\right) \bmod 23$

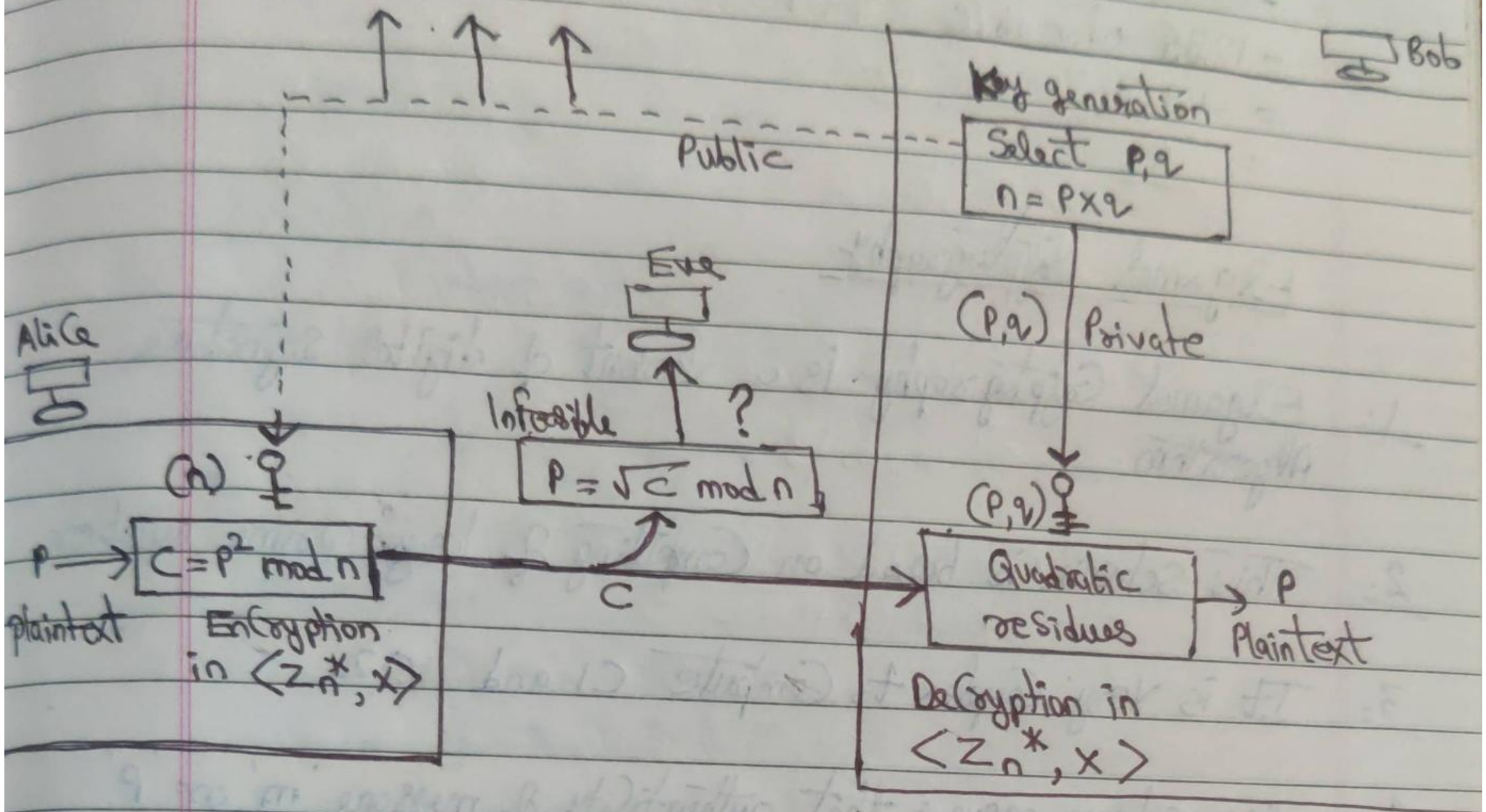
$a_2 = -\left(93^{(23+1)/4}\right) \bmod 23$

