Krantiveer Vasantrao Narayanrao Naik Shikshan Prasarak Sanstha
LOKNETE GOPINATHJI MUNDE
INSTITUTE OF ENGINEERING EDUCATION & RESEARCH
Canada Corner, Sharanpur Road, Nashik 422 002
Approved by AICTE, Accrediated 'B' Grade by NAAC
Computer Engineering Department

Academic Year: 2023-24 **Class:** BE

Subject: Project Lab **Sem :** II

Assignment No: 01

Title: Project workstation selection and review design necessary corrective action taking into consideration the feedback report of term I assessment.

Due Date: Date Submitted:

Guide Name: Prof. A.S.Gaikwad A.S.Gaikwad

Guide Remark: .....

	Student Name(Roll No.)	Performance	Understanding	Submission	Total
(2)	Dhananjay S. Aher	3	3	2	8
(53)	Gaurav M. Vadnere.	4	4	2	10
(54)	komal k. Walke	3	3	2	8
	Pratham G. kotkar	3	3	2	8

Project Coordinator: Prof. D. D. Sharma D.D.S

Head of Department: Prof. R. M. Shaikh R.M.S

1. Which algorithm you have used for implementation?

Ans: BlinkBuzz is the Messenger Application by using SHA-256 with RSA Algorithm.

SHA-256: SHA-256 stands for Secure Hash Algorithm 256- bit and it's used for cryptographic security. **SHA-256 with RSA**: SHA256 with RSA is a hybrid cryptographic algorithm that leverages the SHA-256 hashing algorithm and the RSA digital signature scheme. It utilize SHA-256 to generate a hash value for the data and then signs the hash using RSA with a private key

2 . Your Project or Application can be used in real life? Justify it.

Ans: Yes. Our application can be use in real life. BlinkBuzz- The Indian Messenger app are similar messaging platforms, are extensively used in real life for a multi purposes like, Personal communication, Privacy and Security, Group Chats, Voice and Video Call, File Sharing, Status Upload-Download.

3 . Future scope of the project.

Ans: The main intention of this application is to introduced new features of WhatsApp. In this project, we have successfully designed and implemented an instant messaging application that replicates the core functionalities of WhatsApp while introducing two significant additional features: the ability to add music to user statuses and the capability to download statuses shared by other users. This effort involved extensive software development and testing to ensure a seamless user experience

4 .What are the goals of the project?

Ans: The main goal of our application is to facilitate seamless communication and connection between individuals and groups. Key goals of our app is Instant Messaging, Cross-Platform Compatibility, Multimedia Sharing, Voice and Video Calling, Group Chats, User-Friendly Interface, Status Download, Pin Message, Image Quality Selection, Screenshot Prevention.

5 .Where this developed project can be applied?

Ans: This Project BlinkBuzz - Indian Messenger applications can be applied in various contexts and industries, catering to diverse communication needs and scenarios. This application can be use for personal communication, Business Communication, Group Collaboration, Customer Engagement, Emergency Communication, etc.

6 What is approximate Project Cost?

Ans: Project cost is Rs.

7 What is Front end and Back end of project

Ans:

Front end : XML, Kotlin

Back end : Firebase.

8 .Explain the Algorithms used in the project.

Ans:

Algorithm for Message encryption and decryption using SHA-256 with RSA algorithm.

Encryption:

Step 1 - Message Hashing (SHA-256):

- Generate a SHA-256 hash of the plaintext message. This hash serves as a digest of the message and ensures integrity.
- The SHA-256 hash function produces a fixed-size output (256 bits), regardless of the input message size.

Step 2 - Digital Signature (RSA Encryption):

- Sign the SHA-256 hash value using RSA encryption with the sender's private key.
- RSA encryption involves exponentiating the hash value with the sender's private key and taking the modulus of the result with the public key's modulus.

Step 3 - Sending the Encrypted Message:

- Send the original message along with the RSA-encrypted hash (digital signature) to the recipient.

Decryption:

Step 1 - Digital Signature Verification (RSA Decryption):

- Decrypt the RSA-encrypted hash (digital signature) using the sender's public key.
- RSA decryption involves exponentiating the encrypted hash with the sender's public key and taking the modulus of the result with the private key's modulus.

Step 2 - Message Hashing (SHA-256):

- Recalculate the SHA-256 hash of the received plaintext message.

Step 3 - Comparison:

- Compare the recalculated SHA-256 hash with the decrypted hash (digital signature).
- If they match, the message is considered authentic and has not been tampered with during transmission.