CRYPTUS CYBER
SECURITY PVT. LTD.

What is cryptography?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email

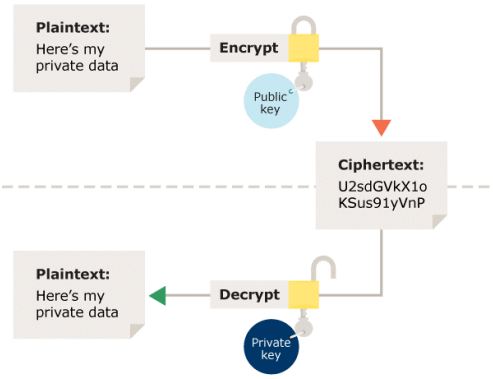
Techniques used For Cryptography: -

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.

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).



(Image Of Encryption and Decryption)

.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.

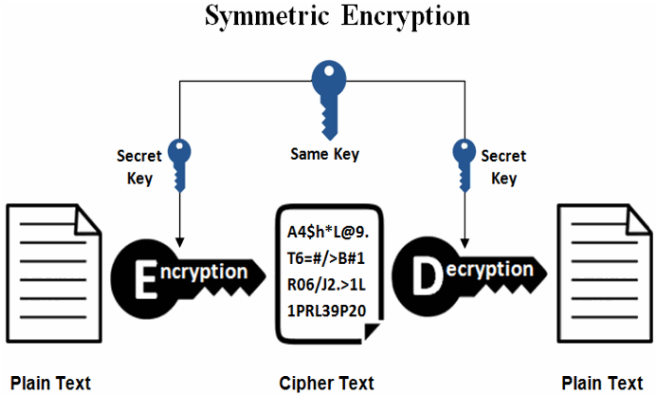
Basic Terms:-

1.Plain Text :- Is an unencrypted Message

2.Cipher Text :- Is an Encrypted Message

3.Key :- In cryptography, a key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

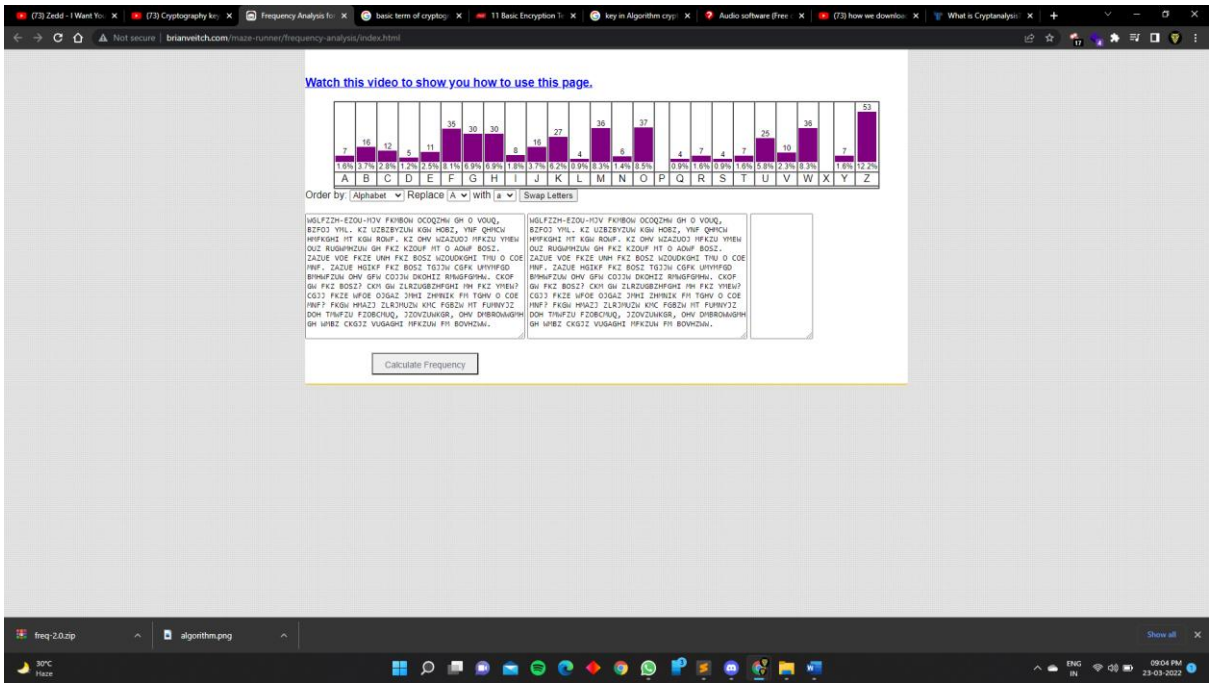
4.Algorithm:- set of mathematical and logical rules use in cryptography Function



Cryptanalysis:-

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

Tool link http://www.brianveitch.com/maze-runner/frequency-analysis/index.html (frequency analysis tool)



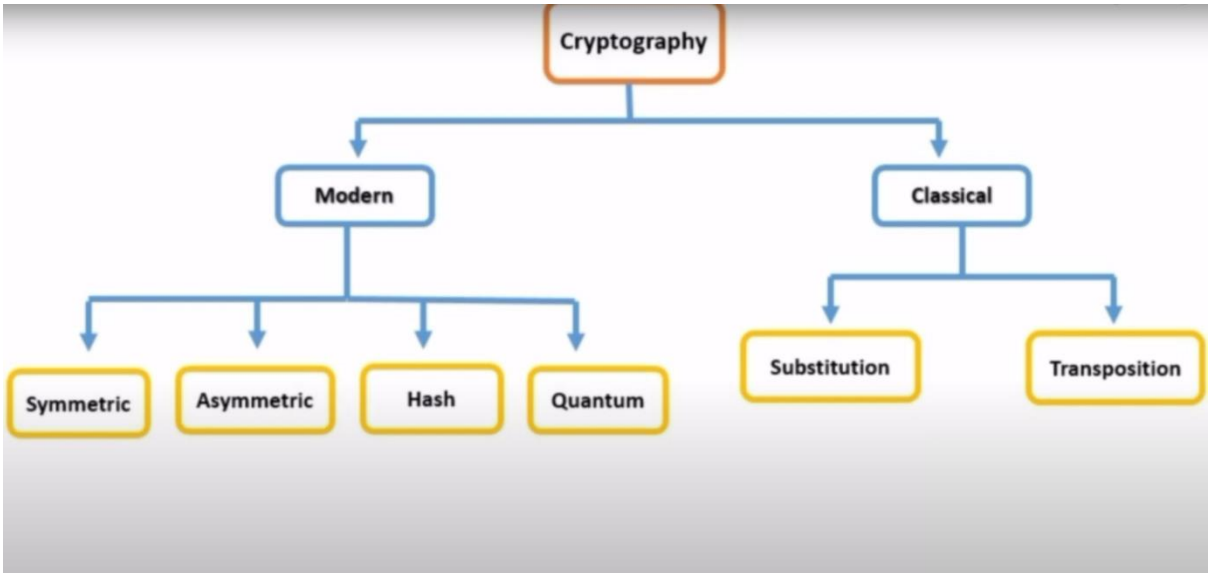
What is cryptology:-

Cryptography, or **cryptology** (from Ancient Greek: κρυπτός, romanized: *kryptós* "hidden, secret";

and γράφειν *graphein*, "to write", or -λογία *-logia*, "study", respectively[1]), is the practice and study of techniques for secure communication in the presence of adversarial behavior.

"The study of both cryptography and cryptanalysis is known as cryptology."

Type Of Cryptography:-



Classical Cryptography:-

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.

Substitution Technique:

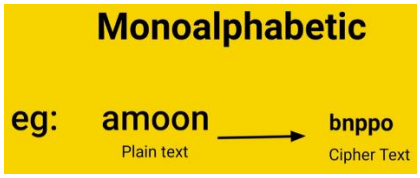
1. Caesar Cipher
2. Monoalphabetic Cipher
3. Playfair Cipher
4. Hill Cipher
5. Polyalphabetic Cipher
6. One-Time Pad

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.

