**Features Of Cryptography are as follows:**

**Confidentiality**:

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

**Integrity**:

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

**Non-repudiation:**

The creator/sender of information cannot deny his or her intention to send information at later stage.

**Authentication**:

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

**OR**

Cryptography deals with various security principles, which are as follows:

**Confidentiality –** It specifies that only the sender and the recipient or recipients should be able to access the message. Confidentiality will get lost if an authorized person can access a message.

**Authentication –** It identifies a user or a computer system so that it can be trusted.

**Integrity –** It checks that a message’s contents must not be altered during its transmission from the sender to the recipient.

**Non-repudiation –** It specifies that the sender of a message cannot be refused having sent it, later on, in the case of a dispute.

**Types** **Of** **Cryptography**:

In general there are three types Of cryptography:

**Symmetric Key Cryptography:**

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

**Hash Functions**:

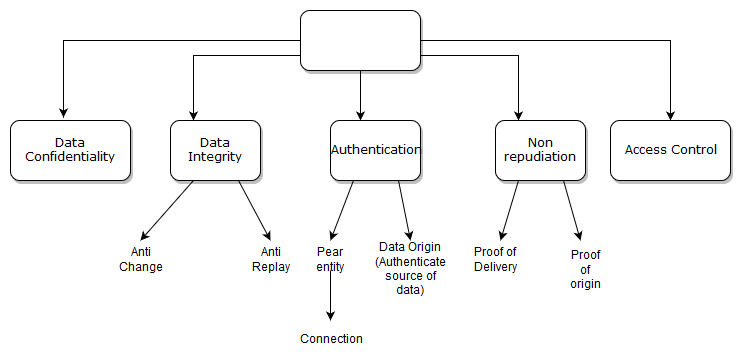
There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

**Asymmetric Key Cryptography**:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

**Security services**

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. Following are the five categories of these services:



**1.Authentication**: The assurance that the communicating entity is the one that it claims to be.

**Peer Entity** Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.

**Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.

**2.Data Confidentiality**: Protects data from unauthorized disclosure.

**3.Access Control:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

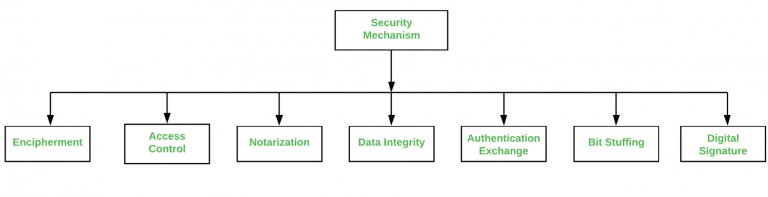
**4.Data Integrity**: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

**5.Non-repudiation:** Protects against denial by one of the entities involved in a communication of having participated in all or part of the communication.

**Proof of Origin**: Proof that the message was sent by the specified party.

**Proof of Delivery**: Proof that the message was received by the specified party.

**Types of Security Mechanism are :**



**Encipherment** :

This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form.

It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

**Access Control :**

This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

**Notarization :**

This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

**Data Integrity** :

This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

**Authentication exchange :**

This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

**Bit stuffing** :

This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

**Digital Signature** :

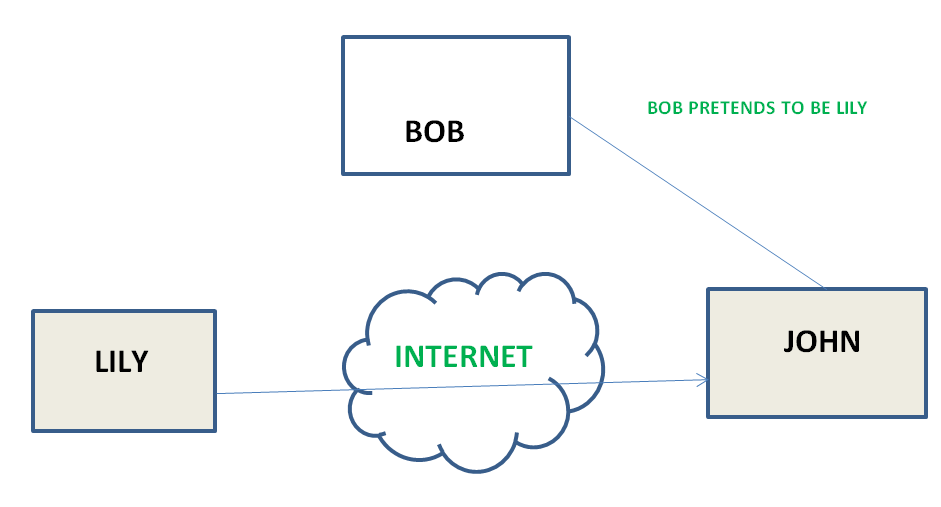
This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender’s identity is to be notified.

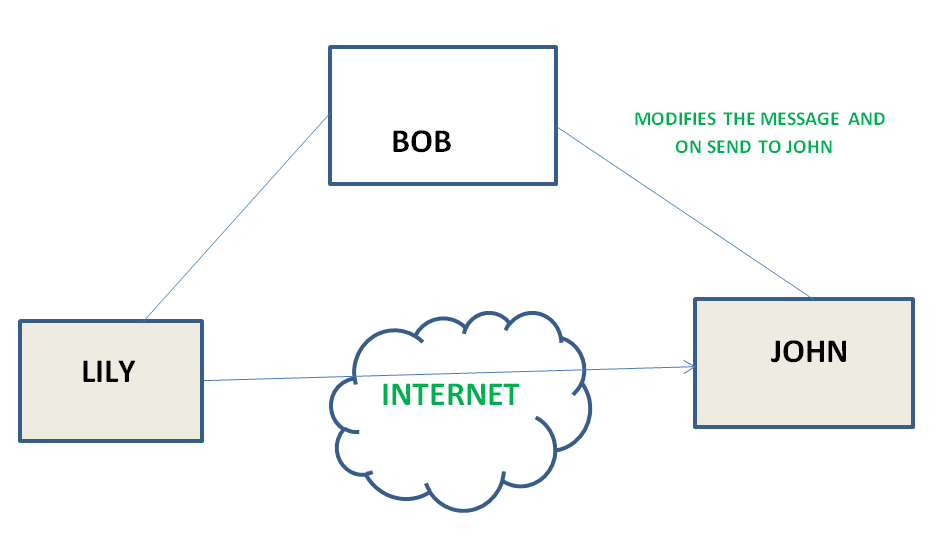
**Security attacks:**

**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 following:

**1.Masquerade –**

Masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks.