$b_1 = +\left(93^{(7+1)/4}\right) \bmod 7$

$b_2 = -\left(93^{(7+1)/4}\right) \bmod 7$

6. Bob takes four possible answers, (a_1, b_1), (a_1, b_2), (a_2, b_1) and (a_2, b_2), and uses the chinese remainder theorem to find four

possible plaintexts: 116, 24, 137 and 45. Note that only the second answer is Alice's plaintext.



Q. Let P = 11, q = 7. Find out public Key and show Encrypt and decryption process using rabin Cryptosystem.

→ $P \equiv q \equiv 3 \pmod 4$.

$n = P \times q = 11 \times 7 = 77$

$11 \bmod 4 = 3 \bmod 4$, $7 \bmod 4 = 3 \bmod 4$

$3 = 3$ $\quad 3 = 3$

$C = P^2 \bmod n$

$C = 121 \bmod 77$

$C = 44$

$a_1 \leftarrow + \left(44^{\frac{3}{4}}\right) \bmod 11$

$a_2 \leftarrow - \left(44^{\frac{3}{4}}\right) \bmod 11$

$b_1 \leftarrow + \left(44^{\frac{3}{4}}\right) \bmod 7$

$b_2 \leftarrow - \left(44^{\frac{3}{4}}\right) \bmod 7$

$a_1 = 44^3 \bmod 11 = 85184 \bmod 11 = 7744$

$a_2 = -44^3 \bmod 11 = -85184 \bmod 11 = -7744$

$b_1 = 44^2 \bmod 7 = 1936 \bmod 7 = 4$

$b_2 = -44^2 \bmod 7 = -1936 \bmod 7 = 3$

Date / /

Note- $-8649 \bmod 7$

$= -1235, 4, 7$ (-8649 ke res ab/c)

-1235 ka or ab/c $7+7$

$= -169, 3, 7$

$= 3$

Elgamal Cryptography

1. Elgamal Cryptography is a variant of digital Signature Algorithm.

2. This scheme is based on Computing of large prime number.

3. It is very Complex to Compute C1 and C2.

4. This scheme assures that authenticity of message 'm' or 'P' Sent by Sender to verifier.

5. As with Elgamal Encryption, the global elements of Elgamal digital Signature is based on prime number and based on primitive roots.

Key generation:

1. Select large prime number, $P = 11$
2. Select decryptive key also called private key denoted by d or x $= 3$.
3. Select second part of Encryption Key i.e. 'e1' or 'g' $= 2$.
4. Select third part of Encryption Key i.e 'e2' or 'y'.

If e2 is not given, then we find the value of e2:

$$e2 = e_1^d \bmod P$$

OR

$$e2 = g^x \bmod P$$

$e_2 = 2^3 \bmod 11$

$e_2 = 8 \bmod 11 = 8$

$e_2 = 8$. i.e, public Key $= (P, e_1, e_2)$

public key $= (11, 2, 8)$

private Key $= 3$

Encryption:

1. Select Random Integer r or $K = 4$.
2. Calculate $C_1 = e_1^r \bmod P$

OR

e_1^K or mod P

$C_2 = m \times e_2^K \bmod P$

Assume $m = 7$

$C_1 = 2^4 \bmod 11$

$= 16 \bmod 11 = 5$

$C_2 = 7 \times 8^4 \bmod 11$

~~$= 7 \times 16 \bmod 11$~~ $= 286172 \bmod 11$

~~$= 112 \bmod 11 = 2$~~ $= 6$

DeCryption:

