Unit-2 Basics Of Cryptography

Cryptography Introduction:

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel.

So, what happens is as follows:
The sender's message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

```
Alice (Sender)       Bob (Receiver)

C = E (m, k)  ---->    m = D (C, k)
```

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively.

Let’s consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3. For example:

```
Plaintext : Geeksforgeeks

Ciphertext : Jhhnvirujhhnv
```

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

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

2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

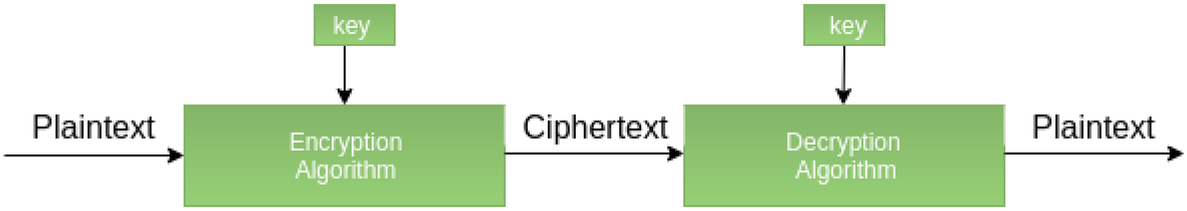
Types Of Cryptography:

In general there are three types of cryptography:

1. **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).

2. **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.

3. **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.



SYMMETRIC KEY CRYTOGRAPHY

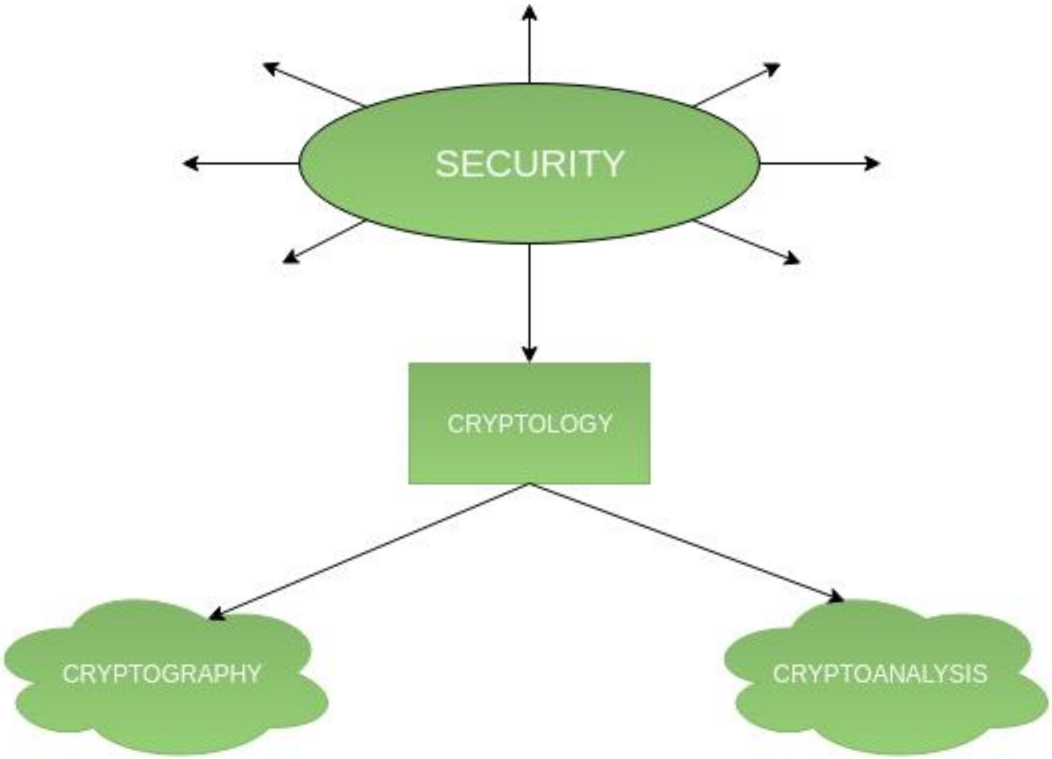
Introduction to Crypto-terminologies

- Symmetric key cryptography – It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message.
- Assymetric key cryptography.
- Hashing.