Example :-

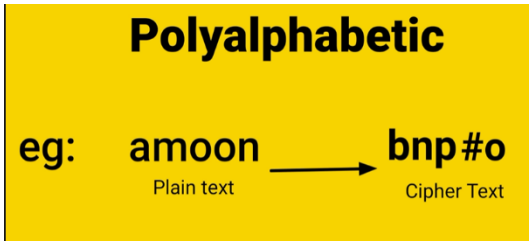


"A monoalphabetic cipher is any cipher in which the letters of the plain

Polyalphabetic Cipher :-

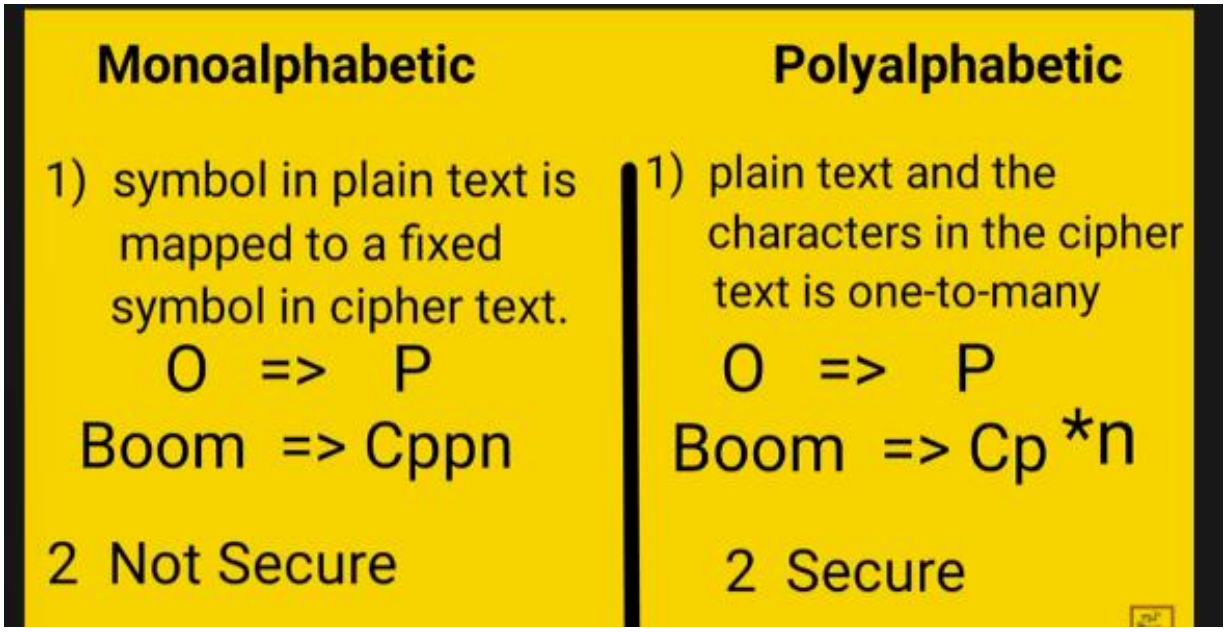
Polyalphabetic cipher is far more secure than a monoalphabetic cipher. As monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message.
But polyalphabetic cipher, each time replaces the plain text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

Example:-



“Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. … each alphabetic character of plain text is mapped on to a unique alphabetic character of a unique alphabetic character of a cipher text.”

Difference Between Polyalphabetic and Monoalphabetic:-



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

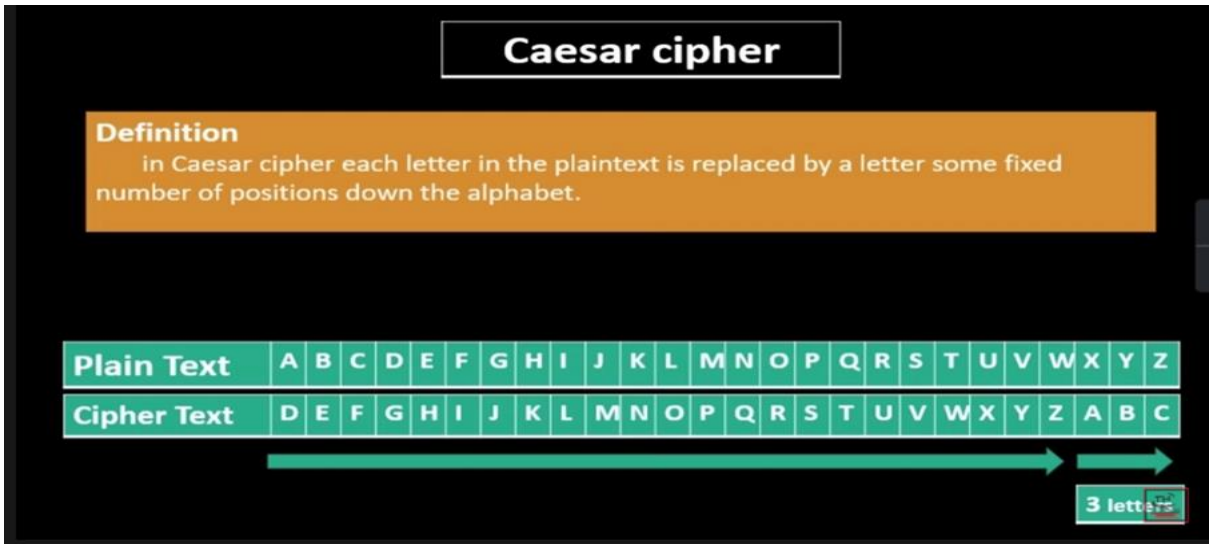
Cipher Text: phhw ph wrpruurz

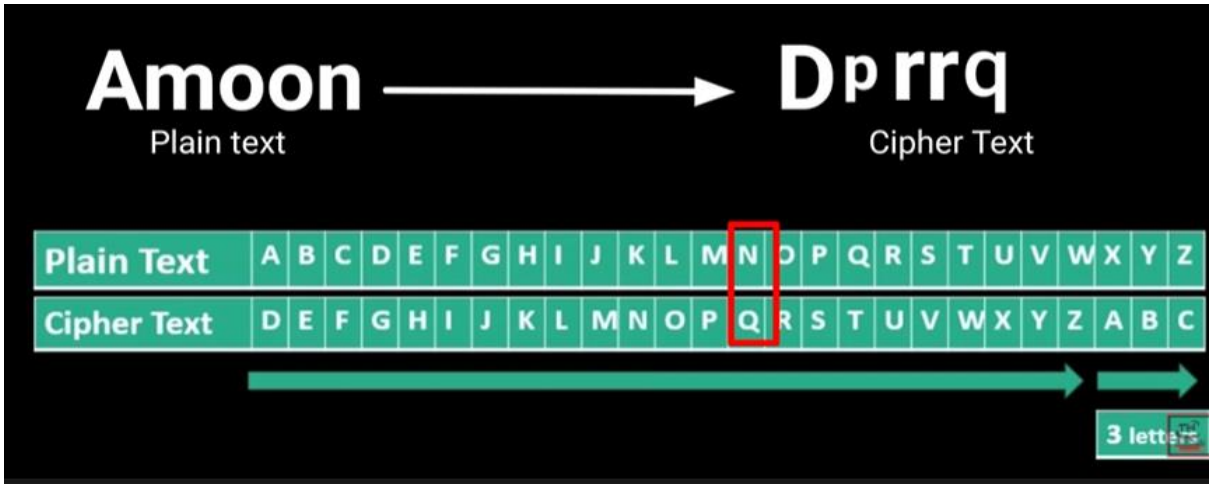
Look at the example above, we have replaced, ‘m’ with ‘p’ which occur three places after, ‘m’. Similarly, ‘e’ is replaced with ‘h’ which occurs in three places after ‘e’.

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.