**2.Modification of messages –**

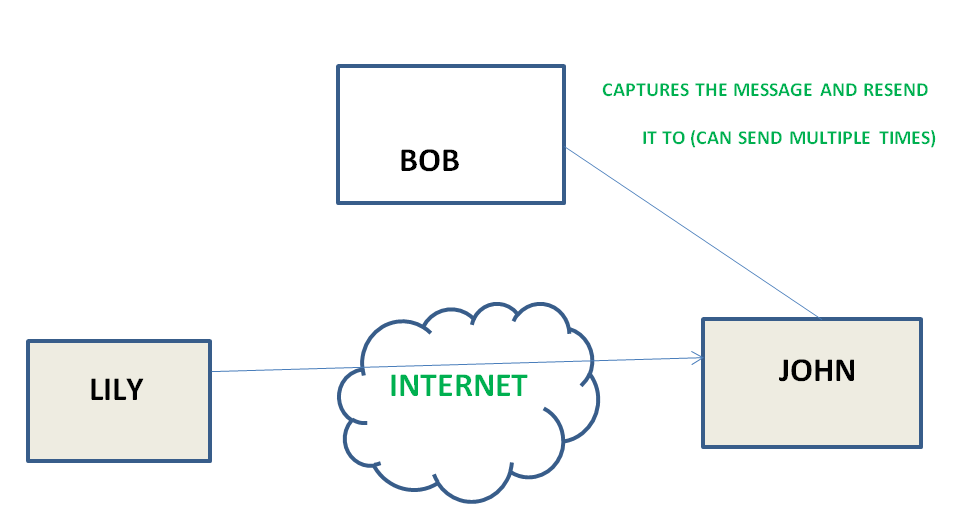
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

**3.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. For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.

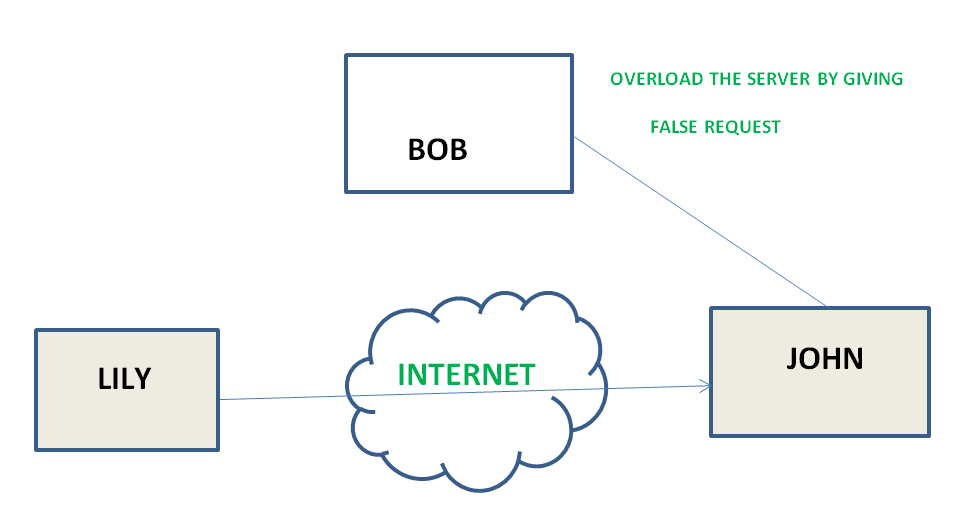
**4.Replay –**

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.



**5.Denial of Service –**

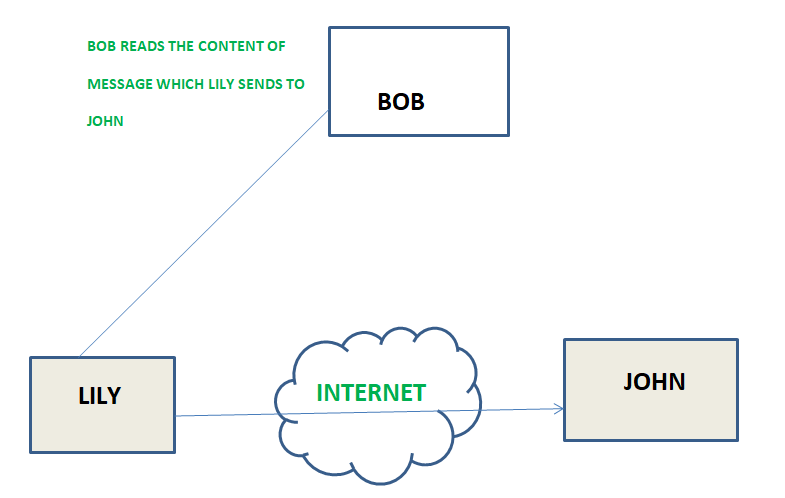
It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.



**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 on or monitoring of transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as following:

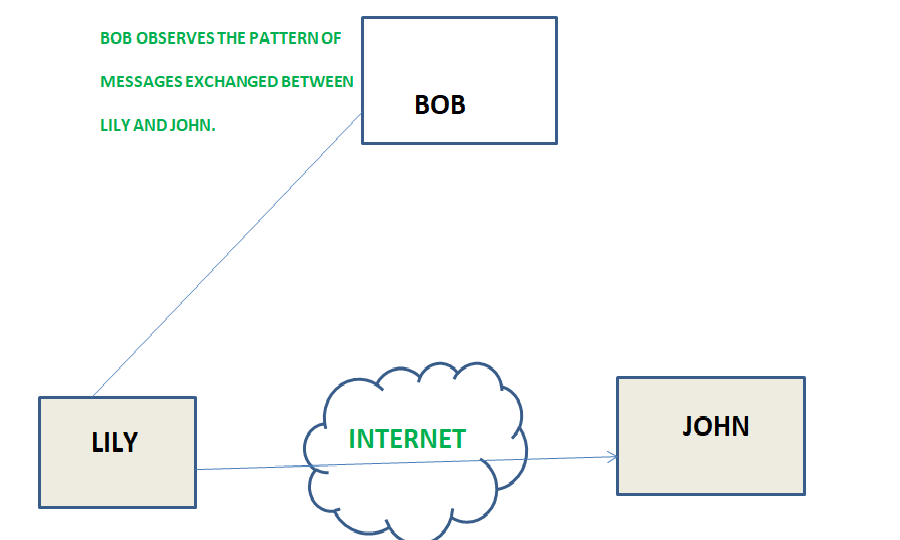
**1.The release of message content –**

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



**Traffic analysis –**

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

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

**Types of Attacks in Cryptography and Network Security**

There are two types of attacks Passive attacks and Active attacks in information security.