$$D = \left[C_2 \times \left((C_1)^d \right)^{-1} \right] \bmod P$$

$$D = \left[6 \times \left((5)^3 \right)^{-1} \right] \bmod 11$$

$$= \left[6 \times (125)^{-1} \right] \bmod 11$$

$= 125 \times x \bmod 11 = 1 \Rightarrow 125 \times 3 \bmod 11 = 1$

$\Rightarrow 375 \bmod 11 = 1$

$\Rightarrow 6 \times 3 \bmod 11 \Rightarrow 18 \bmod 11 = 7$

Date / /

Q. $P = 13, e_1 = 2, d = 3, r = 7, m = 4$. Find out C_1, C_2 & DeCryption by using Elgamal ~~Algorithm~~ Cryptography.

→ $C_1 = e_1^r \bmod P$

$= 2^7 \bmod 13$

$= 128 \bmod 13$

$= \underline{\underline{11}}$

$e_2 = e_1^d \bmod P$

$= 2^3 \bmod 13$

$= 8 \bmod 13$

$= 8$

$C_2 = m \times e_2^K \bmod P$

$= 4 \times 8^7 \bmod 13$

$= 4 \times 2097152 \bmod 13$

$= 8388608 \bmod 13$

$= \underline{\underline{7}}$

$D = \left[7 \times \left((11)^3 \right)^{-1} \right] \bmod 13$

$= \left[7 \times (1331)^{-1} \right] \bmod 13$

$\Rightarrow 1331 \times x \bmod 13 = 1$

$\Rightarrow 1331 \times 8 \bmod 13 = 1$

$\Rightarrow 10648 \bmod 13 = 1$

$\Rightarrow 7 \times 8 \bmod 13 = 56 \bmod 13$

$\Rightarrow \underline{\underline{4}}$

Date / /

Q.1 $x=3, n=5$. Solve by using Fermat's Theorem.

Q.2 $x=6, n=7$. Solve by using Fermat's Theorem.

Q3 $x=11, n=10$. Solve by using Fermat's Theorem.

Q.4 $P=3, q=10$. Solve by Euler Theorem.

Q5 $P=11, g=2, d=3, K=4, m=7$. Find out Cipher Text and decryption message by using Elgamal Cryptography.

A.1. $x^{n-1} \equiv 1 \bmod n$

$3^{5-1} \equiv 1 \bmod 5$

$3^4 \equiv 1 \bmod 5$

$81 \bmod 5 = 1 \bmod 5$

$1 = 1$

A.2. $x^{n-1} \equiv 1 \bmod n$

$6^{7-1} \equiv 1 \bmod 7$

$6^6 \equiv 1 \bmod 7$

$46656 \bmod 7 = 1 \bmod 7$

$1 = 1$

A3. $x^{n-1} \equiv 1 \bmod n$

$11^{10-1} \equiv 1 \bmod 10$

$11^9 \equiv 1 \bmod 10$

$2357947691 \bmod 10 = 1 \bmod 10$

$1 = 1$

A.4. $x = 3, n = 10$

$\phi(10) = 4$ using Euler's theorem,

$x^{\phi(n)} \equiv 1 \bmod n$

$\mathcal{E}^{\phi/n} \bmod n = 1 \bmod n$

$3^4 \bmod 10 = 1 \bmod 10$

$81 \bmod 10 = 1 \bmod 10$

$\underline{1 = 1}$

A-5- $C_1 = e_1^r \bmod p$

$= 2^4 \bmod 11$

$= 16 \bmod 11 = \boxed{5}$

$C_2 = e_1^d \bmod p$

$= 2^3 \bmod 11$

$= 8 \bmod 11$

$= \underline{8}$

$C_2 = m \times e_2^K \bmod p$

$= 7 \times 8^4 \bmod 11$

$= 28672 \bmod 11$

$= \boxed{6}$

$D = \left[6 \times ((5)^3)^{-1} \right] \bmod 11$

$= \left[6 \times (125)^{-1} \right] \bmod 11$

$= 125 \times x \bmod 11 = 1 \Rightarrow 125 \times 3 \bmod 11 = 1$

$\Rightarrow 375 \bmod 11 = 1$

$\Rightarrow 6 \times 3 \bmod 11 \Rightarrow 18 \bmod 11 = \boxed{7}$

Q6 Alice selects 2 prime number : $p = 5, q = 11$, Alice selects her public exponent $= 3$ Compute d, the private exponent of Alice.

