Smart Bengal Hackathon (SBH-Sr)-2025

Team Name: Crypt-Think

PS No. : SBHRCCIIT033

Area/Theme: Cryptography

Hack-Proof Messages: The Future of Secure Communication

Category: Software

Objective:

- To create a Secure Messaging Application using **Post Quantum Cryptography** (**PQC**) techniques.
- Ensures end-to-end encryption using **optimised AES 256 algorithm** that remains secure against future quantum computer attacks.

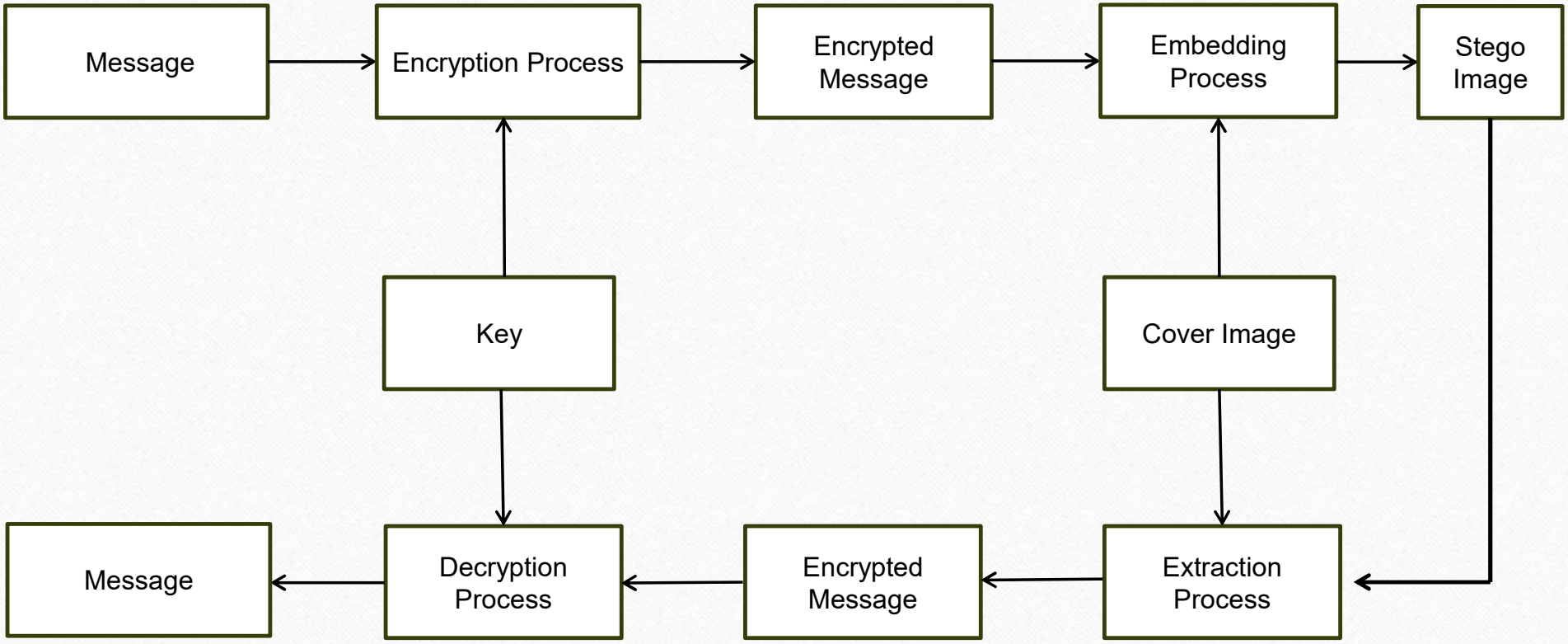
Major Societal Benefit/Target Community:

- **Individuals & Businesses :** Secure messaging platform for personal and professional correspondence.
- **Government & Defense :** Facilitate secure communication, data protection for sensitive information and operations.
- **Healthcare & Finance :** Secure transmission of sensitive data.

Other Application Areas:

- **Cloud Storage Encryption**
- **Secure Internet of Things (IoT) Communications**
- **Blockchain and Cryptocurrency Security**

Block diagram : (Hack-Proof Message)