**Passive Attacks**

These attacks are not very dangerous as they do not cause any modification to the data. These attacks are generally done to secretly listen and monitor the communication of other parties. Passive attacks are very difficult to detect because these attacks do not change the information of the data.

There are two types of passive attacks in cryptography and network security: Traffic analysis and Release of Message content

**1.Traffic Analysis:** In this attack, an attacker tries to predict the nature of communication by using information. The information such as analyzing traffic, identify communication hosts, and frequency of messages.

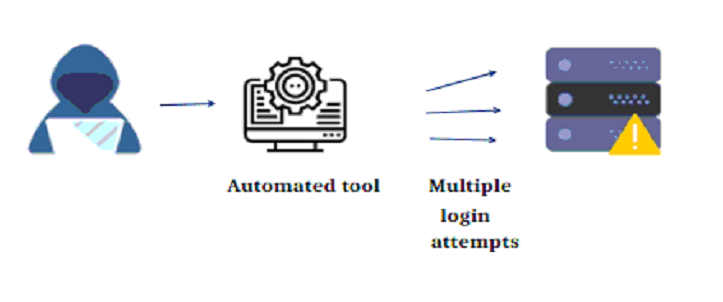
2.**Release of Message content:** It is similar to hearing a telephone conversation between two users. In this attack, the attacker can monitor the content of the transmitted data such as email messages, etc.

**Active Attacks**

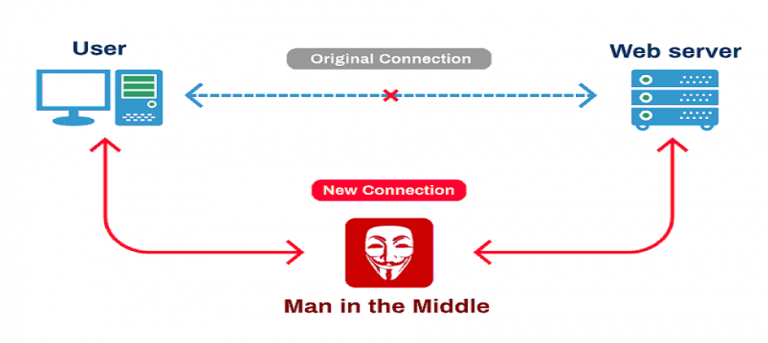
These are some types of attacks in cryptography and network security that can cause modification to the data. These are often difficult to perform but these attacks are very powerful attacks. It is possible to detect these types of attacks.

Several types of active attacks in cryptography and network security:

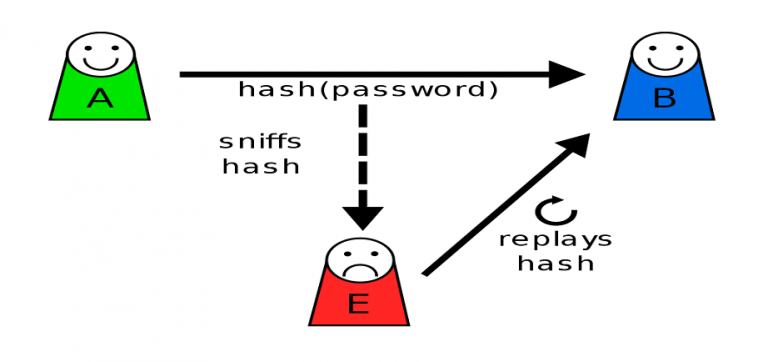
**1.Brute-Force Attack:** A brute-force attack is a very simple attack. An attacker uses a list of passwords and executes such operation in which the system tries every password from the list to login. If it recognizes the right password, the attacker gain access to the victim’s account, and if not then the attacker fails to gain access.



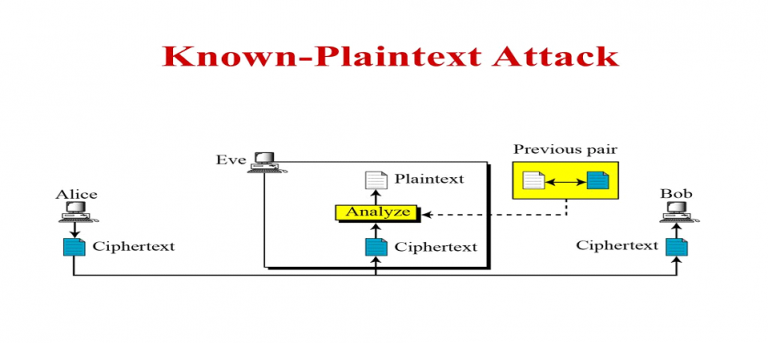
**2.Man-in-the-Middle Attack:** In this, the attacker can see and probably change the communications between two parties who believe that they are communicating with each other. In this attack, the attacker makes an independent connection with the victim and will see or broadcast the messages between them. Further, he can use the revealed information for some illegal activities.



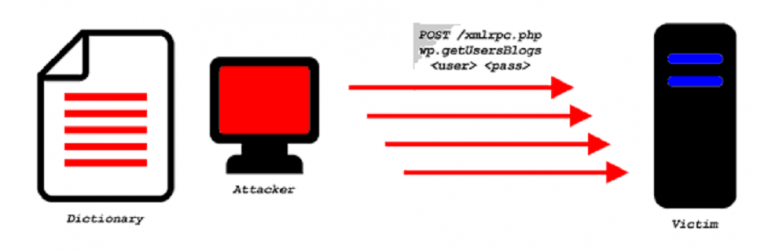
**3.Replay Attack:** A replay attack is one of the types of attacks in cryptography and network security. In this scenario. During this attack, the attacker captures each piece of traffic between two parties and re-transmits it constantly. An attacker can easily fool the participants by replaying the transactions and participants think that they have completed the operation.