Date / /

~~P=5, q=11, c_1=3,~~

→ Assignment-2

Q.1. Differentiate b/w Conventional Encryption and public Key.

Q.2. Differentiate b/w RSA and DES.

Q.3. Sender A choose p=13 and e_1=2 and d=3. So, the public Key are p, g, e and the Private Key is 3. Now, Receiver select, r=7 and Calculate C_1 and C_2 for the plaintext 4.

Q.4. Write a brief note on Key Management System and public Key distribution.

Q.5 Write a brief note on 'What are the Requirement of Authentication in Cryptography'.

A.6. P=5, q=11, e=3

$ed \bmod \phi(n) = 1$

or

$ed = 1 \bmod \phi(n)$

~~$3 \times d = 1 \bmod 40$~~

~~$d = \frac{1 \bmod 40}{3} = \frac{1}{3}$~~

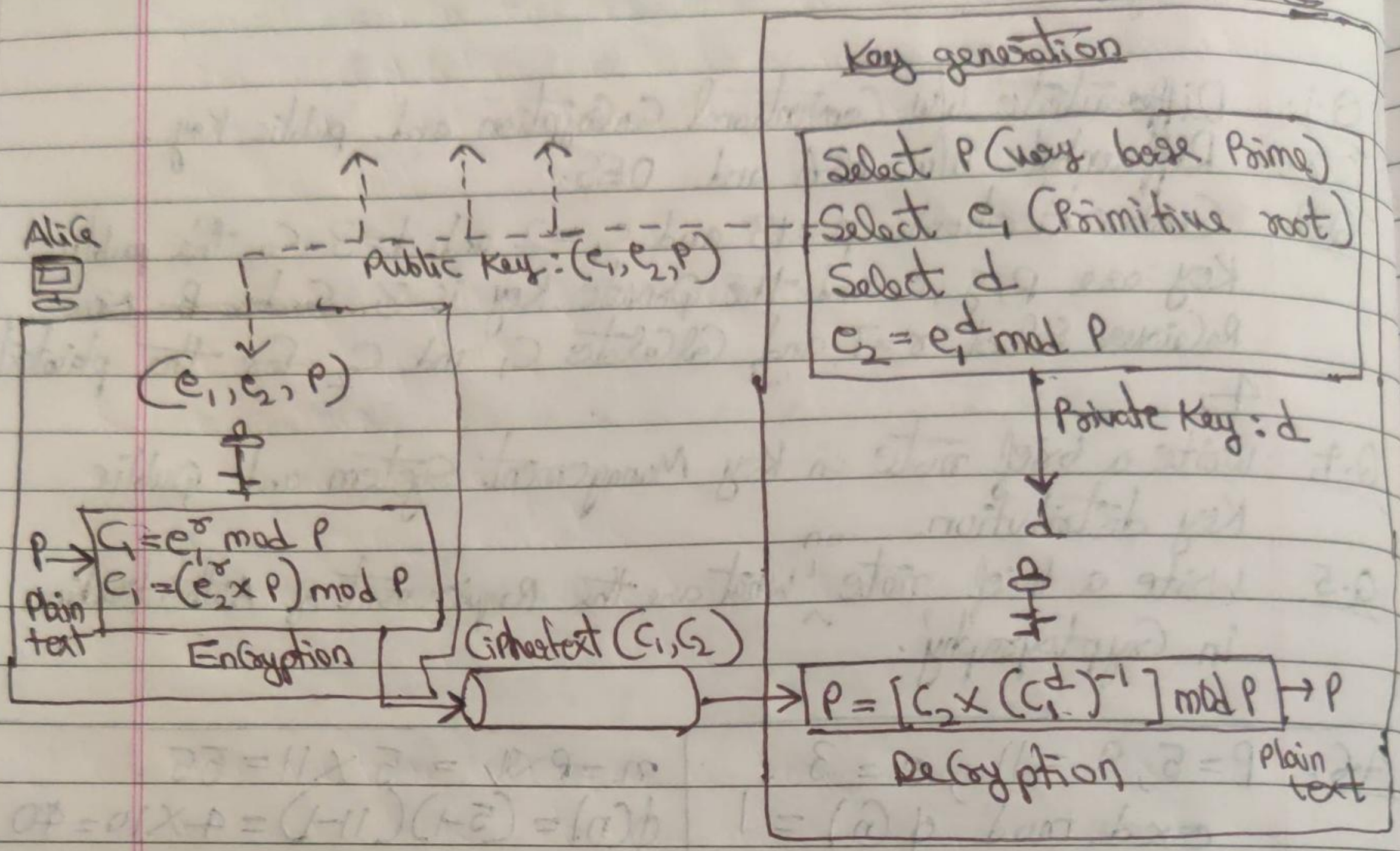
or, $d = \frac{1 + K(\phi n)}{3} \Rightarrow \frac{1 + 2 \times 40}{3} = \frac{1+80}{3} = \frac{81}{3}$

