Introduction: -

Nowadays, real time communication is increasingly rapidly. The popularity of this communication is mostly seen through messages and chats, whether be it personal messages or confidential emails. Thus, there is a need of some protection system which could prevent other party from intruding the privacy of the users. Encrypted Chatbot is such project where two or more authorized users can have chats and messages with no invasion of external party. The chats are encrypted end to end with use of different encryption methods and keys. This is done so as to protect the privacy of people and their messages. For securing of information, it is encrypted before it leaves a user's device and can only be decrypted by the intended recipient. The encrypted message is called as cipher text. For encryption and decryption both the users will require a Key, which might be public or private. The key needs to be created, stored, and offered robust end-to-end secure encryption. Therefore, this project will create ciphertexts and keys taking plain texts as input. Have a safe space for your chats!

Research: -

<https://www.scientificamerican.com/article/crack-the-code-make-a-caesar-cipher/>

<https://www.comparitech.com/blog/information-security/rsa-encryption/>

In cryptography, two techniques are used for encryption and decryption: 1. Caesar Cipher 2. RSA algorithm.

**Caesar Cipher**: It shifts the entire alphabet by the number picked by the user. For example, if the number chosen by the user is 2, then A would be replaced by C, B would become D, and so on.

**RSA algorithm: It is based on two prime numbers. These numbers are used for generating encryption and decryption keys.**

Swot Analysis: -

STRENGHTS

The ultimate strength is privacy and security of our plain texts.

WEAKNESS  
If the unauthorized user gets to know the key somehow then the text can go in wrong hands.

OPPORTUNITIES

The newer technologies can provide stronger encryption methods and keys.

THREAT

Exploitation of safety of public and private keys is one of the threats in this field.

HIGH LEVEL REQUIREMENTS: -

|  |  |  |
| --- | --- | --- |
| ID | DESCRIPTION | CATEGORY |
| HLR01 | User should be able to encrypt message. | Technical |
| HLR02 | User should be able to decrypt message. | Technical |
| HLR03 | The key should be produced & matched. | Mathematical |

LOW LEVEL REQUIREMENTS: -

|  |  |  |
| --- | --- | --- |
| ID | DESCRIPTION | STATUS |
| LLR01 | The plain text for encryption and decryption. | IMPLEMENTED |
| LLR02 | The prime numbers for generation of key. | IMPLEMENTED |
| LLR03 | Formulae for public and private keys. | IMPLEMENTED |

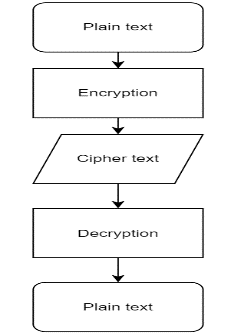
Architecture

Tools: -

* draw.io (<https://app.diagrams.net/>)
* Microsoft Word
* or any other free tool

Behavioural Diagram: -

Flowchart



Structural Diagram: -

