DATA ENCRYPTER

"Information is power"

INTRODUCTION

End-to-end encryption (**E2EE**) is a method of secure communication that prevents third-parties from accessing data while it's transferred from one end system or device to another.

In End-to-End encryption (E2EE), the data is encrypted on the sender's system or device and only the recipient is able to decrypt it. No other person or hacker can decrypt the data transferred.

Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a business's customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, lawsuits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures. In computer systems, the information is stored traditionally in form of files. A file is considered as a basic entity for keeping the information. In Unix like systems, the concept of the file is so important that almost all input/output devices are considered as a file. Therefore, the problem of securing data or information on computer systems can be defined as the problem of securing file data. We all will agree that in today's world, securing file data is very important.

PROBLEM STATEMENT

Use of cryptography algorithms to achieve the end to end encryption for memo communication (Cyber Security). There have been instances where memos have been leaked in the Indian defense sector which leads to a lot of embarrassment for defence ministry. The software can be used to eliminate these incidences. Memos are shared between different departments and also to facilitate communication between ministry, different defense forces and supreme commander. Expected Outcome: The resultant software should be able to encrypt and decrypt popular file and image formats and also facilitate https communication of these files. So, the information at any moment it could have gone to someone else. For this reason, this project work is a concern with the development of secure messaging, file and image system using the cryptographic technique.

This project work is designed and developed for secure messaging, file and image both in web and Android platforms. The application is well featured and provides encryption/decryption that can protect the message, files, and images from unauthorized access and disclosure over networks. To send a message, a recipient, a file or an image and encrypts a text message using the keyword mono-alphabetic substitution algorithm with a key, selected from the key list. The encrypted message is stored in the database and receiver's inbox with a serial number of key (not the value). The receiver, after log into his/her own account, selects the key value and then decrypts the encrypted message with the key to see

the original message. Compared to other messaging systems, the proposed secure messaging system can be used for chat, messaging and real-time file sharing in both web and Android platforms.

ABSTRACT

There are various approaches available to ensure file data security, such as encryption tools like 'AES Crypt' in Linux or integrated encryption application software or disk encrypted. But each one has its own inherent disadvantages, rendering them less frequently used. These approaches are generally cumbersome and inconvenient to the users. Therefore, there is a need for a mechanism/system which can ensure reliable and efficient file data security in a transparent and convenient manner. We have taken this as a challenge and tried to solve the problem of file data security by integrating our proposed Secure File System into the kernel itself.

Today data communication is a modern technology that contains a powerful computer processor to exchange information. But brute force attacks are made to break the encryption techniques and these attacks are the main drawbacks of older algorithms. This abstract is concerned with the development of a secure messaging, file and image system based on cryptographic algorithms which are faster, better immune to attacks.

Secure messaging, file and image is a server-based approach to protect sensitive data from unauthorized access over the Internet. It is confidential and authenticated exchange by any internet user worldwide. Secure messages provide non-repudiation as the recipients are personally identified and transactions are logged by the secure email platform. Brute force attacks are made to break the encryption and they are growing so faster. These attacks are the main drawbacks of an older algorithm. But with added features, this algorithm will be replaced by other techniques that will provide better protection. In this abstract we are going to propose secure messaging, file and image system that is implemented by an encryption technique which is faster, better immune to attacks, more complex, easy to encrypt and many more advanced security features included.

PROJECT OBJECTIVE

The main objectives of the proposed system:

- To transfer message in a communication system securely.
- Android-based and web-based applications for secure messaging have been developed using cryptographic algorithms for the users to send their message between registered users on any organization securely.
- The application is supported through user authentication before sending a message. The proposed secure messaging system uses minimal processing with little overhead while maintaining security.
- The authentication of each user is made strong by storing sensitive credentials for each user by using Salt in the database.

