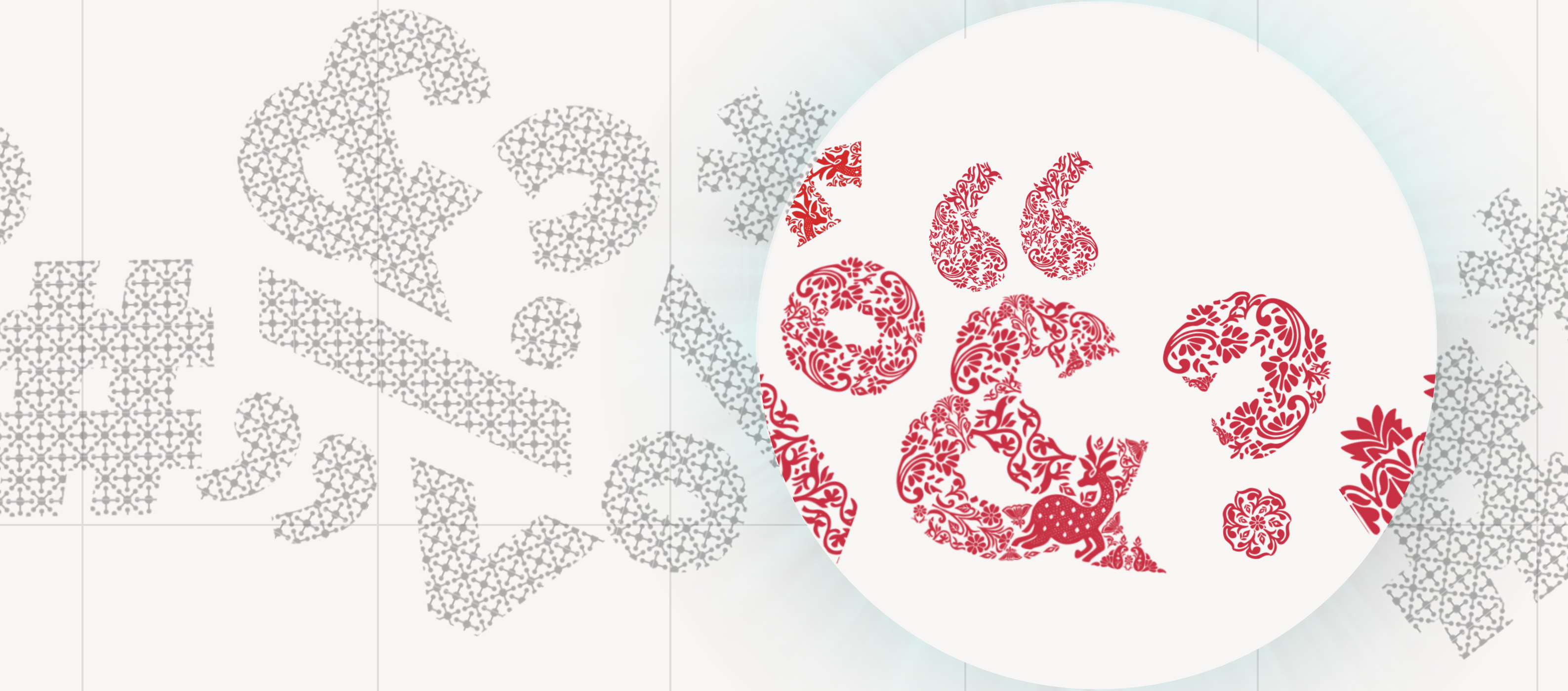
ethos 22 - 23
Blistering past horizons.

Coding Club
IIT Guwahati



Saptang Labs - Software Development Challenge

Saptang Labs

Challenge Overview:

Your task is to develop a cutting-edge secure communications app that ensures privacy and security for messaging, voice, and video communications. This app must seamlessly function across desktop, Android, and iOS platforms while integrating advanced encryption and security features, such as message expiration, secure file sharing, and multi-factor authentication (MFA). This challenge is designed to push the boundaries of cross-platform secure communications.

Software Development

Objectives

In the first round, teams must develop a functional Proof of Concept (POC) along with a detailed paper outlining the software architecture, encryption methodologies, and initial user interface design. The POC will demonstrate the basic capabilities of the app, ensuring foundational security features are in place.

Requirements for Round 1:

1. POC Submission:

a. Basic Secure Communications App: Build a secure communications app that supports encrypted messaging on one or more platforms (desktop, Android, or iOS).

b. End-to-End Encryption: Implement secure protocols such as Matrix, Signal, or other well-established encryption libraries to protect communication channels.

c. Core Functionality: Demonstrate the ability to send secure, encrypted messages, ensuring data protection and security are prioritised.

2. Document Submission:

a. Software Architecture Plan: Provide a detailed breakdown of the app's overall architecture, including:
i. Chosen encryption protocols and how they will be implemented.
ii. Data flow diagrams outlining message routing, encryption/decryption points, and secure storage mechanisms.
iii. Platform-specific considerations for desktop, Android, and iOS.

b. Security Features: Detail how the app will protect against tampering, data leaks, and unauthorized access.

c. Feature Plan: Include a roadmap outlining advanced security features such as message expiration, MFA, and secure file sharing that will be built in the next round.

d. UI/UX Design: Provide wireframes or design mockups showing how security and usability will be integrated into the user interface.

Evaluation Criteria

1. POC Quality: How well the POC demonstrates secure messaging and encryption.

2. Software Architecture Plan: Depth and clarity of the architectural design, including encryption methodologies and security measures.

3. Technical Feasibility: Scalability and feasibility of implementing the solution across desktop, Android, and iOS.

4. Innovation: Creativity in solving cross-platform communication security challenges.

Rules

1. Use secure open-source libraries for encryption and authentication.

2. Ensure compliance with all data protection regulations.

3. Teams must demonstrate the app's security and cross-platform functionality during the final round.

4. Teams are responsible for their own resources, including cloud services or development environments (e.g., AWS, Firebase).