Example:-





Encryption

C=E(3,P) (P+3)mod26

Decryption

C=D(3,P) (P-3)mod 26

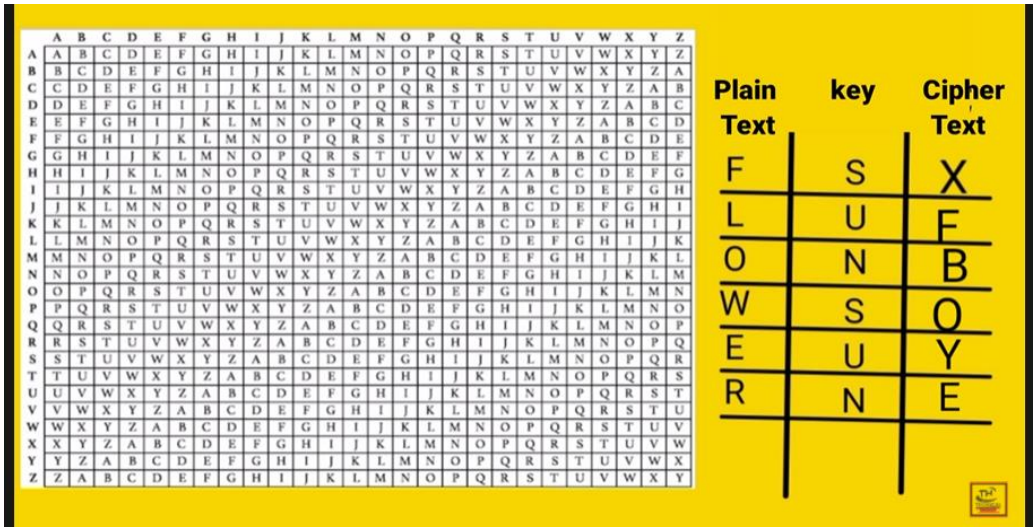
Vigenere Cipher

It is type of Polyalphabetic Cipher

It is Classical Cryptography

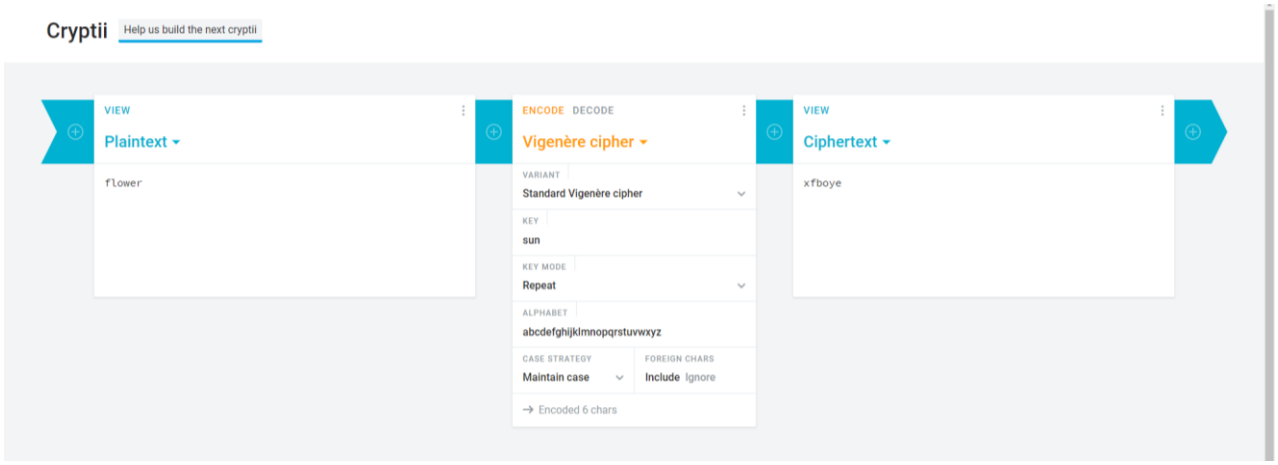
The encryption of the original text is done using the Vigenere Sequence or Vigenere table

Example:-



Vigenere Table

Website :- https://cryptii.com/pipes/vigenere-cipher



Decrypt the message with the help of website:-

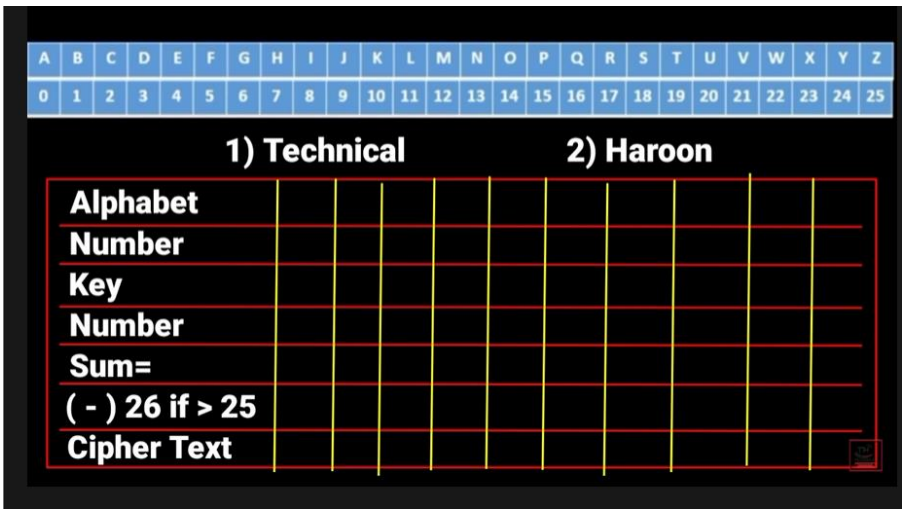
One time pad (OTP)

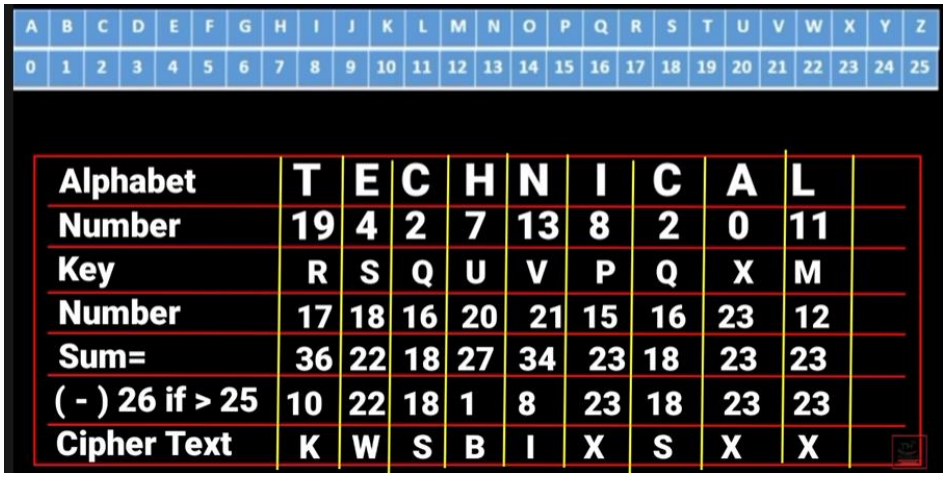
1. Difficult to crack encryption
2. Sender always use the new key for encryption

3. Plain text and key size will be same
4. Key will be use use only one time. Next time key will be change
5. It is use in polyalphabetic cipher and its substitution cipher cryptography technique
6. It is also called vernam cipher