- Encryption and decryption of the message are done by using the keyword mono-alphabetic substitution algorithm, which is based on Advanced Encryption Standard (AES).
- An eavesdropper that breaks into the message will return a meaningless message. Obviously, encryption and decryption are the best ways of hiding the meanings of a message from intruders in a network environment.
- The proposed secure messaging can be used in many areas with personal and company-wide sensitive data exchanges.
- For example, financial institutions, insurance companies, public services, health organizations, and service providers rely on the protection by Secure Messaging. This research work includes a background study and comparative analysis of existing systems.

TECHNOLOGY STACK:

PROGRAMMING LANGUAGES: JAVA, JAVASCRIPT, PHP, XML.

WEB APPLICATION DEVELOPMENT: HTML5, CSS3, BOOTSTRAP.

WEB APPLICATION FRAMEWORKS: NODE, ANGULAR.

DATABASES: FIREBASE, 000WEBHOST.

TOOLS REQUIRED: ANDROID STUDIO, VS CODE, ATOM.

ALGORITHM

STEP1: Initially with the help of Our Desktop and Android application actual file is going to be encrypted or decrypted.

STEP2: This encryption can be done by using SHA-256/SHA-512 algorithms, that algorithms can be implemented by using node framework.

STEP3: After encryption, we get the result as an encrypted file. A sender can send this encrypted file to the receiver with the help of PGP (PRETTY GOOD PRIVACY) protection.

STEP4: Whenever our file is encrypted it is sender responsibility to keep password and that password is encrypted by using PGP.

STEP5: There are a separate public and private key for all the user. This data is stored in a database for further verification.

STEP6: Every user is allotted with a separate cabin, it will reduce the ambiguity between the users.

STEP7: After a file is encrypted, it can be sent by selecting a particular cabin (cabin belongs to the receiver).

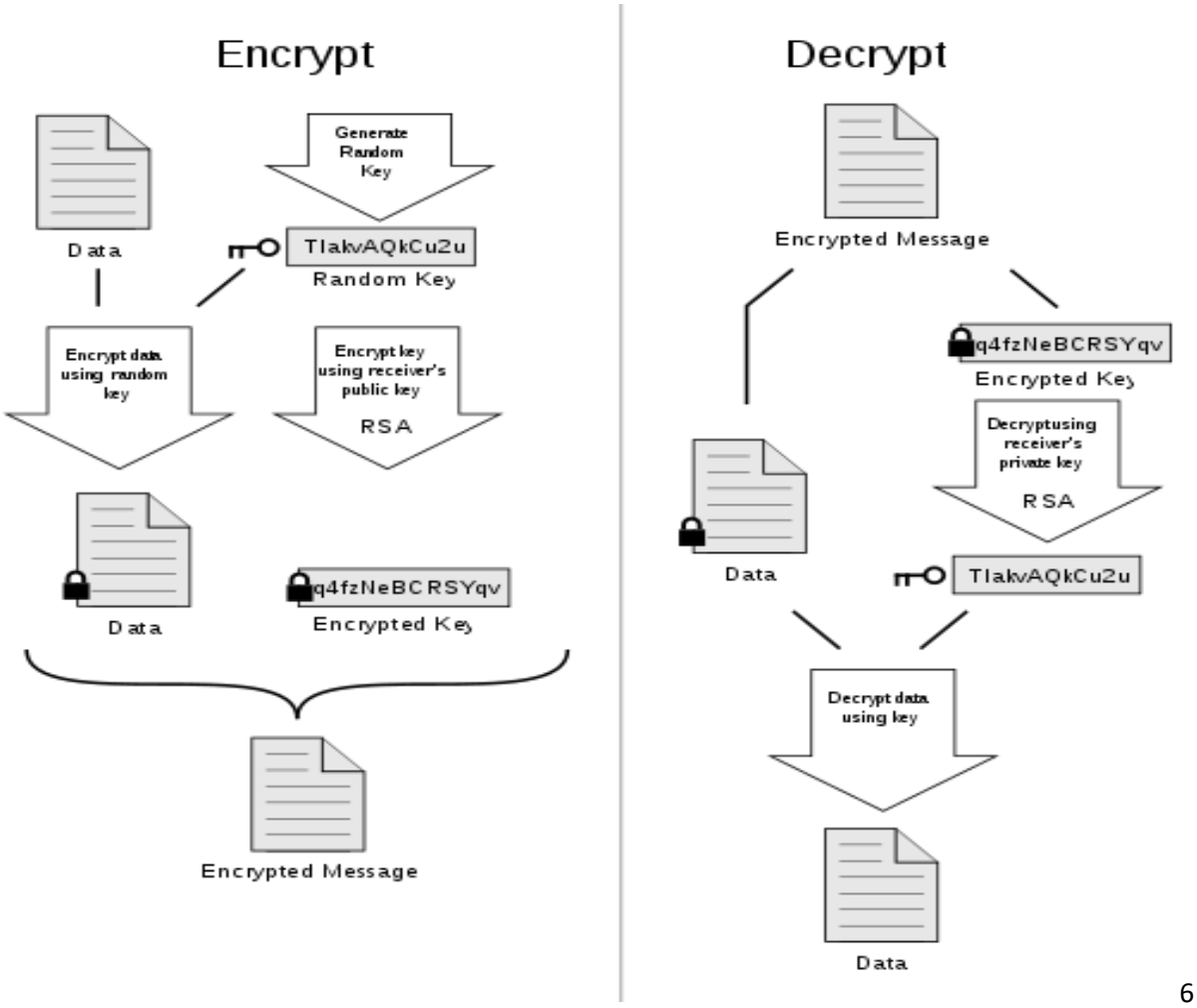
STEP8: The process will be the same for decryption also but the receiver just needs to decrypt it.