$\Rightarrow$ 27

$n = p \times q = 5 \times 11 = 55$

$\phi(n) = (5-1)(11-1) = 4 \times 10 = 40$

Block diagram of Elgamal Cryptography



Hash Function

Hash Function are Irreversible, one way function which protect the data at the cost of not being able to recover the original message.

Hashing is a way to Transform a given String into a fix length String. A good hashing algorithm will produce unique output for each input given. A hash can be used for hashing data such as a hash can be used for hashing data such as password and in Certificates. It is also called Compressed Numerical Value.

Hash Function is a Series of mathematical Concept or Series mathematical process that hold role in public Key Cryptography.

Role in Public Key Cryptography

1- ~~Secure~~ Securely Store password in database.

2. Ensure data Integrity by ~~Integrating~~ Indicating when data has been altered.

3. Make Sure Authentication possible.

Q. Write Some Properties of Hash Algorithm.

Note → Message Digest

→ A message Digest is a fixed Size numeric representation of the Content of a message Computed by a hash function. A message digest Can be encrypted forming a digital Signature.

Note - A message digest Created using a Secret Symmetric Key is known as message authentication Code (MAC) because, it Can provide Security that the message had not been modified.

Note - A message digest is Computed by a hash function which is a transformation that meets two Criteria:

1. The Hash Function must be one way. It must not be possible to reverse the function to find the message Corresponding to a particular message digest, other than by testing all possible message.

2. It must be infeasible to find two message that hash to the Same digest.

Examples of Common Hashing Algorithms & Families of Algorithms

1. Secure Hash Algorithm (SHA) - This family of hashes Contains SHA-1, SHA-2 (a family within a family that includes SHA-224, SHA-256, SHA-384, and SHA-512), and SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512). SHA-1 has been deprecated and the most Commonly hashing algorithm now is SHA-256.

Date / /

2. Message Digest (MD) - This family of hashes contains a variety of hash functions that include MD2, MD4, MD5, and MD6. MD5 was long considered a go-to hashing algorithm but it's now considered broken because it results in collisions in the wild.

Applications of Cryptographic hash functions

Note- Some of the uses of hashing include:

* Digital Signatures,
* Biometrics,
* Password Storage,
* Code Signing Certificates,
* Document Signing Certificates, and
* Email Signing Certificates

Note- When you have to compare a large piece of data or software you can't check each code and word of it. But if you hash it, it converts big data into small, fixed length hash values which you can check and compare a lot more easily.