#### Introduction of Cryptography

Cryptography is a technique of secure communication that deals with developing and analyzing protocols capable of providing information security. It is based on mathematical algorithms that provides information security services between the parties.

The main objectives of using cryptography is to provide following security measures:

1. Confidentiality

It provides confidentiality so that the information can only be accessed by certain peoples or places.

1. Data Integrity

It prevents improper information modification or destruction so that the data remains accurate and consistent throughout its life cycle.

1. Non-repudiation

It provides an assurance so that the acting entity cannot deny the authenticity of the creation and transmission of the information at later stage.

1. Authentication

It verify that users are who they say they are and that each input arriving at the system came from a trusted source. It ensure receiver that the data received is sent by the verified sender.

### Importance of cryptography in network security

Network security is very important in modern day world. The need of network security increases to maintain the confidentiality and data integrity so that the information is delivered securely from sender to the intended receiver without any intervene from unauthorized access.

While we are communicating over a public network our information is at risk of breaching. Using cryptography when we send a message in plain text after reaching the network it is converted into cipher text and finally it is converted into plain text after reaching the receiver keeping the information secure.

In modern day world we store very important things in the internet like digital contract, digital signature, password, e banking etc. Breaching of such important information results in huge loss. Everybody wants to have their important information safe and secured thus promoting the need of cryptography in network security.

Cryptography offers us non-repudiation and authentication so that both sender and receiver are verified by the cryptographic system and one cant deny their action at later stage.

# Motivation

Nowadays, the use of informative data is increasing day by day. Most people have little knowledge about how to protect their factual data from unauthorized users. Many people just give their credential information in open source where many user can access their data in a easy way. We want to overcome such vulnerability method in important data. We want to give access of data only to the known users. Only cryptography can protect our data from hackers or unknown users. With the help of cryptography we can securely use our password in vast network for online purchase and e-banking. Cryptography is used to secure all transmitted information in the world connected by internet. For example bank transactions wouldn’t be safe without cryptography.

Internet traffic would come to halt and use can no longer make phone calls. Without cryptography international organization cannot protect their valuable information and the information could be exposed and cause huge loss. Cryptography is one of those areas where a little knowledge goes a long way. Even understanding a few basic terms can really help you in using encryption services, and will mean that you are less likely to get ripped off by over-paid security.

### Programming language and software tools

We decided to use python programming language for this project. To write and execute code we used Anaconda framework, Postgresql, TKinter and socket programming.

### Anaconda framework

Anaconda is open source distribution of python and R language for scientific data computing to ease the package management and deployment. Various features and libraries of the anaconda framework are used in designing this project.

### Postgresql

Postgresql is a free and open source relational database management system. We used postgresql to store out data and to maintain integrity of the data. It helps developers to build and run complex program.

### Tkinter module

Tkinter is a open source GUI library designed to use in python programming. We use Tkinter because it is easier, faster and powerful interface to Tk GUI toolkit. It helps programmers to design attractive graphical interface.

### Socket programming in python

Socket programming is a way to connect two nodes in a network so that they can communicate with each other. It is used to establish communication link between client and server. Sockets and socket API are used to send message across the network. They provide a form of inner process communication.

### Expected outcome

To understand the basics of cryptography and network security. To store username and password using hash function SHA-512. To create and store data using postgresql database.To establish communication between client and served using socket programming. Use DHKE( Diffie-Hellman key exchange) to encrypt and decrypt the message sent over the network