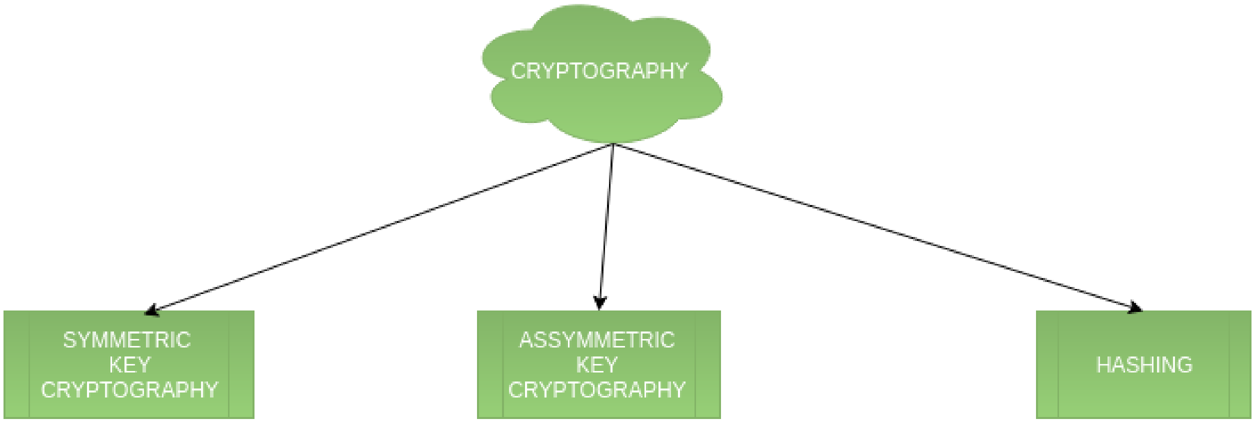
Cryptography is an important aspect when we deal with network security. ‘Crypto’ means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. These both terms are a subset of what is called as Cryptology.

Classification –

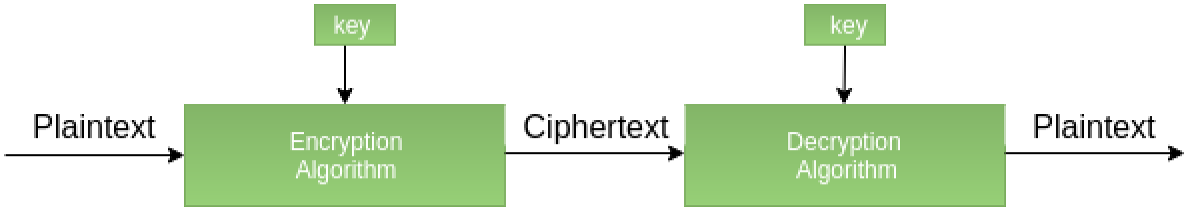
The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto-terminologies and their various types.



- **1. Cryptography –**
  Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing. Below are the description of these types.

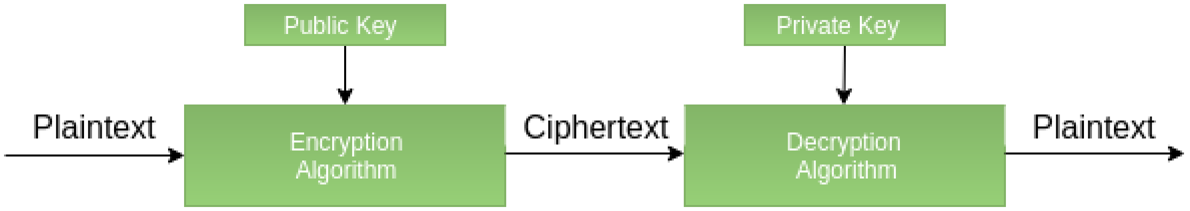
- 

1. **Symmetric key cryptography –**
   It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel.



SYMMETRIC KEY CRYTOGRAPHY

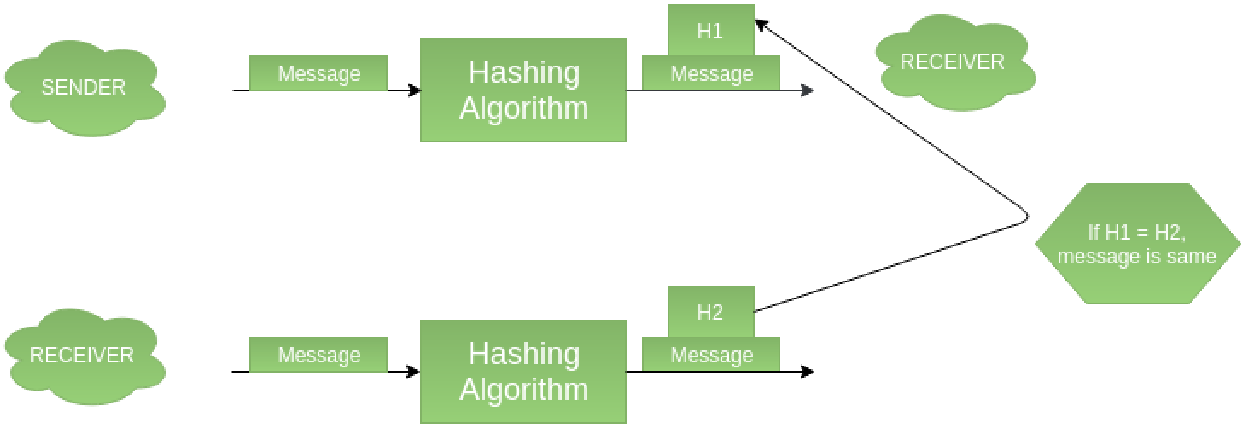
2. **Assymetric key cryptography –**
   It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties uses different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