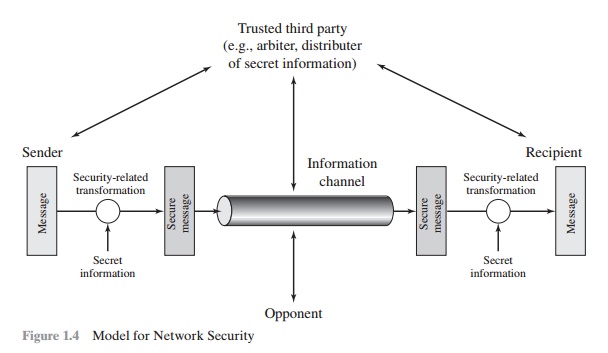
**4.Known Plain Text Attack:** This attack is a standard attack for breaking ciphers and was used throughout the second warfare. In the known-plain text attack, the attacker is aware of the number of plain texts and also the cipher text. Then, the attacker will figure the ‘key’ by reverse engineering and will decipher the alternative messages that use an equivalent ‘key’ and algorithm. The ‘known-plain text’ attack was effective against straightforward ciphers like the ‘substitution cipher’.



**5.Dictionary Attack:** This attack is a very simple attack that involves the compiling of the dictionary. The attacker makes a dictionary of cipher texts and their corresponding plain texts. When the attacker gets the cipher text then with the help of the dictionary, the attacker tries to find the corresponding plain text.



**A MODEL FOR NETWORK SECURITY**



When we send our data from source side to destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established between them by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

When we use the protocol for this logical information channel the main aspect security has come. who may present a threat to confidentiality, authenticity, and so on. All the technique for providing security have to components:

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

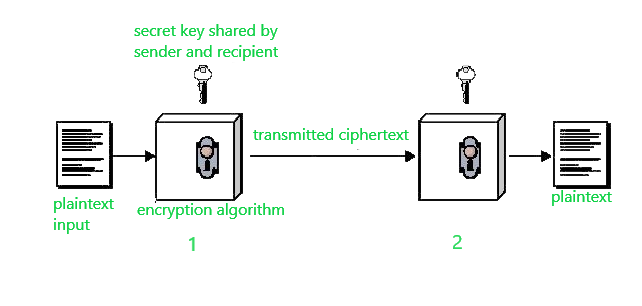
2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

**Conventional encryption**

Conventional encryption is a cryptographic system that uses the same key used by the sender to encrypt the message and by the receiver to decrypt the message. It was the only type of encryption in use prior to the development of public-key encryption.



Suppose A wants to send a message to B, that message is called plaintext. Now, to avoid hackers reading plaintext, the plaintext is encrypted using an algorithm and a secret key (at 1). This encrypted plaintext is called ciphertext. Using the same secret key and encryption algorithm run in reverse(at 2), B can get plaintext of A, and thus the message is read and security is maintained.

The idea that uses in this technique is very old and that’s why this model is called conventional encryption.

Conventional encryption has mainly 5 ingredients :

**Plain text –**

It is the original data that is given to the algorithm as an input.

**Encryption algorithm –**

This encryption algorithm performs various transformations on plain text to convert it into ciphertext.

**Secret key –**

The secret key is also an input to the algorithm. The encryption algorithm will produce different outputs based on the keys used at that time.

**Ciphertext –**

It contains encrypted information because it contains a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it. It is output from the algorithm.

**Decryption algorithm –**

This is used to run encryption algorithms in reverse. Ciphertext and Secret key is input here and it produces plain text as output.

**Substitution techniques**

**Caesar Cipher**

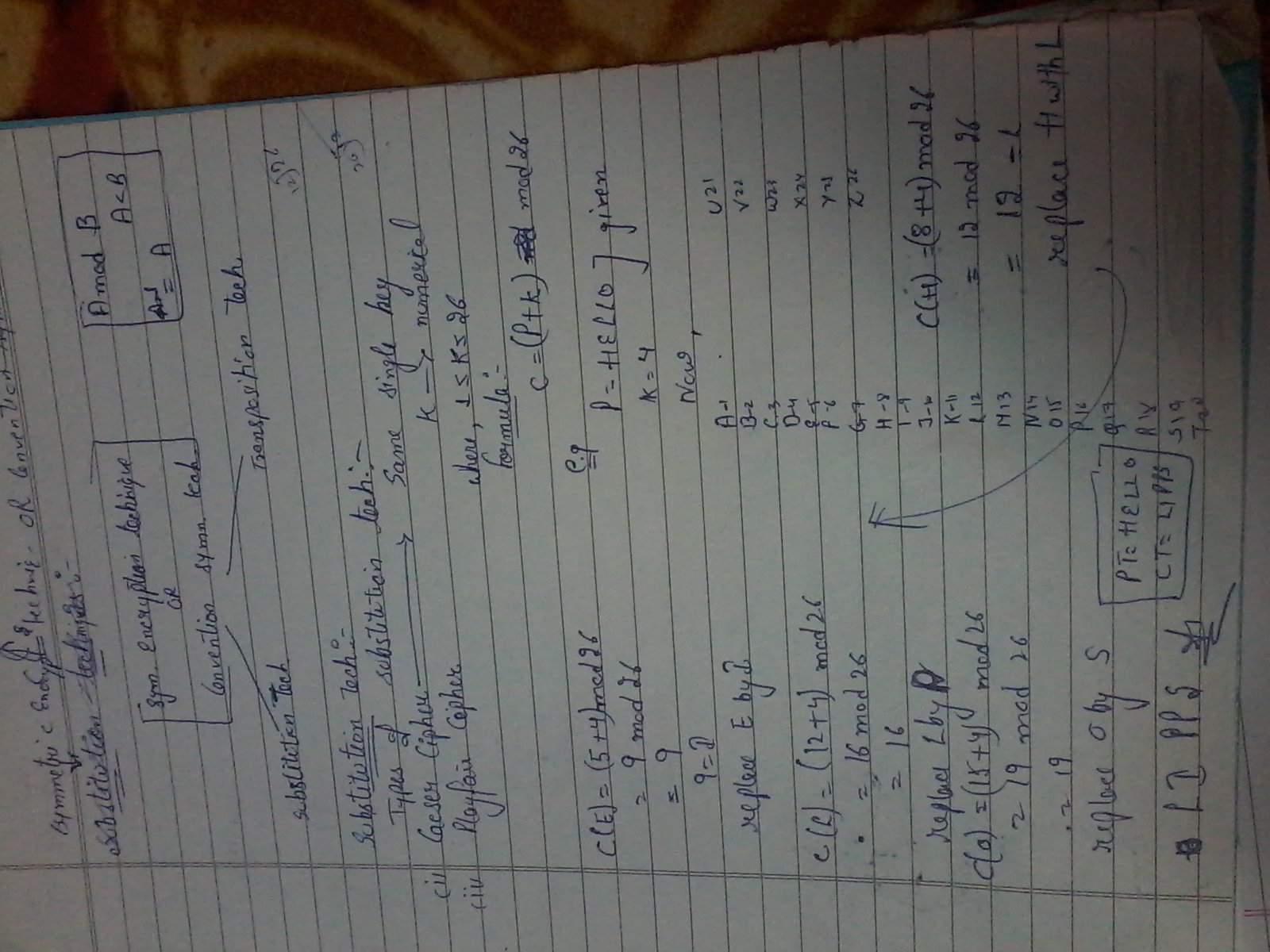
This the simplest substitution cipher by Julius Caesar. In this substitution technique, to encrypt the plain text, each alphabet of the plain text is replaced by the alphabet three places further it. And to decrypt the cipher text each alphabet of cipher text is replaced by the alphabet three places before it.