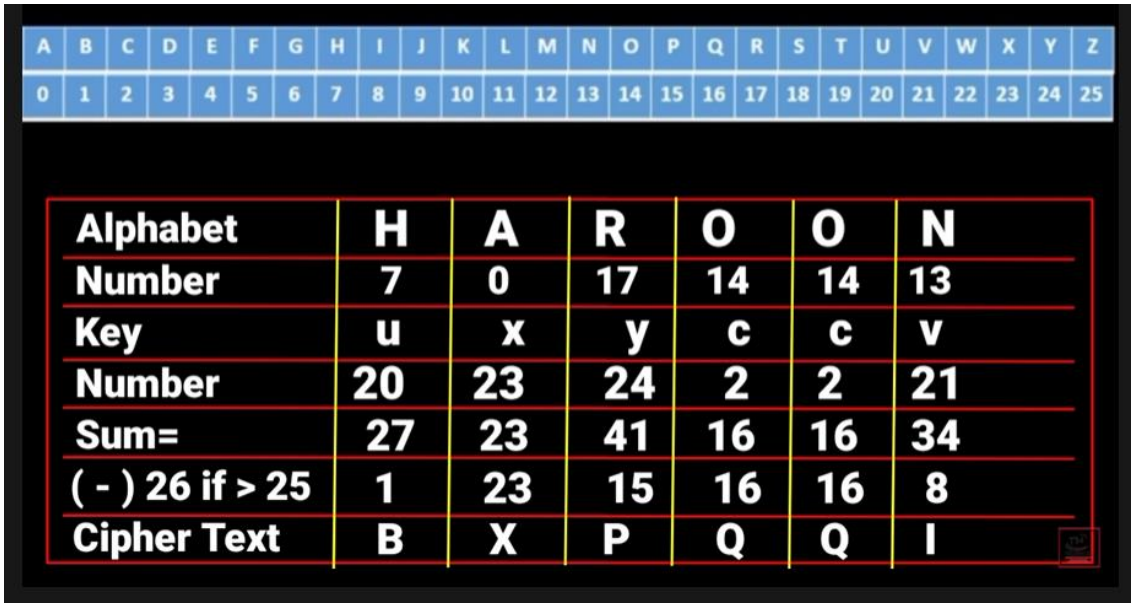
Example:-

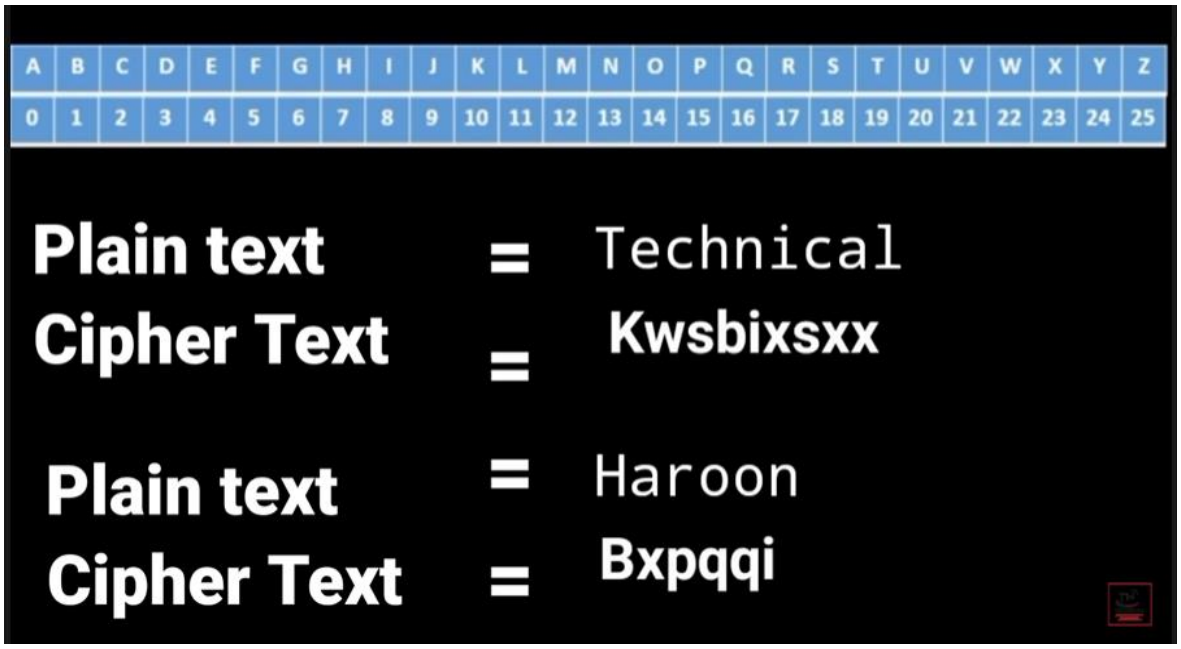
Plain text :- Technical Haroon





Alphabet	T	E	C	H	N	I	C	A	L
Number	19	4	2	7	13	8	2	0	11
Key	R	S	Q	U	V	P	Q	X	M
Number	17	18	16	20	21	15	16	23	12
Sum=	36	22	18	27	34	23	18	23	23
(-) 26 if > 25	10	22	18	1	8	23	18	23	23
Cipher Text	K	W	S	B	I	X	S	X	X

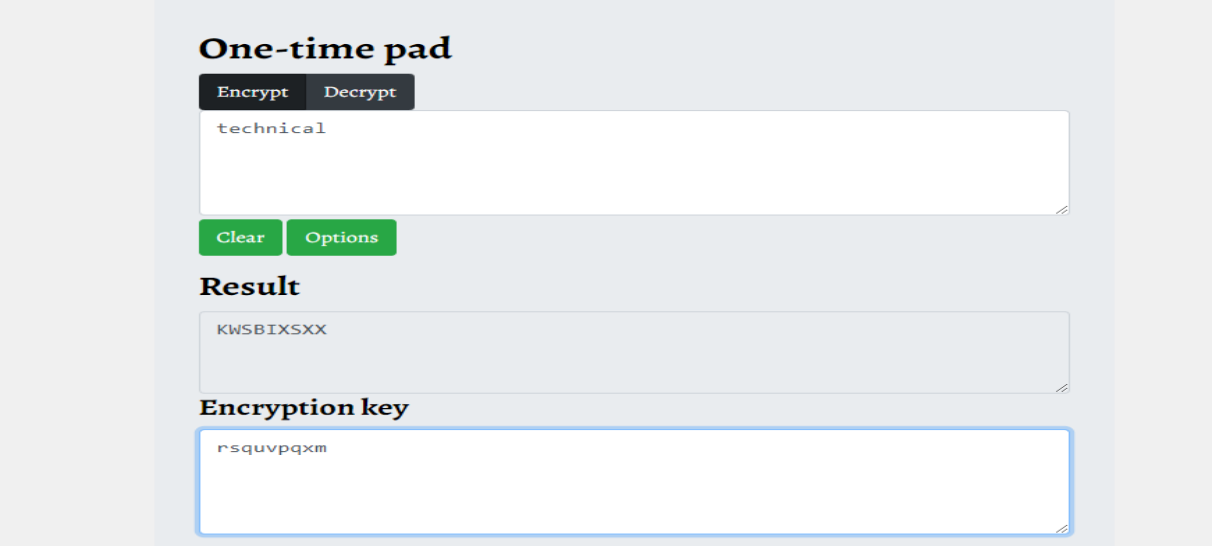


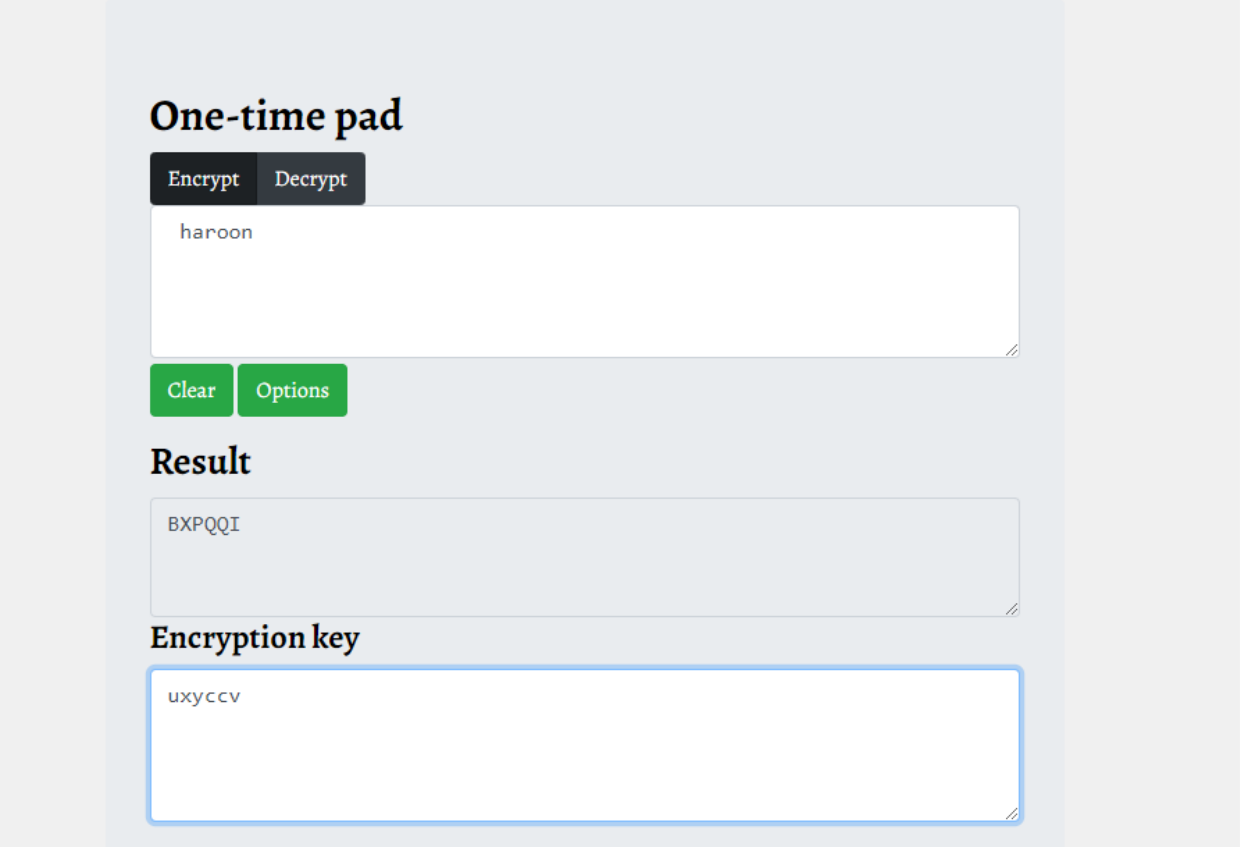


(Manually method)