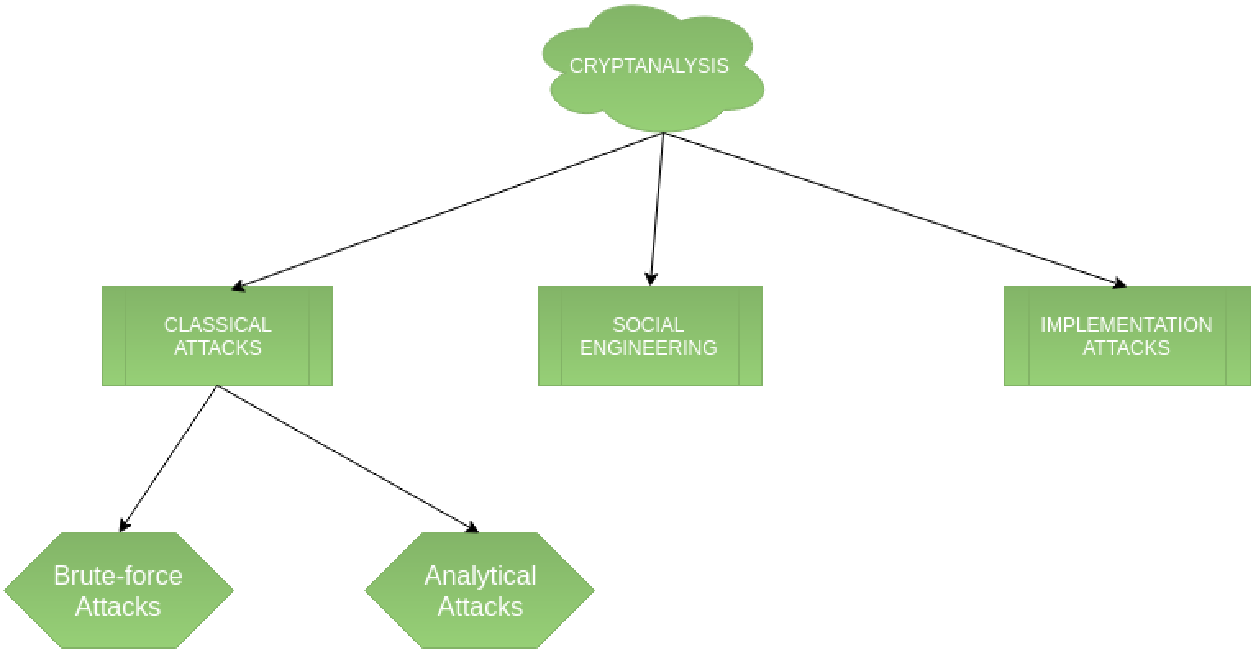
ASYMMETRIC KEY CRYTOGRAPHY

3. **Hashing –**

   It involves taking the plain-text and converting it to a hash value of fixed size by a hash function. This process ensures integrity of the message as the hash value on both, sender\'s and receiver\'s side should match if the message is unaltered.



2. Cryptanalysis –



1. **Classical attacks –**
   It can be divided into a)Mathematical analysis and b) Brute-force attacks. Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.

2. **Social Engineering attack –**
   It is something which is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.

3. **Implementation attacks –**
   Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

Substitution Technique in Cryptography

Substitution technique is a classical encryption technique where the characters present in the **original message** are **replaced** by the **other characters or numbers or by symbols.** If the plain text (original message) is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text.

We will discuss some of the substitution techniques which will help us to understand the procedure of converting plain text o cipher text. In this section, we will study the following substitution techniques:

Substitution Technique:

1. Caesar Cipher
2. Monoalphabetic Cipher
3. Playfair Cipher

4. Hill Cipher
5. Polyalphabetic Cipher
6. One-Time Pad

1. 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’.

Note: If we have to replace the letter ‘z’ then the next three alphabets counted after ‘z’ will be ‘a’ ‘b’ ‘c’. So, while counting further three alphabets if ‘z’ occurs it circularly follows ‘a’.

There are also some drawbacks of this simple substitution technique. If the hacker knows that the Caesar cipher is used then to perform brute force cryptanalysis, he has only to try 25 possible keys to decrypt the plain text. The hacker is also aware of the encryption and decryption algorithm.

2. Monoalphabetic Cipher

Monoalphabetic cipher is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.

In simple words, if the alphabet ‘p’ in the plain text is replaced by the cipher alphabet ‘d’. Then in the entire plain text wherever alphabet ‘p’ is used, it will be replaced by the alphabet ‘d’ to form the ciphertext.