Let us take a simple example:

Plain Text: meet me tomorrow

Cipher Text: phhw ph wrpruurz

Look at the example above, we have replaced, ‘m’ with ‘p’ which occur three places after, ‘m’. Similarly, ‘e’ is replaced with ‘h’ which occurs in three places after ‘e’.



**Playfair cipher**

In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

The Playfair Cipher Encryption Algorithm:

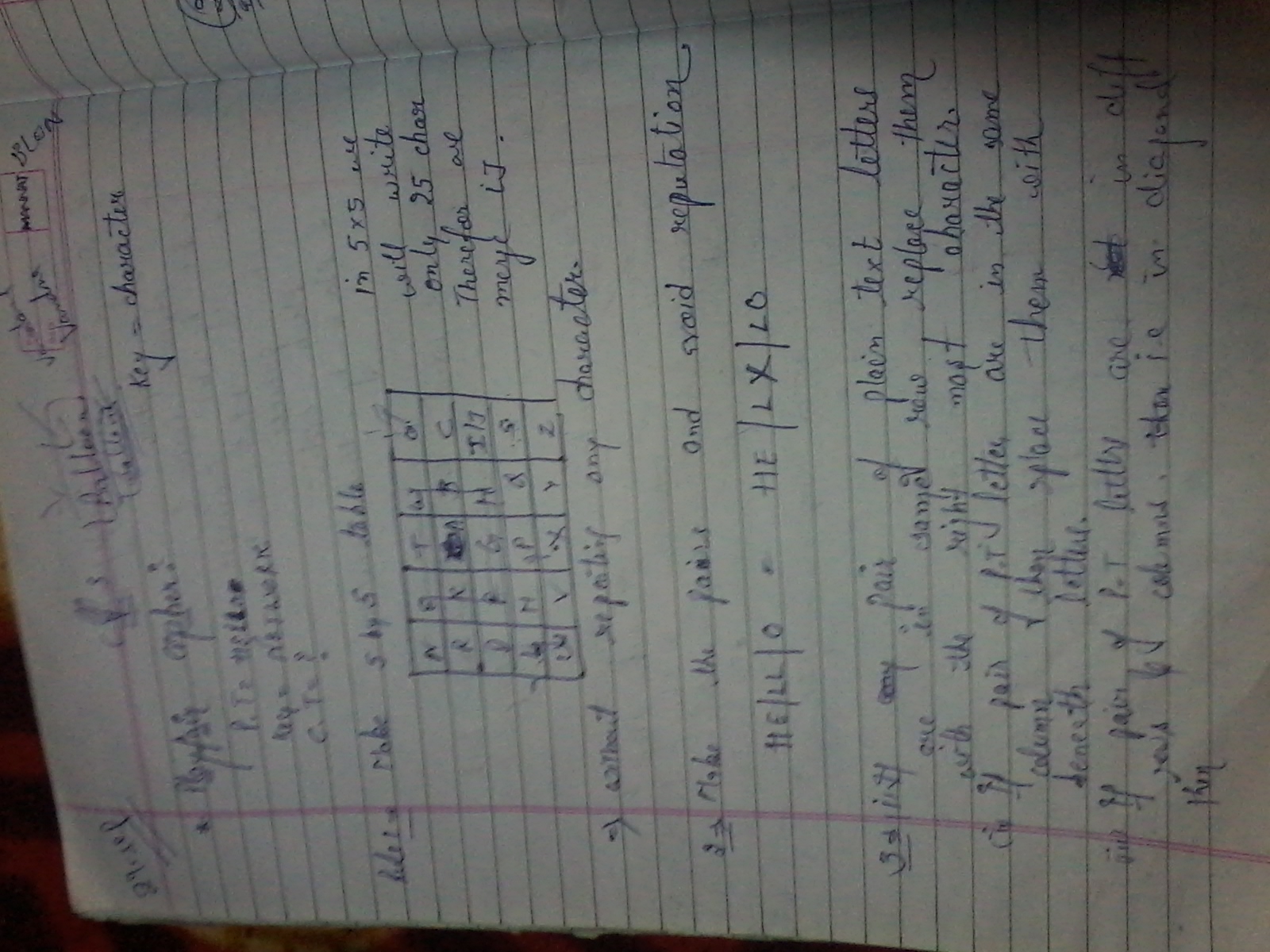
The Algorithm consists of 2 steps:

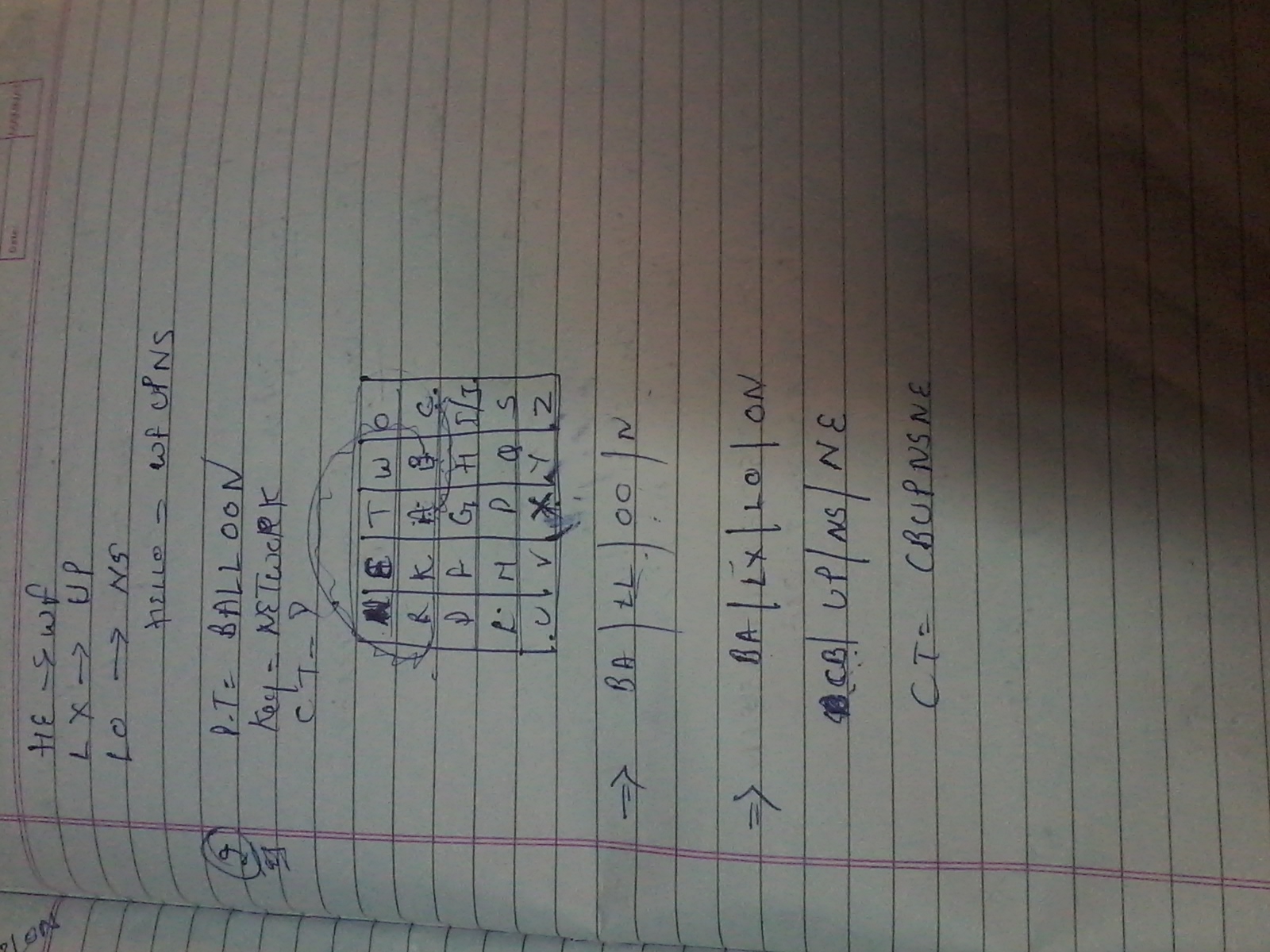
1.Generate the key Square(5×5):

The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2.Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.





**Transposition Techniques**

Transposition Techniques are based on the permutation of the plain-text instead of substitution.