Tool:-

Website :- https://www.boxentriq.com/code-breaking/one-time-pad





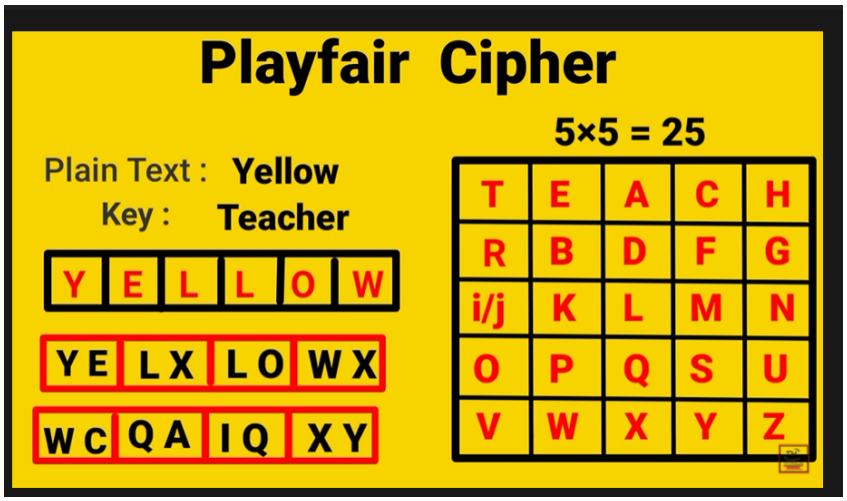
Playfair Cipher :-

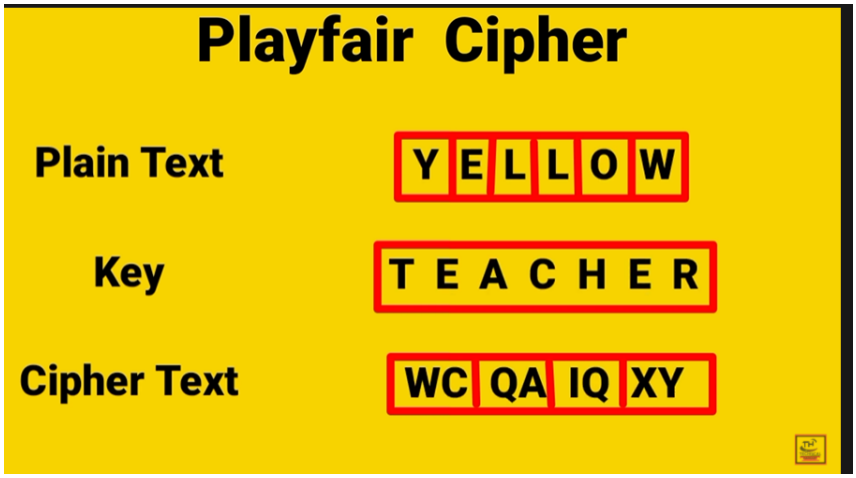
1. **Playfair Cipher was the first practical digraph substitution cipher**

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

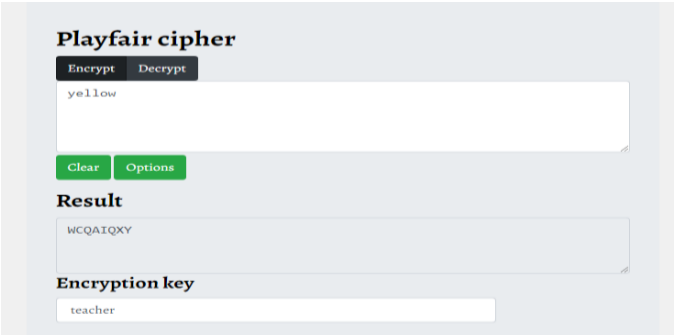
3. Its is a polygraphic cipher and using substitution technique.

Example:-

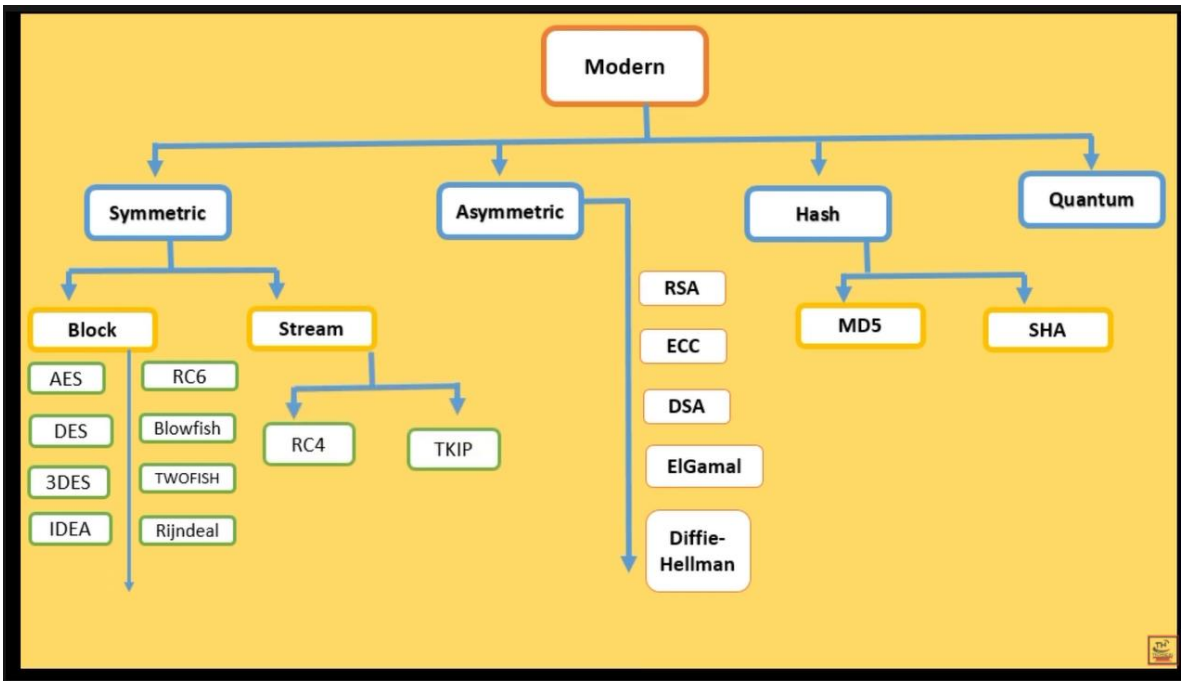




Website:- https://www.boxentriq.com/code-breaking/playfair-cipher



MORDEN CRYPTOGRPHY:-



Types of Cryptography

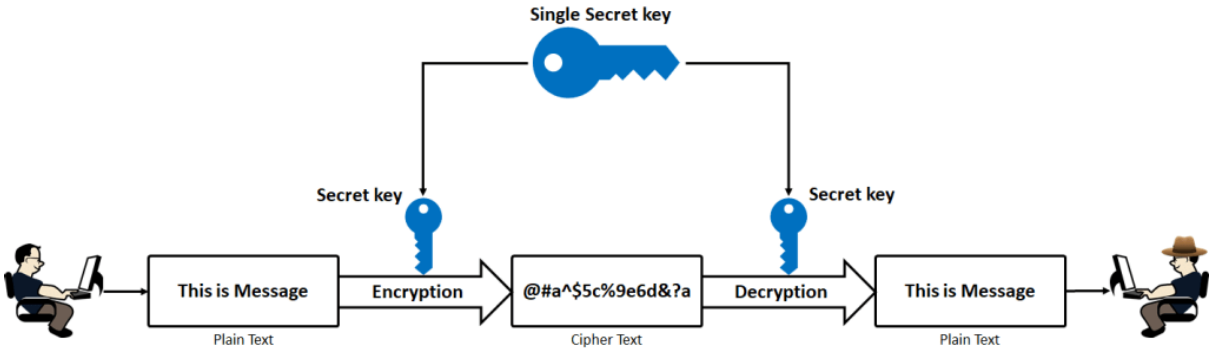
So, based on how we encrypt and decrypt the file, Cryptography is mainly classified as two types

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

Let's discuss both in detail.

Symmetric Key Cryptography

Symmetric key cryptography is also called Private key Cryptography. In this approach, both the sender and receiver will use the same key for encrypting and decrypting the message.

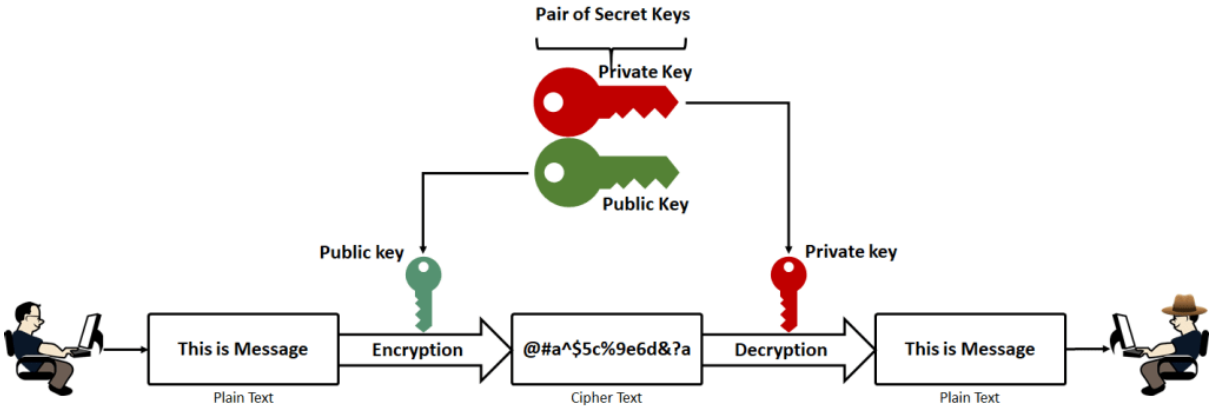


Symmetric Cryptography

This means, In Symmetric Key Cryptography Sender will encrypt the data with a secret key. Then the receiver will use the same key to decrypt the received data. AES, DES, RC4, RC5, and RC6 are examples of symmetric key Cryptography

Asymmetric Key Cryptography

Asymmetric Key Cryptography is called as Public-key cryptography. In this approach, Receiver will use Private Key to Decrypt and Sender will use Public Key Encrypt.