3. Playfair Cipher

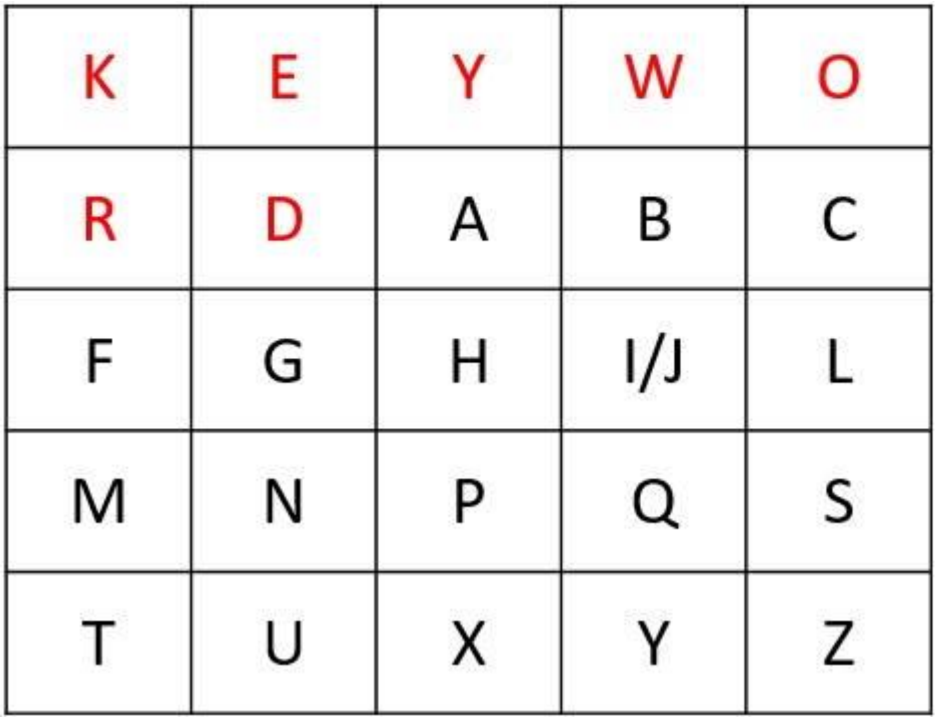
Playfair cipher is a substitution cipher which involves a 5X5 matrix. Let us discuss the technique of this Playfair cipher with the help of an example:

Plain Text: meet me tomorrow

Key: KEYWORD

Now, we have to convert this plain text to ciphertext using the given key. We will discuss the further process in steps.

Step 1: Create a 5X5 matrix and place the key in that matrix row-wise from left to right. Then put the remaining alphabets in the blank space.



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

Note: If a key has duplicate alphabets, then fill those alphabets only once in the matrix, and I & J should be kept together in the matrix even though they occur in the given key.

Step 2: Now, you have to break the plain text into a pair of alphabets.

Plain Text: meet me tomorrow

Pair: me et me to mo rx ro wz

Note

- Pair of alphabets must not contain the same letter. In case, pair has the same letter then break it and add 'x' to the previous letter. Like in our example letter 'rr' occurs in pair so, we have broken that pair and added 'x' to the first 'r'.
- In case while making pair, the last pair has only one alphabet left then we add 'z' to that alphabet to form a pair as in our above example, we have added 'z' to 'w' because 'w' was left alone at last.
- If a pair has 'xx' then we break it and add 'z' to the first 'x', i.e. 'xz' and 'x_'.

Step 3: In this step, we will convert plain text into ciphertext. For that, take the first pair of plain text and check for cipher alphabets for the corresponding in the matrix. To find cipher alphabets follow the rules below.

Note

- If both the alphabets of the pair occur in the **same row** replace them with the alphabet to their **immediate right**. If an alphabet of the pair occurs at extreme right then replace it with the first element of that row, i.e. the last element of the row in the matrix circularly follows the first element of the same row.
- If the alphabets in the pair occur in the **same column**, then replace them with the alphabet **immediate below** them. Here also, the last

element of the column circularly follows the first element of the same column.

- If the alphabets in the pair are **neither in the same column and nor in the same row,** then the alphabet is replaced by the element in its own row and the corresponding column of the other alphabet of the pair.

Pair: me et me to mo rx ro wz

Cipher Text: kn ku kn kz ks ta kc yo

So, this is how we can convert a plain text to ciphertext using Playfair cipher. When compared with monoalphabetic cipher Playfair cipher is much more advanced. But still, it is easy to break.

4. Hill Cipher

Hill cipher is a polyalphabetic cipher introduced by Lester Hill in 1929. Let us discuss the technique of hill cipher.

Plain text: Binary

Key: HILL

Choose the key in such a way that it always forms a **square matrix**. With HILL as the key, we can form a 2×2 matrix.

Now, of plain text, you have to form a column vector of length similar to the key matrix. In our case, the key matrix is 2×2 then the column vectors of plain text would be 2×1.