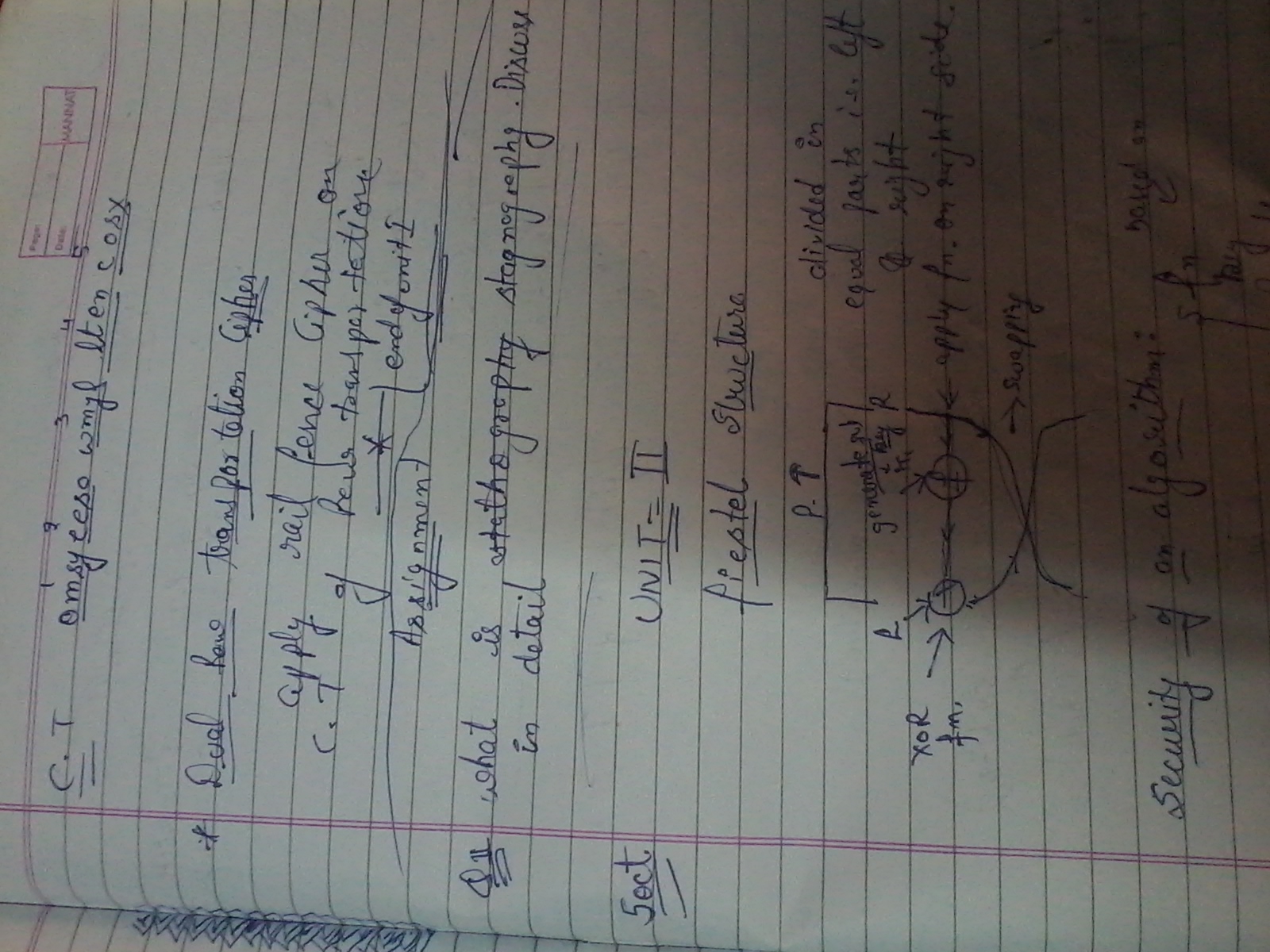
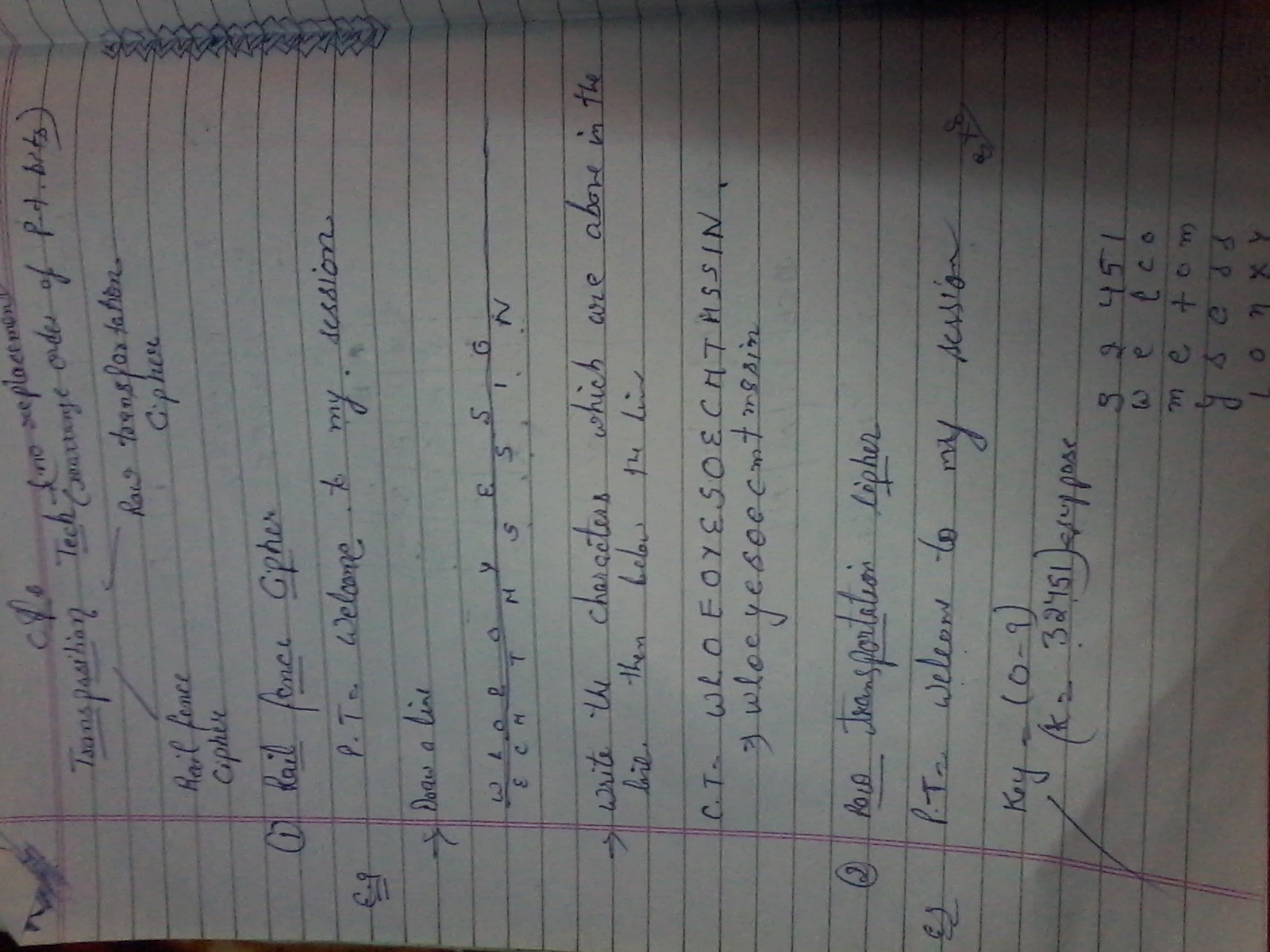
**1) Rail-Fence Technique**

This technique is a type of Transposition technique and does is write the plain text as a sequence of diagonals and changing the order according to each row.

It uses a simple algorithm,

Writing down the plaintext message into a sequence of diagonals.

Row-wise writing the plain-text written from above step.

2.**Row transposition cipherm**

**Simplified Data Encryption Standard Key Generation**

Simplified Data Encryption Standard (S-DES) is a simple version of the DES Algorithm. It is similar to the DES algorithm but is a smaller algorithm and has fewer parameters than DES. It was made for educational purposes so that understanding DES would become simpler. It is a block cipher that takes a block of plain text and converts it into ciphertext. It takes a block of 8 bit.