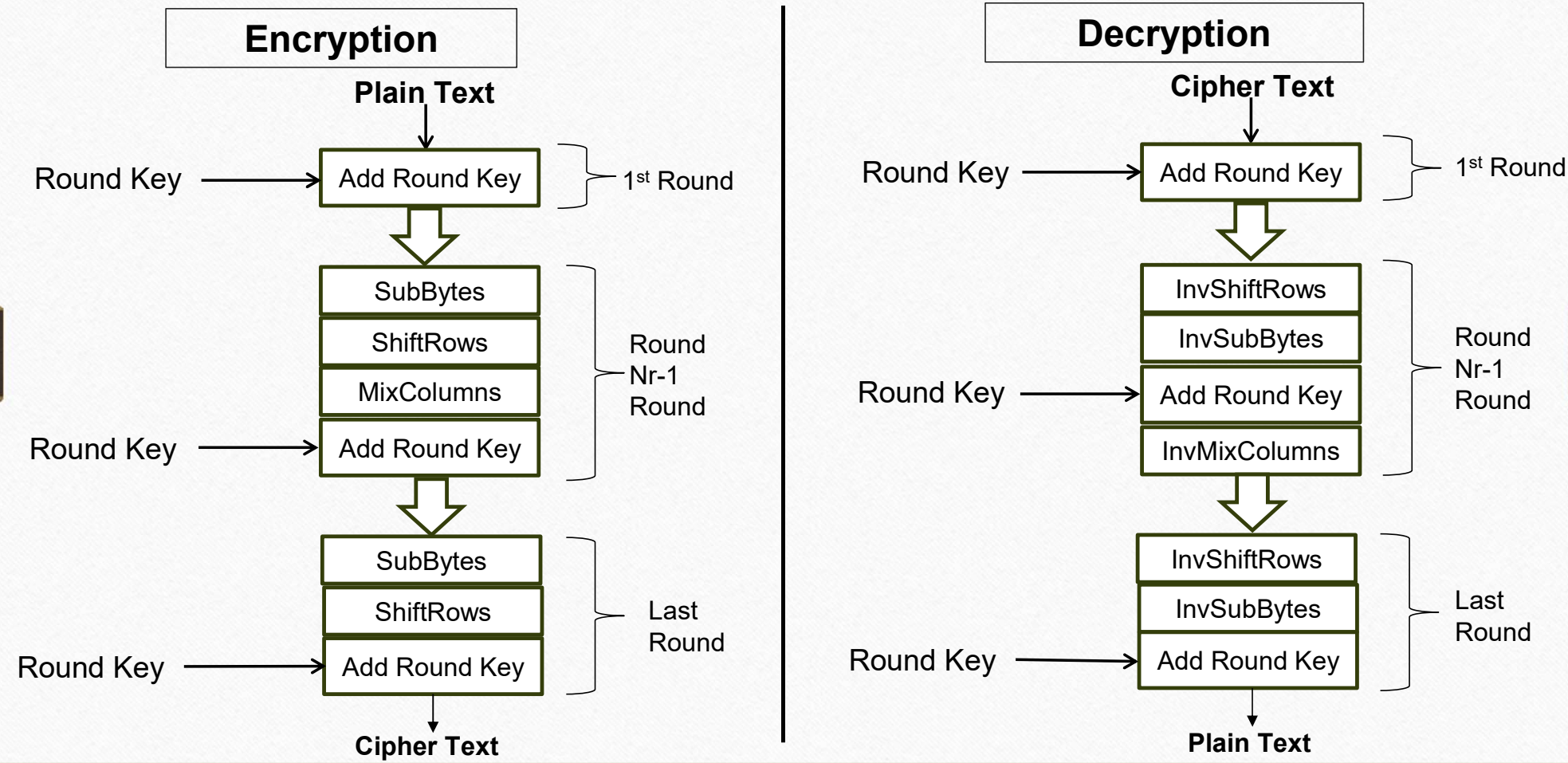
Market/Literature Survey :

- **Existing Platforms :** WhatsApp, Telegram, Signal (uses conventional encryption).
- **Threats :** Quantum computers can break conventional encryption **(RSA & ECC algorithm)** used in messaging platforms.
- **Post Quantum Cryptography (PQC) Adoption : NIST's PQC algorithms** such as **Kyber**, **Dilithium** gaining attraction.
- **References : https://ieeexplore.ieee.org/abstract/document/4682291**

Novelty (comparative study between proposal & survey):

- **Existing Apps :** Uses **RSA & ECC algorithm**, vulnerable to quantum attacks.
- **Our Solution :** Implements **Lattice based encryption** (**Kyber**, **Dilithium**) and **optimised AES 256 algorithm** to prevent quantum decryption.
- **Focus :** Protecting data**,** offering high level privacy by encrypting data using a **256-bit key**.

Data flow diagram: (AES 256 Algorithm)



Component list (if applicable):

NA (Not applicable)

Software used (whether open source, mention):

- **Programming Language:** Python (Backend), JavaScript (Frontend).
- **Libraries and framework:** Flask, FastAPI, Websockets, Open quantum safe(SQS).
- **Database:** Firebase, SQLite.
- **Platform:** Web.
- **Open source:** Yes.

Total price (if applicable):

NA (Not-Applicable).

Features (*highlight keywords*):

- Secure exchange of information.
- No third-party access.
- Fully end-to-end encrypted chats (using **Optimised AES 256 algorithm)**
- Secure against future **Quantum Computer Attacks**.
- Time compatible.
- Multi device support.
- **Opensource** and transparent.
- Cost effective.

Team details

Name	College/ University Name	Department	Degree	Year	Univ Roll No	Position
Samanway Bhattacharya	Guru Nanak Institute of Technology	Cyber Security	B.Sc.	2nd	31140423026	Team Leader
Subhronil Paul	Guru Nanak Institute of Technology	Cyber Security	B.Sc.	2nd	31140423033	Member
Srija Jana	Guru Nanak Institute of Technology	Cyber Security	B.Sc.	2nd	31140423032	Member
Sholankee Saha	Guru Nanak Institute of Technology	Data Science	B.Sc.	2nd	31140523042	Member

Mentor details

Name	College/University Name	Department
Sumit Kumar Banerjee	Guru Nanak Institute of Technology	Computer Science & Engineering