The general equation to find cipher text using hill cipher is as follow:

$$C = KP \bmod 26$$

$$(c_1\, c_2) = \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} \begin{pmatrix} p_1 \\ p2 \end{pmatrix}\ mod\ 26$$

For our example, our key matrix would be: $\begin{pmatrix} H & I \\ L & L \end{pmatrix}$

And our plain text matrices of 2×1 will be as follow:

$$\begin{pmatrix} B \\ I \end{pmatrix} \begin{pmatrix} N \\ A \end{pmatrix} \begin{pmatrix} R \\ Y \end{pmatrix}$$

Now, we have to convert the key matrix and plain text matrices into numeric matrices. For that number the alphabets such as A=0, B=1, C=2, …………, Z=25. So, considering the alphabet numbering:

Key matrix will be:

$$K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

Plain text matrices would be:

$$\begin{pmatrix} 1 \\ 8 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{pmatrix} 17 \\ 24 \end{pmatrix}$$

In the first calculation, we would get two cipher alphabets for plain text alphabet ‘B’ & ‘I’.

$$(c_1\, c_2) = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 1 \\ 8 \end{pmatrix} \; mod\ 26$$

$$(c_1\, c_2) = \begin{pmatrix} 71 \\ 99 \end{pmatrix} mod\ 26$$

$$(c_1\, c_2) = \begin{pmatrix} 71 \\ 99 \end{pmatrix} mod\ 26$$

$$(c_1\, c_2) = \begin{pmatrix} 19 \\ 21 \end{pmatrix}$$

$$(c_1\, c_2) = \begin{pmatrix} T \\ V \end{pmatrix}$$

So, the cipher alphabet for plain text alphabet ‘B’ & ‘I’ is ‘T’ & ‘V’. Similarly, we have to calculate ciphertext for remaining plain text. And then accumulate them to form the ciphertext.

The calculated **ciphertext** for ‘**Binary**’ using hill cipher is ‘**TVNNZJ**’.

5. Polyalphabetic Cipher

Polyalphabetic cipher is far more secure than a monoalphabetic cipher. As monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message.
But polyalphabetic cipher, each time replaces the plain text with the different ciphertext.

6. One-Time Pad

The one-time pad cipher suggests that the **key length** should be **as long as the plain text** to prevent the repetition of key. Along with that, the **key** should be **used** only **once** to encrypt and decrypt the single message after that the key should be discarded.

Onetime pad suggests a new key for each new message and of the same length as a new message. Now, let us see the one-time pad technique to convert plain text into ciphertext. Assume our plain text and key be:

Plain text: Binary

Key: Cipher

Now again convert the plain text and key into the numeric form. For that number the alphabets such as A=0, B=1, C=2, …………, Z=25. So, our plain text and key in numeric form would be:

Plain text: 1 8 13 0 17 24

Key: 2 8 15 7 4 17

Now, you have to add the number of the plain text alphabet, to the number of its corresponding key alphabet. That means, for this example, we will add:

B+C = 1+2 = 2

I+I = 8+8 = 16

N+P = 13+15 = 28

A+H = 0+7 = 7

R+E = 17+4 = 21

Y+R = 24+17 = 41

The resultant ciphertext numbers we get are (2, 16, 28, 7, 21, 41)

If the addition of any plain text number and the key number is >26, then subtract only that particular number from 26. We have the addition of two pair of plain text number and a key number, greater than 26, i.e. N+P=28 & Y+R=41.

Subtract them by 26.

N+P = 28 – 26 = 2

Y+R = 41 – 26 = 15

So, the final **ciphertext numbers are (2, 16, 2, 7, 21, 1)**. Now convert this number to alphabets assuming A to be numbered 0 and B to be 1…..Z to 25.

Ciphertext: Cqchvb.

What is transposition technique in cryptography?

The transposition technique is a **cryptographic technique that converts the plain text to cipher text by performing permutations on the plain text**, i.e., changing each character of plain text for each round.

Transposition Techniques :

The transposition technique is a cryptographic technique that converts the plain text to cipher text by performing permutations on the plain text, i.e., changing each character of plain text for each round. It includes various techniques like the Rail Fence technique, Simple columnar transposition technique, simple columnar transposition technique with multiple rounds, Vernam cipher, and book Cipher to encrypt the plain text in a secure way.

Below is the list of transposition techniques.

1. Rail-Fence Technique

Rail-Fence is the simple Transposition technique that involves writing plain text as a sequence of diagonals and then reading it row by row to produce the ciphertext.

Algorithm

Step 1: Write down all the characters of plain text message in a sequence of diagnosis.

Step 2: Read the plain text written in step 1 as a sequence of rows.

To understand it in a better manner, let’s take an example.

Example: Suppose plain text corporate bridge, and we want to create the ciphertext of the given.

First, we arrange the plain text in a sequence of diagnosis, as shown below.