PRETTY GOOD PRIVACY(PGP)

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

- The main features of PGP are:
- Compatibility
- Confidentiality
- Web of trust
- Security quality

HOW PGP ENCRYPTION WORKS



.

HOW TO USE PGP

In order to use this functionality, the customer must provide LivePerson with a public key in the following format: RSA 4096-bit (below you can find the exact procedure for how to do that).

LivePerson will decrypt the original encrypted data using LP keys and re-encrypt it using the customer public key by using the following algorithm:

1. Symmetric encryption - AES-256
2. Digest - SHA-512
3. Compressed
4. Encoding the message on Radix-64 (armor format)

The customer will receive the Data Access files in the usual JSON format and will need to decrypt the encrypted data using the private key pair. Each encrypted record will come attached with the public key to help with tacking the right pair of keys.

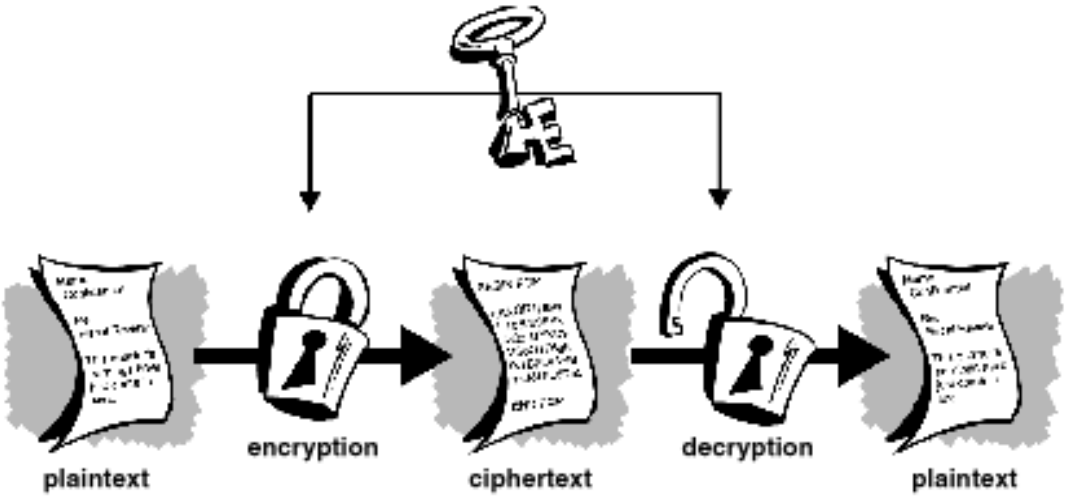
HOW TO CREATE A PGP WITH PUBLIC KEY

- PGP –version
- Verify you are using PGP 1.4.10 or higher
- PGP –gen-key -a
- Choose RSA (1)
- Choose key length 4096
- Choose key not expire (0)
- Input real name, email, comment
- Enter passphrase
- Verify your PGP is configured to avoid SHA-1