It is a symmetric key cipher i.e. they use the same key for both encryption and decryption.

**Step 1:** We accepted a 10-bit key and permuted the bits by putting them in the P10 table.

Key = 1 0 1 0 0 0 0 0 1 0

(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (1, 0, 1, 0, 0, 0, 0, 0, 1, 0)

P10 Permutation is: P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, k2, k7, k4, k10, k1, k9, k8, k6)

After P10, we get 1 0 0 0 0 0 1 1 0 0

**Step 2**: We divide the key into 2 halves of 5-bit each.

l=1 0 0 0 0, r=0 1 1 0 0

**Step 3:** Now we apply one bit left-shift on each key.

l = 0 0 0 0 1, r = 1 1 0 0 0

**Step 4:** Combine both keys after step 3 and permute the bits by putting them in the P8 table. The output of the given table is the first key K1.

After LS-1 combined, we get 0 0 0 0 1 1 1 0 0 0

P8 permutation is: P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k7, k4, k8, k5, k10, k9)

After P8, we get Key-1 : 1 0 1 0 0 1 0 0

**Step 5:** The output obtained from step 3 i.e. 2 halves after one bit left shift should again undergo the process of two-bit left shift.

Step 3 output - l = 0 0 0 0 1, r = 1 1 0 0 0

After two bit shift - l = 0 0 1 0 0, r = 0 0 0 1 1

**Step 6:** Combine the 2 halves obtained from step 5 and permute them by putting them in the P8 table. The output of the given table is the second key K2.

After LS-2 combined = 0 0 1 0 0 0 0 0 1 1

P8 permutation is: P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k7, k4, k8, k5, k10, k9)

After P8, we get Key-2 : 0 1 0 0 0 0 1 1

**Final Output:**

Key-1 is: 1 0 1 0 0 1 0 0

Key-2 is: 0 1 0 0 0 0 1 1

**What is Block Cipher**

Block cipher is an encryption method which divides the plain text into blocks of fixed size. Each block has an equal number of bits. At a time, block cipher operates only on one block of plain text and applies key on it to produce the corresponding block of ciphertext.

**Block Cipher Principles**

A block cipher is designed by considering its three critical aspects which are listed as below:

1.Number of Rounds

2.Design of Function F

3.Key Schedule Algorithm

1. Number of Rounds

The number of rounds judges the strength of the block cipher algorithm. It is considered that more is the number of rounds, difficult is for cryptanalysis to break the algorithm.

It is considered that even if the function F is relatively weak, the number of rounds would make the algorithm tough to break.

2. Design of Function F

The function F of the block cipher must be designed such that it must be impossible for any cryptanalysis to unscramble the substitution. The criterion that strengthens the function F is it non-linearity.

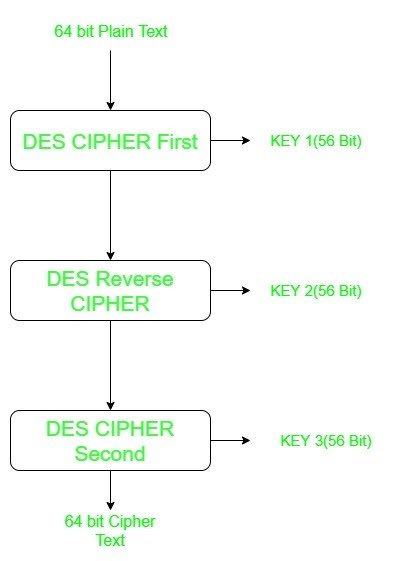
3.Key Schedule Algorithm

It is suggested that the key schedule should confirm the strict avalanche effect and bit independence criterion.

**Triple DES:**

Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

Triple DES is also vulnerable to meet-in-the middle attack because of which it give total security level of 2^112 instead of using 168 bit of key. The block collision attack can also be done because of short block size and using same key to encrypt large size of text. It is also vulnerable to sweet32 attack.



**International Data Encryption Algorithm (IDEA)** is a type of cryptography as a block cipher algorithm designed by "Xuejia Lai" and "James L.Massey" of ETH-Zürich and was first published in the 1991 year. Then, the original algorithm went through a few modifications and finally named as International Data Encryption Algorithm (IDEA) as follows. The mentioned algorithm works on 64-bit plain text and cipher text block at one time in the algorithm. Then, For encryption, the 64-bit plain text is divided into four 16 bits sub-blocks of the algorithm. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits) as the divide of 4 blocks. Here, each of these blocks goes through 8 ROUNDS and one OUTPUT TRANSFORMATION phase at the end of the operation. In each of these eight rounds, some as arithmetic and logical operations are performed by this algorithm. Therefore, the eight ROUNDS are the same sequences of operations are repeated after every round in the cryptography.

Blowfish Algorithm with Examples

Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use.

blockSize: 64-bits

keySize: 32-bits to 448-bits variable size

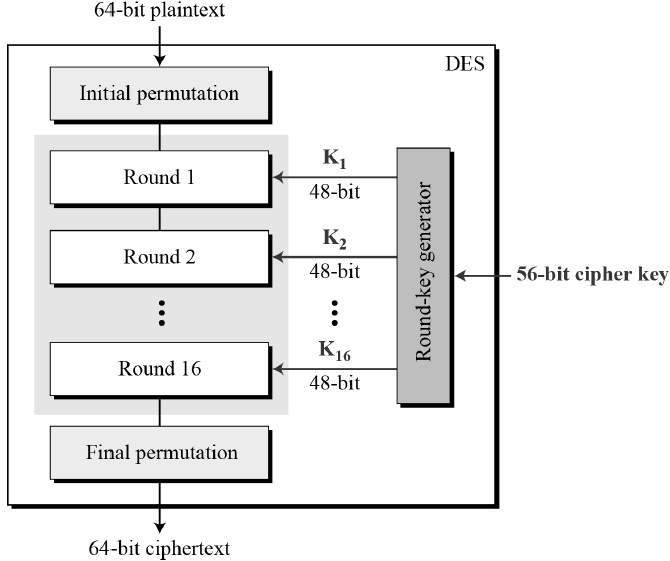
number of subkeys: 18 [P-array]

number of rounds: 16

number of substitution boxes: 4 [each having 512 entries of 32-bits each]

DES

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration



Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES

Round Function

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.