Now read the plain text by row-wise, i.e. croaerdeoprtbig.

So, here the plain text is a corporate bridge, and ciphertext is croaerdeoprtbig. The Rail-Fence technique is quite easy to break.

2. Simple columnar transposition techniques

The simple columnar transposition technique can be categorized into two parts – Basic technique and multiple rounds.

Simples columnar transposition technique – basic technique. The simple columnar transposition technique simply arranges the plain text in a sequence of rows of a rectangle and reads it in a columnar manner.

How does this algorithm work?

Step 1: Write all the characters of plain text message row by row in a rectangle of predefined size.

Step 2: Read the message in a columnar manner, i.e. column by column.

Note: For reading the message, it needs not to be in the order of columns. It can happen in any random sequence.

Step 3: The resultant message is ciphertext.

Example: Let's assume that Plain text is a corporate bridge, and we need to calculate the cipher text using a simple columnar transposition technique.

Let's take 6 columns and arrange the plain text in a row-wise manner.

Column 1	**Column 2**	**Column 3**	**Column 4**	**Column 5**
C	o	r	P	o
A	t	e	B	r
D	g	e		

Decide the column order for reading the message – let's assume 1,3,5,2,4,6 is an order.

Now read the message in a columnar manner using the decided order. – cadreeorotgpbri

cadreeorotgpbri is a ciphertext.

3. Simple columnar transposition technique – Multiple rounds

Simple columnar transposition technique with multiple rounds is the same as basic; only the difference is that we iterate the process multiple times in multiple rounds.

Working of an algorithm

Step 1: Write all the characters of plain text message row by row in a rectangle of predefined size.

Step 2: Read the message in a columnar manner, i.e. column by column.

Note: For reading the message, it needs not to be in the order of columns. It can happen in any random sequence.

Step 3: The resultant message is ciphertext.

Step 4: Repeat the procedure from step 1 to step 3 many times as desired.

Example: Let's assume that Plain text is a corporate bridge, and we need to calculate the cipher text using a simple columnar transposition technique.

Let's take 6 columns and arrange the plain text in a row-wise manner.

Column 1	Column 2	Column 3	Column 4	Column 5

C	o	r	p	o
A	t	e	b	r
D	g	e		

Decide the column order for reading the message – let’s assume 1,3,5,2,4,6 is an order.

Now read the message in a columnar manner using the decided order. – cadreeorotgpbri

cadreeorotgpbri is a ciphertext.

Let’s perform step 1 to step 3 one more time.

Column 1	**Column 2**	**Column 3**	**Column 4**	**Column 5**
C	a	d	r	e
O	r	o	t	g
B	r	i		

In the second iteration, the order of the columns will be the same.

Ciphertext – cobdoiegarrrtep

Continue the same procedure if more iteration is required.

4. Vernam Cipher

A subset of Vernam cipher is called a one-time pad because it is implemented using a random set of nonrepeating characters as an input ciphertext.

Note: Once the input ciphertext is used for transposition, it never used for any other message. The length of input ciphertext must be equal to the length of plain text.

Working of Algorithm

Step 1: Arrange all characters in the plain text as a number i.e. A = 0, B = 1, ….. Z = 25.

Step 2: Repeat the same procedure for all characters of the input ciphertext.

Step 3: Add each number corresponding to the plain text characters to the corresponding input ciphertext character number.

Step 4: If the sum of the number is greater than 25, subtract 26 from it.

Step 5: Translate each number of the sum into the corresponding characters.

Step 6: The output of step 5 will be a ciphertext.

In Vernam cipher, once the input ciphertext is used, it will never be used for any other message; hence it is suitable only for short messages.

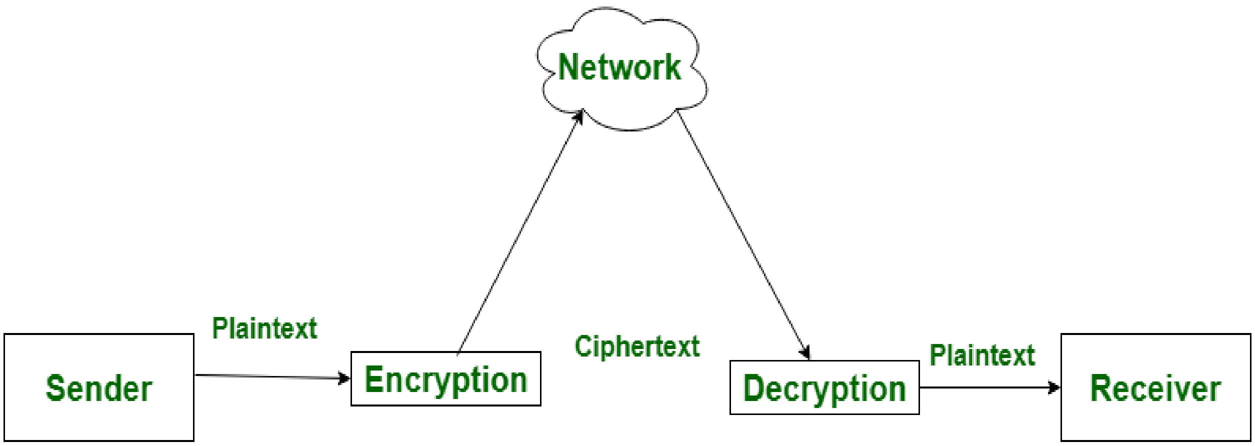
Example: The plain text is educba and ciphertext is ntcbar

