SYNOPSIS

ON

“Secure Communication System using Cryptographic Protocols”

Submitted in

Partial Fulfillment of requirements for the Award of Degree

*of*

Bachelor of Technology

*In*

Computer Science and Engineering

By

**(Project Id: 23D07)**

# Mohammad Anas (1901640100168)

# Aman Rawat (1901640100044)

# Aditya Sharma(1901640100026)

# Ankit Kumar Chaubey (1901640100055)

Under the supervision of

**Dr. Manoj Kumar Mishra**

**(Associate Professor)**



**Pranveer Singh Institute of Technology**.

 Kanpur - Agra - Delhi National Highway - 19

Bhauti -Kanpur - 209305.

(Dr. A.P.J. Abdul Kalam Technical University)

1. Introduction

Information security can be summed up to info, a group of steps, procedures, and strategies that are used to stop and observe illegal access, troubleshooting, revelation, perturbation and adjustment of computer network sources.

Enhancing the privacy, eligibility and reliability of the work requires a lot work to strengthen the current methods from constant trials to break them and to improve new ways that are resistant to most kinds of attacks if not all. Accordingly, it was proven that encoding is one of the most reliable strategies used to secure information since the ancient days of the Romans who used similar methods to enable security on their valued information and documents Cryptography is the art of creating written or generated codes that allow information to be kept secret.

Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it.

Cryptography is a technique of securing information and communications through use of codes so that only those people 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”.

**2. Project Objective**

The main objective of this project is to develop an chat application through which we can perform encryption of text in order to allow only the intended recipients of a message to receive the message properly while interrupt eavesdroppers from understanding the message.

In current computer systems, cryptography provides a strong, economical basis for keeping data classified and for verifying data indignity. While our conventional cryptography methods, such as AES (encryption) and RSA (signing), work well on systems which have reasonable processing power and memory capabilities, these do not scale well into a world with embedded systems and sensor networks.

Thus, lightweight cryptography methods are proposed to overcome many of the problems of conventional cryptography. The cryptosystem performs its encryption by encrypting the plaintext using enhanced cryptographic protocol RSA.

This Django based chat application project sets out to contribute to the general body of knowledge in the area of classical cryptography where you can send messages encrypted using RSA algorithm.

**3. Literature Survey**

* The security of web for keeping money, account passwords, messages, accounts, etc. requires content protection in mechanized media. It shows the security besides, pressure for the information with the move encryption standard. RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.
* Caesar cipher, otherwise called the shift cipher, is one of the least complex and most generally known old style encryption systems. It is a kind of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the letters in order. For example, with a shift of 3, A would be replaced by D, B would become E, etc. This algorithm is not so secure and can be cracked easily by security attacks techniques.
* The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised.
* Encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.
* Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser. This chat application would be really helpful for messaging as the data would me securely encrypted in 128 bits and in 1048 bits as well.

4. Feasibility Study:

Feasibility study is about the viability of a system. It measures the organizational benefit or applicability of an information system and helps in taking decisions such as which software to use, hardware combinations, etc.

The four phases of feasibility study for the project include :

1. Technical Feasibility

* The H/W and S/W required are easy to install and handle.
* The necessary H/W configuration and software platform is already there.
* The system supports interactivity with the user through web application.

2) Behavioral Feasibility

* The proposed system has user-friendly interface.
* It is reliable.
* It requires no efforts for training the software.

1. Economical Feasibility

* This application can be used by anyone who wants to securely transmit private information.
* There will be no training cost as system has very user friendly GUI.
* Our system will reduce time that is wasted in manual processes.

1. Operational Feasibility

* The application will fulfill the user’s requirements for secure and fast encryption and transfer of information.
* It is designed such that it is lightweight i.e. it neither consumes much memory of the system nor takes much time in performing the encryption or decryption processes.

