SimPriv API Progress Report

Team Members: Ayush Kohli and Utsav Dhungel

Project :

Simpriv is a REST based API for exchanging notes. We are trying to implement a service like privnote (https://privnote.com) and Snapchat. Features include:

- User signs up for the service and can send messages to other users. Upon signup user receives a public key, private key and their username
- After the message is posted a random http URL is generated which contains the message and the sender provides http URL to the receiver to view the message. The message is encrypted by sender with receivers' public key. The desired receiver decrypts the message with the URL and their own private key
- Message gets destroyed permanently after the user opens the Http URL.
- All sensitive data is either hashed or encrypted

Technical Aspects:

- Linux OS for development
- Java 8 and Spring Boot for REST API development
- SQL for data storage (H2 database for development)
- Java Security API for key generation (RSA with key size 1024) and asymmetric cryptography
- Services
    - Api/users
        - POST username creates response with username, public key and private key
        - GET retrieves list of all users and their public key
    - Api/message
        - POST message with senders private key, receivers public key. Senders private key is used to verify if sender has an account with our system and receivers public key is used for encryption of message
        - POST Api/message/UUID
            - Receive submit a POST request on endpoint with receiver's private key. Private key is used for decrypting the message and then deleting it
- Security
    - Hash public and private key when creating account
    - Encrypt message to ensure security

- Delete message after successful retrieval

Similar systems:

There is not much documentation on both Snapchat and Privnote but we have found information below.

- Snapchat uses symmetric encryption to encrypt messages and uses the same key for each message between users (http://cryptofundamentals.com/snapchat)
- Privnote generates a NoteID after message is created and uses NoteID to encrypt it. It is stored with the SHA1 Hash as database key (https://pablohoffman.com/how-privnote-really-works)

Status Update:

- Added Travis CI integration
- Created URL endpoints for both api/message and api/users
- Created Class for Asymmetric key generation

Responsibilities:

- Utsav
  - Database design and implementation
  - User endpoint
  - Continuous Integration
- Ayush
  - Message endpoint
  - Classes for Key Generation and Encryption and Decryption
  - Hashing