Plain text	E	d	u	c	b
	4	3	20	2	1
Input ciphertext	N	t	c	b	a
	13	19	2	1	0
Addition of plain text and input ciphertext	17	22	22	3	1
Ciphertext	R	w	w	d	b

Hence, the ciphertext is rwwdbr.

Difference between Encryption and Decryption:

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that secret writing is that the conversion of a message into an unintelligible kind that’s undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.



Let’s see that the difference between encryption and decryption:

S.NO	Encryption	Decryption
1.	Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
2.	Encryption is the process which take place at sender’s end.	While decryption is the process which take place at receiver’s end.
3.	Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
4.	Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
5.	In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information(Cipher text) and convert into plain text.

Characteristics or properties of good 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.
- Non-repudiation.
- Authentication.

Types Of Encryption Systems:

What Are the Different Types of Encryption?

Cybersecurity and protected data are becoming more important every day. As we take more of our banking, health, and business data online, keeping them secure can be difficult. That’s why most programs and apps we use rely on some form of data encryption to keep our information safe.

What are the different types of encryption? While the most common are AES, RSA, and DES, there are other types being used as well. Let’s dive into what these acronyms mean, what encryption is, and how to keep your online data safe.

What is data encryption?

Data encryption is what happens when you take the text or data you use and convert it to a code (also called “ciphertext”) that can’t be understood by those who do not have the correct key. For the data to be useable, it must be changed back or decrypted.

Encryption is necessary because it allows us to send relevant and often-sensitive information over the internet and through electronic means without unauthorized people seeing it. For the data to be decrypted, it needs a key, which authorized users will have. However, keep in mind that even encrypted data can sometimes be decrypted by those with enough skills or resources, some of whom may have malicious intent.

Encryption generally prevents the theft or sharing of important data, whether it’s the movies we watch, which use digital rights management (DRM) to prevent illegal copying, or the banking login passwords we type into the bank’s website.

Why encryption type matters

Encryption methods vary by how much data they can handle at once and what kind of key it needs for its decryption. Some encryption is more easily hacked than others. While some companies or individuals choose encryption type according to standards dictated by legal or industrial regulations, others may simply choose their type based on personal preference. It matters to you because it's your data that's being protected. You will want the best encryption type for the data you are storing or transmitting.

The various encryption types

The three major encryption types are DES, AES, and RSA. While there are many kinds of encryption - more than can easily be explained here - we will take a look at these three significant types of encryption that consumers use every day. Most of the others are variations on older types, and some are no longer supported or recommended. Tech is evolving every day and even those considered to be modern will be replaced by newer versions at some point.

DES encryption

Accepted as a standard of encryption in the 1970s, DES encryption is no longer considered to be safe on its own. It encrypts just 56-bits of data at a time and it was found to be easily hacked not long after its introduction. It has, however, served as the standard upon which future, more-secure encryption tools were based.

3DES

A more modern 3DES is a version of block cipher used today. Triple Data Encryption Standard (3DES) works as its name implies. Instead of using a single 56-bit key, it uses three separate 56-bit keys for triple protection.

The drawback to 3DES is that it takes longer to encrypt data. Also, the shorter block lengths are encrypted three times, but they can still be hacked. Banks and businesses still rely on it at this point in time, but newer forms may soon phase out this version.

When should use you use DES encryption?

You probably won't use DES or even 3DES on your own today. Banking institutions and other businesses may use 3DES internally or for their private transmissions. The industry standard has moved away from it, however, and it's no longer being incorporated into the newest tech products.

AES encryption

One of the most secure encryption types, Advanced Encryption Standard (AES) is used by governments and security organizations as well as everyday businesses for classified communications. AES uses "symmetric" key encryption. Someone on the receiving end of the data will need a key to decode it.

AES differs from other encryption types in that it encrypts data in a single block, instead of as individual bits of data. The block sizes determine the name for each kind of AES encrypted data:

- AES-128 encrypts blocks of a 128-bit size
- AES-192 encrypts blocks of a 192-bit size
- AES-256 encrypts blocks of a 256-bit size

In addition to having different block sizes, each encryption method has a different number of rounds. These rounds are the processes of changing a plaintext piece of data into encrypted data or ciphered text. AES-128, for example, uses 10 rounds, and AES-256 uses 14 rounds.