Asymmetric Cryptography

So, when you send some data with Asymmetric Key cryptography to Joe, you will Encrypt the data with a public key which can be opened only by You with the Private Key Not even the Public Key. This method is considered more secure than the Symmetric Key Cryptography. Some most used Asymmetric Key Cryptography is Elliptic curve techniques, RSA, DSA, PKCS.

Hashing :-

A hashing algorithm is a mathematical function that garbles data and makes it unreadable.

Hashing algorithms are one-way programs, so the text can't be unscrambled and decoded by anyone else. And that's the point. Hashing protects data at rest, so even if someone gains access to your server, the items stored there remain unreadable.

Hashing can also help you prove that data isn't adjusted or altered after the author is finished with it. And some people use hashing to help them make sense of reams of data.

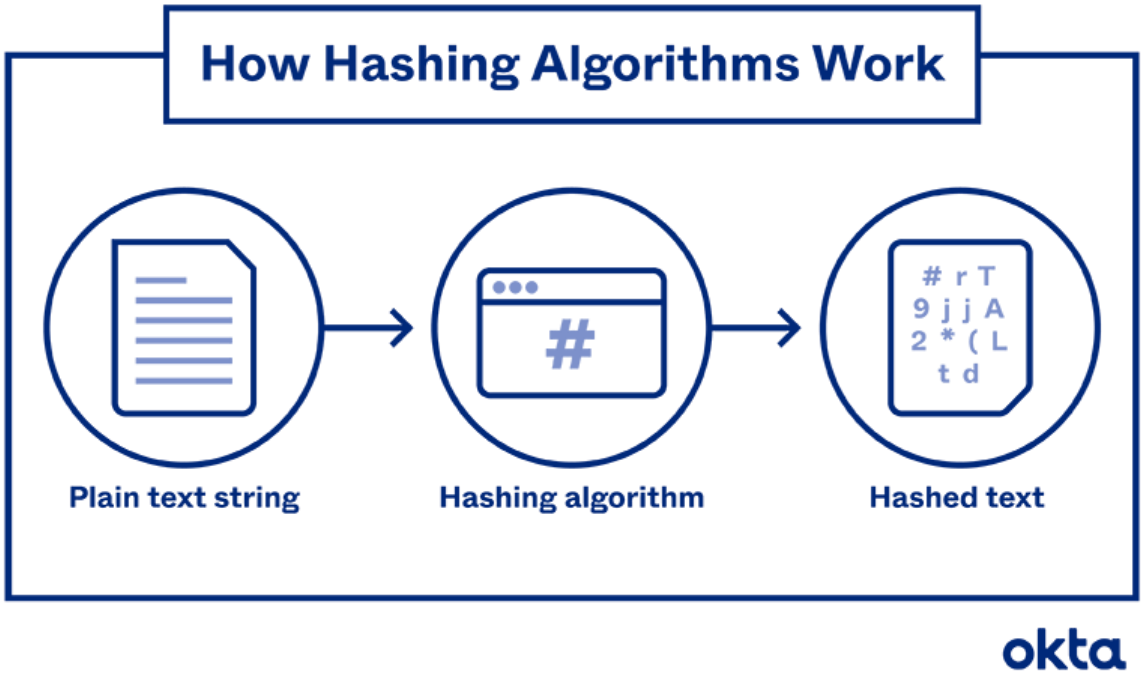
What Is a Hashing Algorithm?

Dozens of different hashing algorithms exist, and they all work a little differently. But in each one, people type in data, and the program alters it to a different form.

All hashing algorithms are:

- **Mathematical.** Strict rules underlie the work an algorithm does, and those rules can't be broken or adjusted.
- **Uniform.** Choose one type of hashing algorithm, and data of any character count put through the system will emerge at a length predetermined by the program.
- **Consistent.** The algorithm does just one thing (compress data) and nothing else.
- **One way.** Once transformed by the algorithm, it's nearly impossible to revert the data to its original state.

It's important to understand that hashing and encryption are different functions. You might use them in concert with one another. But don't use the terms interchangeably.



How Does a Hashing Algorithm Work?

It's possible to create an algorithm with nothing more than a chart, a calculator, and a basic understanding of math. But most people use computers to help.

Most hashing algorithms follow this process:

- **Create the message.** A user determines what should be hashed.
- **Choose the type.** Dozens of hashing algorithms exist, and the user might decide which works best for this message.
- **Enter the message.** The user taps out the message into a computer running the algorithm.
- **Start the hash.** The system transforms the message, which might be of any length, to a predetermined bit size. Typically, programs break the message into a series of equal-sized blocks, and each one is compressed in sequence.
- **Store or share.** The user sends the hash (also called the "message digest") to the intended recipient, or the hashed data is saved in that form.

The process is complicated, but it works very quickly. In seconds, the hash is complete.

What Are Hashing Algorithms Used For?

The very first hashing algorithm, developed in 1958, was used for classifying and organizing data. Since then, developers have discovered dozens of uses for the technology.

Your company might use a hashing algorithm for:

- **Password storage.** You must keep records of all of the username/password combinations people use to access your resources. But if a hacker gains entry, stealing unprotected data is easy. Hashing ensures that the data is stored in a scrambled state, so it's harder to steal.

- **Digital signatures.** A tiny bit of data proves that a note wasn't modified from the time it leaves a user's outbox and reaches your inbox.

- **Document management.** Hashing algorithms can be used to authenticate data. The writer uses a hash to secure the document when it's complete. The hash works a bit like a seal of approval.

  A recipient can generate a hash and compare it to the original. If the two are equal, the data is considered genuine. If they don't match, the document has been changed.

- **File management.** Some companies also use hashes to index data, identify files, and delete duplicates. If a system has thousands of files, using hashes can save a significant amount of time.

Hashing Algorithm Examples

It may be hard to understand just what these specialized programs do without seeing them in action.

Imagine that we'd like to hash the answer to a security question. We've asked, "Where was your first home?" The answer we're given is, "At the top of an apartment building in Queens." Here's how the hashes look with:

- **MD5:** 72b003ba1a806c3f94026568ad5c5933
- **SHA-256:** f6bf870a2a5bb6d26ddbeda8e903f3867f729785a36f89bfae896776777d50af

Now, imagine that we've asked the same question of a different person, and her response is, "Chicago." Here's how hashes look with:

- **MD-5:** 9cfa1e69f507d007a516eb3e9f5074e2
- **SHA-256:** 0f5d983d203189bbffc5f686d01f6680bc6a83718a515fe42639347efc92478e

Notice that the original messages don't have the same number of characters. But the algorithms produce hashes of a consistent length each time.

And notice that the hashes are completely garbled. It's nearly impossible to understand what they say and how they work.

Popular Hashing Algorithms Explained

Many different types of programs can transform text into a hash, and they all work slightly differently.

Common hashing algorithms include:

- **MD-5.** This is one of the first algorithms to gain widespread approval. It was designed in 1991, and at the time, it was considered remarkably secure.

  Since then, hackers have discovered how to decode the algorithm, and they can do so in seconds. Most experts feel it's not safe for widespread use since it is so easy to tear apart.

- **RIPEMD-160.** The RACE Integrity Primitives Evaluation Message Digest (or RIPEMD-160) was developed in Belgium in the mid-1990s. It's considered remarkably secure, as hackers haven't quite figured out how to crack it.

- **SHA.** Algorithms in the SHA family are considered slightly more secure. The first versions were developed by the United States government, but other programmers have built on the original frameworks and made later variations more stringent and harder to break. In general, the bigger the number after the letters "SHA," the more recent the release and the more complex the program.

For example, SHA-3 includes sources of randomness in the code, which makes it much more difficult to crack than those that came before. It became a standard hashing algorithm in 2015 for that reason.

- **Whirlpool.** In 2000, designers created this algorithm based on the Advanced Encryption Standard. It's also considered very secure.

