Internship Project Report
Secure Chat Application with End-to-End Encryption

Introduction

In today's digital world, secure communication is more important than ever. As part of my cybersecurity internship, I developed a secure chat application that ensures complete privacy using real-time encrypted messaging between users.

Abstract

The project implements a secure chat platform using a combination of RSA and AES encryption to achieve end-to-end encrypted communication. It allows real-time chatting via Flask-SocketIO, where messages are encrypted on the sender's side and only decrypted by the receiver. This ensures no third party, including the server, can read the messages.

Tools & Technologies Used

- Python 3
- Flask
- Flask-SocketIO
- cryptography (RSA, AES)
- HTML, CSS, JS
- WebSockets

Workflow / Steps Involved

1. RSA Key Generation: Each user generates a public-private RSA key pair upon joining.
2. Public Key Exchange: Users share their public keys for AES key encryption.
3. AES Key Generation: A new AES key is generated for each conversation and encrypted using the recipient's public key.
4. Message Encryption: Each message is encrypted with AES before being sent.
5. Real-Time Messaging: Messages are transmitted via SocketIO.

6. Client-Side Decryption: Receiver decrypts AES key and then the message.

Features

- Real-time chatting via WebSocket
- End-to-end encryption using AES + RSA
- Secure public key sharing
- Enter-to-send functionality
- Chat alignment: sent on right, received on left
- Chat auto-scroll from bottom
- Stylish UI (dark mode optional)
- Emoji support (optional)
- Scalable for future file sharing or notifications

Conclusion

This project helped me understand practical cryptography and how to secure communication over the web. It also taught me how to work with web sockets, Flask servers, and frontend-backend integration. The app is simple but lays the foundation for fully secure messaging systems.

Acknowledgment

I would like to thank my internship mentor and ChatGPT for continuous support in code correction, encryption understanding, and project organization.