When should you use AES encryption?

Most of the data tools available on the market today use AES encryption. Even those that allow you to use other methods with their programs recommend the AES standard. It works in so many applications, and it’s still the most widely-accepted and secure encryption method for the price. In fact, you’re probably using it without even knowing it.

RSA Encryption

Another popular encryption standard is “Rivest-Shamir-Adleman” or RSA. It is widely used for data sent online and relies on a public key to encrypt the data. Those on the receiving end of the data will have their own private key to decode the messages. It’s proven to be a secure way to send information between people who may not know each other and want to communicate without compromising their personal or sensitive data.

When should you use RSA encryption?

You’ll need to know a little bit about using RSA to make it part of your routine, but once established, it has many uses. Some people use it to verify a digital signature and ensure the person they are communicating with is really who they say they are. It takes a long time to encrypt data this way, however, and isn’t practical for large or numerous files.

Difference between Confusion and Diffusion

Confusion and **diffusion** area unit the properties for creating a secure cipher. Each Confusion and diffusion area unit wont to stop the secret writing key from its deduction or ultimately for preventing the first message. Confusion is employed for making uninformed cipher text whereas diffusion is employed for increasing the redundancy of the plain text over the foremost a part of the cipher text to create it obscure. The stream cipher solely depends on confusion, or else, diffusion is employed by each stream and block cipher.

```
Confusion = Substitution
a --> b
Caesar Cipher


Diffusion = Transposition or Permutation
abcd --> dacb
          DES
```

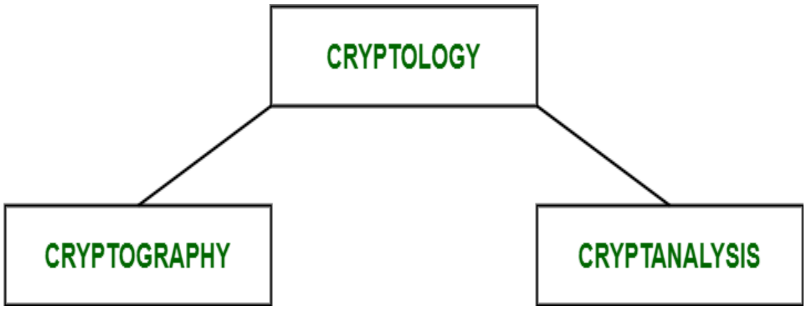
Let’s see the difference b/w Confusion and Diffusion:

S.NO	Confusion	Diffusion
1.	Confusion is a cryptographic technique which is used to create faint cipher texts.	While diffusion is used to create cryptic plain texts.
2.	This technique is possible through substitution algorithm.	While it is possible through transportation algorithm.
3.	In confusion, if one bit within the secret’s modified, most or all bits within the cipher text al so will be modified.	While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified
4.	In confusion, vagueness is increased in resultant.	While in diffusion, redundancy is increased in resultant.

5.	Both stream cipher and block cipher uses confusion.	Only block cipher uses diffusion.
6.	The relation between the cipher text and the key is masked by confusion.	While The relation between the cipher text and the plain text is masked by diffusion.

Cryptanalysis and Types of Attacks:

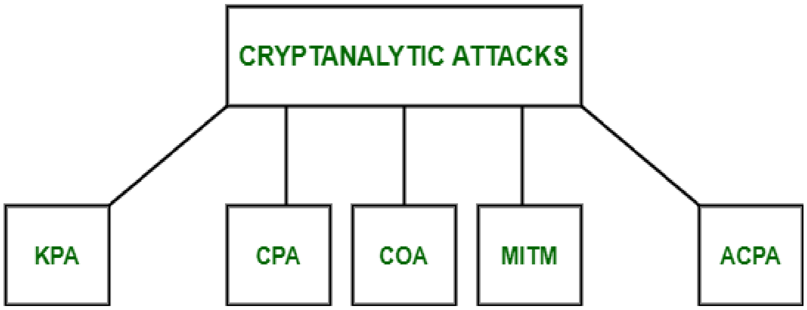
Cryptology has two parts namely, **Cryptography** which focuses on creating secret codes and **Cryptanalysis** which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a **Cryptanalyst**. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For example, a Cryptanalyst might try to decipher a ciphertext to derive the plaintext. It can help us to deduce the plaintext or the encryption key.



Parts Of Cryptology

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called **Cryptanalytic attacks.** The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.

Types of Cryptanalytic attacks :



The Five Types of Cryptanalytic Attacks

- **Known-Plaintext Analysis (KPA) :**
  In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

- **Chosen-Plaintext Analysis (CPA) :**
  In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. Its very simple to implement like KPA but the success rate is quite low.

- **Ciphertext-Only Analysis (COA) :**
  In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required.

- **Man-In-The-Middle (MITM) attack :**
  In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel.

- **Adaptive Chosen-Plaintext Analysis (ACPA) :**
  This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.