The government may no longer be involved in writing hashing algorithms. But the authorities do have a role to play in protecting data. The Cryptographic Module Validation Program, run in part by the National Institute of Standards and Technology, validates cryptographic modules. Companies can use this resource to ensure that they're using technologies that are both safe and effective.

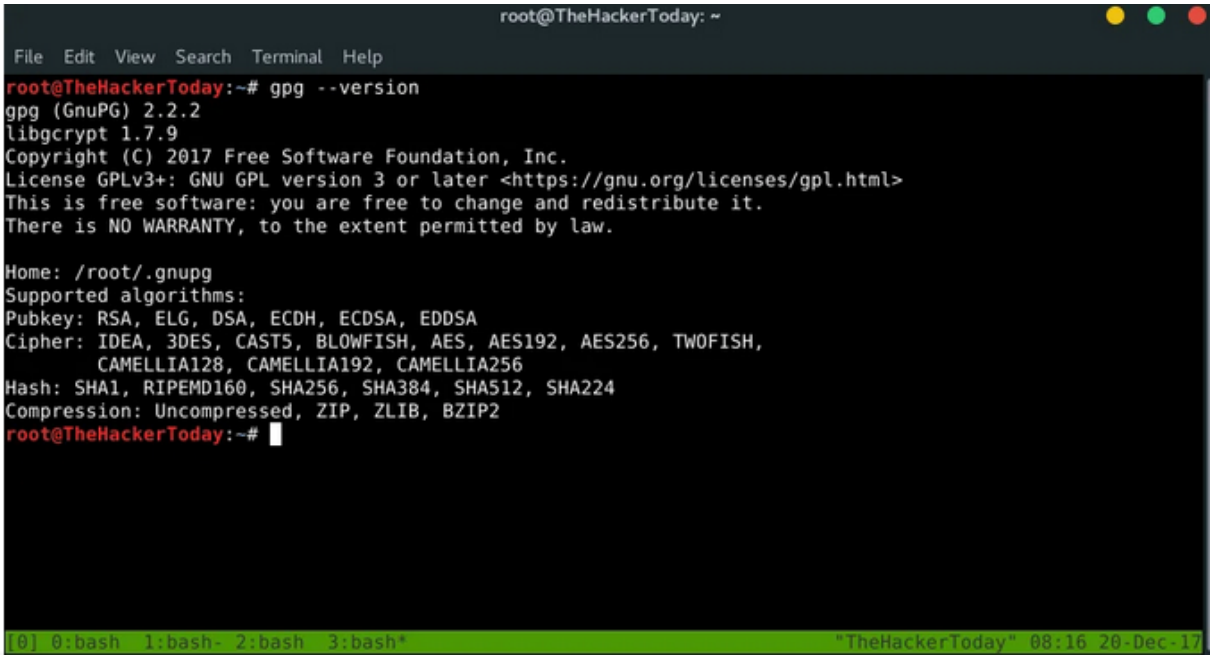
Practical Of GPG Tool

Today we're going to encrypt a file or directory using Gpg tool which can be installed in any Linux version. If you are really concerned about your privacy and you don't want your friends to sneak into your laptop or files you can use strong passwords, hide files somewhere in safe locations, or in some cases, you can encrypt files. You can do pretty much everything from encrypting a file to an entire hard drive.

Also Read: Creating an Encrypted Folder in Kali Linux/Ubuntu/Windows & Mac using TrueCrypt

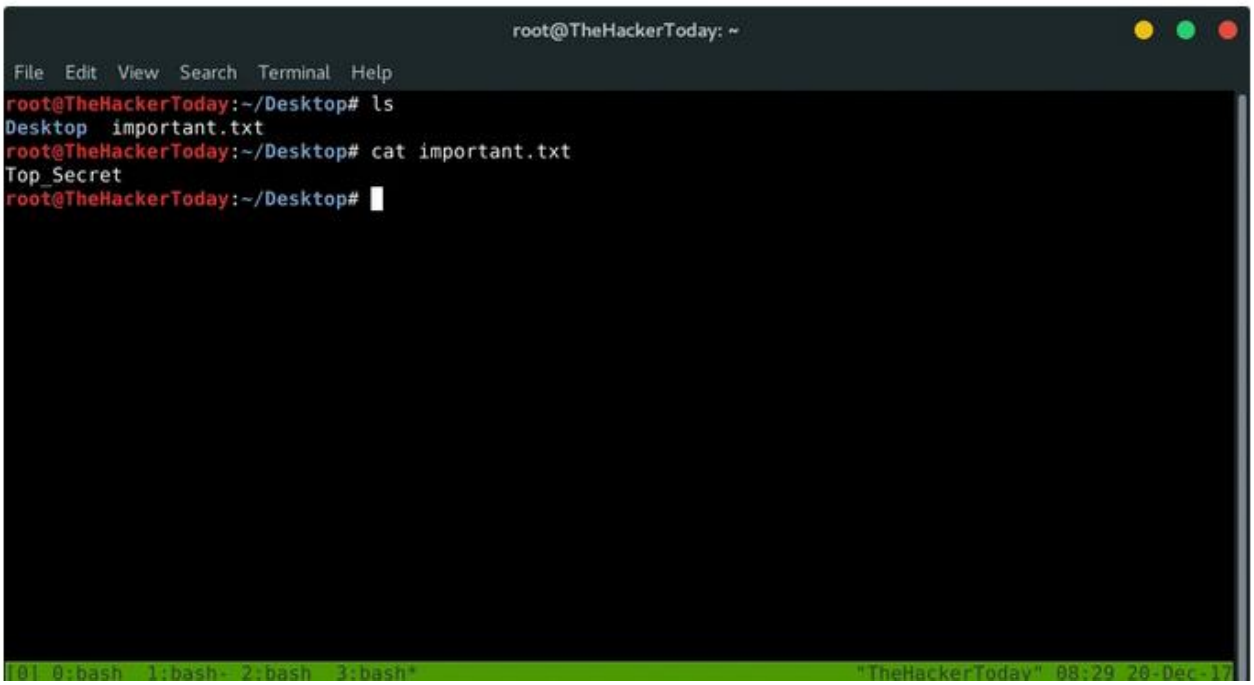
Gpg is a free tool that is used to encrypt a single file or folder with few commands, the only way to decrypt those files is with a password.

Let's get started! For this tutorial, I'm using Kali Linux and it has Gpg pre-installed not just Kali it comes pre-installed in every Linux version.

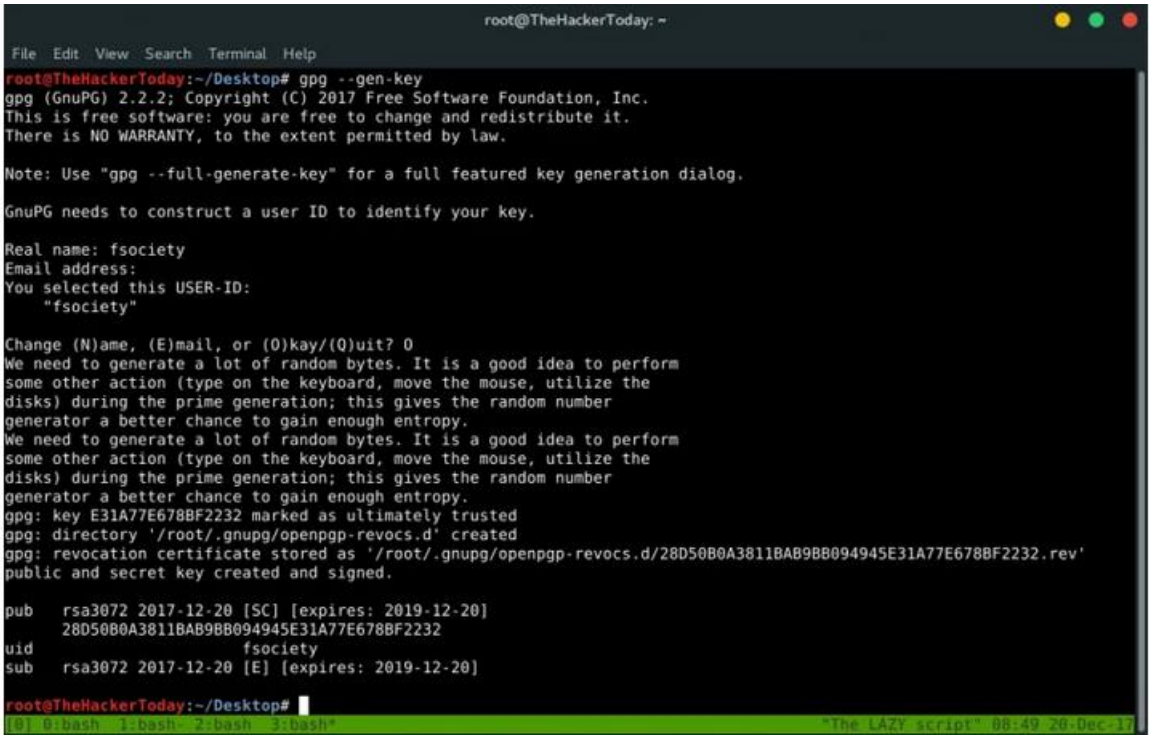


How to Encrypt/Decrypt a File in Linux using gpg (Kali Linux)

Let's say you have file name important.txt and it contains some classified information or some secret stuff that you wanna hide. This 'important.txt' file contains the text "Top_Secret" or something totally depends on your work, let's say it's a password.