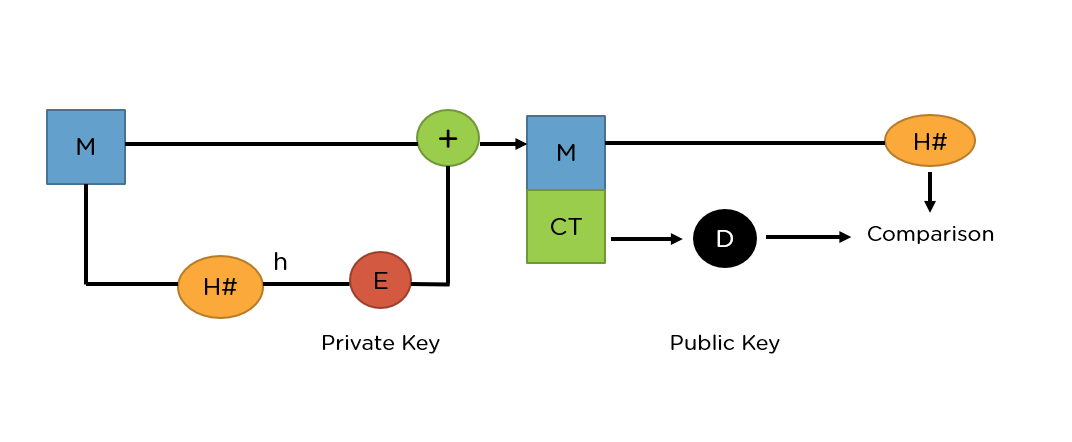
5. Methodology/ Planning of work

A web application will be built which will provide the features of strong encryption and decryption of text using RSA Cryptographic technique. The application will also perform authentication so that only the intended users can access the message. Lightweight Cryptography as Cipher is taken for Consideration for System. The famous classical cipher is used for the Defined plan to do encryption in chat application that is described below.

**RSA Algorithm**

The RSA algorithm is a public-key signature algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman. Their paper was first published in 1977, and the algorithm uses logarithmic functions to keep the working complex enough to withstand brute force and streamlined enough to be fast post-deployment.

The image below shows it verifies the digital signatures using RSA methodology.



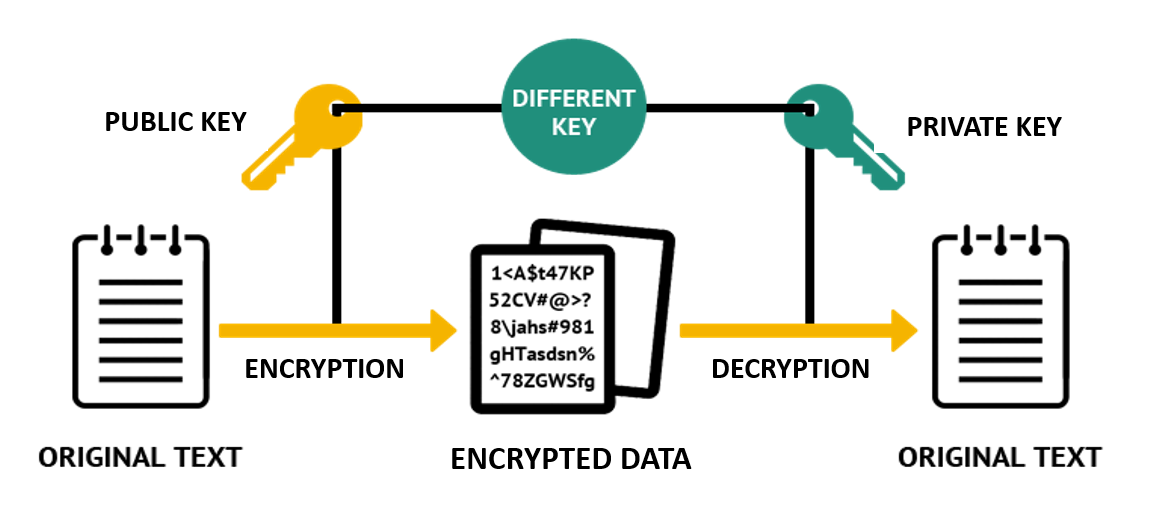
Source – simplilearn

**What Is Asymmetric Encryption?**

In Asymmetric Encryption algorithms, you use two different keys, one for encryption and the other for decryption. The key used for encryption is the public key, and the key used for decryption is the private key. But, of course, both the keys must belong to the receiver.

When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory and use it to encrypt the message before sending it.

The recipient of the message can then decrypt the message using their related private key.



Asymmetric Encryption`

Source – simplilearn

When using RSA for encryption and decryption of general data, it reverses the key set usage. Unlike signature verification, it uses the receiver’s public key to encrypt the data, and it uses the receiver’s private key in decrypting the data.

Thus, there is no need to exchange any keys in this scenario.

There are two broad components when it comes to RSA cryptography, they are:

**Key Generation**: Generating the keys to be used for encrypting and decrypting the data to be exchanged.

**Encryption/Decryption Function**: The steps that need to be run when scrambling and recovering the data.

6. Tools/Technology Used:

6.1 Hardware Requirements

CPU Type : Intel i3, i5, i7 or AMD

RAM Size : Minimum 512 MB

Hard Disk Capacity : Minimum 2 GB

6.2 Software Requirements

Operating System : Windows/ Linux/ iOS

Programming Languages/ Python, HTML, CSS, Django

Frameworks :

IDE : VSCode, PyCharm

7. References [IEEE format]:

* [RSA algorithm - Wikipedia](https://en.wikipedia.org/wiki/RSA_(cryptosystem))