Now, Before everything we have to generate a key first. You will be prompted to enter some security information. Use the defaults when available, otherwise enter your name and email address. You will also be prompted for a passphrase. Remember this passphrase.



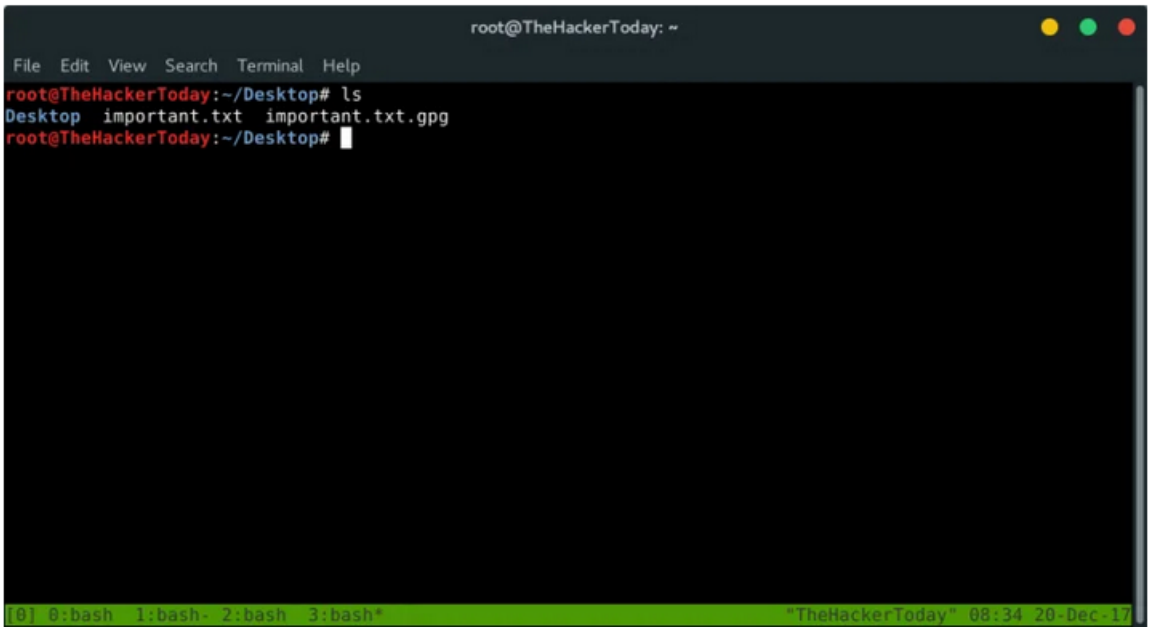
gpg --gen-key

After generating the key. We have to encrypt our file.

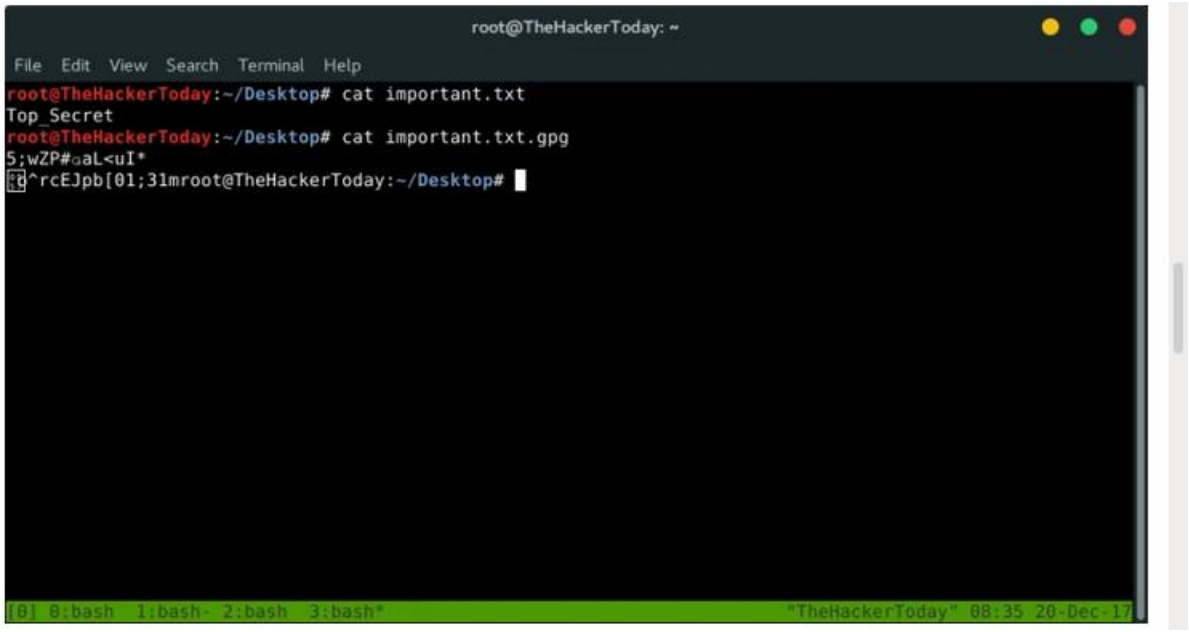
Type

gpg -e -r fsociety important.txt

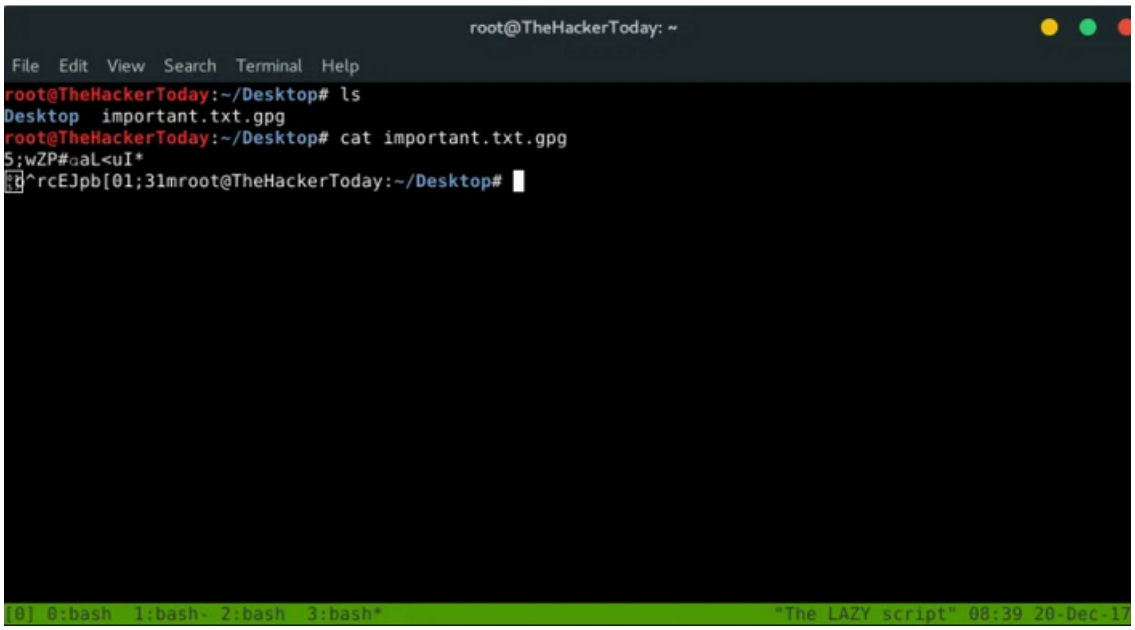
If you remember fsociety is our USER-ID. After typing that command your file will be encrypted and another file will be generated with a .gpg extension to delete your original non-encrypted file.



Now you'll see two files "important.txt" and "important.txt.gpg" let's cat to see the difference.



As you can see gpg has encoded our string or password inside "important.txt" file and now you can delete your previous text file.



Now, It's time to decrypt our "important.txt.gpg" back to "important.txt" and readable text.

Type:

gpg -d -o decrypted.txt important.txt.gpg

You will be prompted to enter a password for the key and boom!