Once the key is created, please contact LivePerson support and pass it to them. They will need to validate it, to make sure it meets LivePerson security standards.

CRYPTOGRAPHY

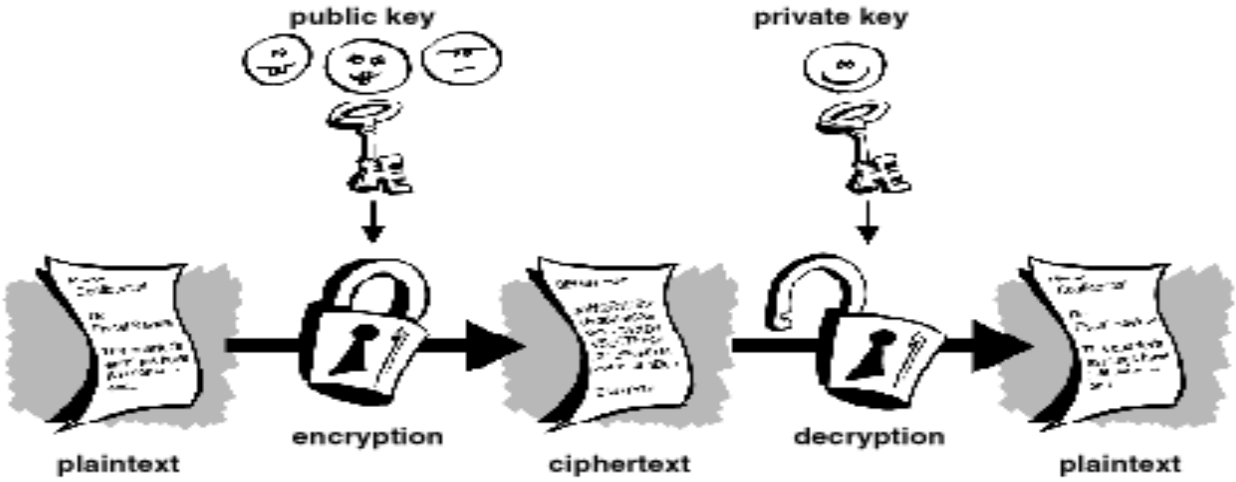
- Cryptography is related to computer security. It involves two processes which are encryption (scramble) and decryption (unscramble).



- In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.
- The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government. The above figure is an illustration of the conventional encryption process.

PUBLIC KEY CRYPTOGRAPHY

- Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. Even people you have never met.



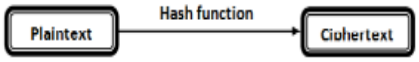
- It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.
- The primary benefit of public key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

Keyword mono-alphabetic encryption

A mono-alphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed. An affine cipher E(x) = (ax+b) MOD 26 is an example of a mono-alphabetic substitution. In a keyword monoalphabetic cipher, substitution characters are a random permutation of the 26 letters of the alphabet. To get the clear view once check out the Figure - 1.

(a) *Symmetric-key Cryptography: A single key for both encryption and decryption.*

(b) *Public-key Cryptography: A pair of keys, one for encryption and the other for decryption.*



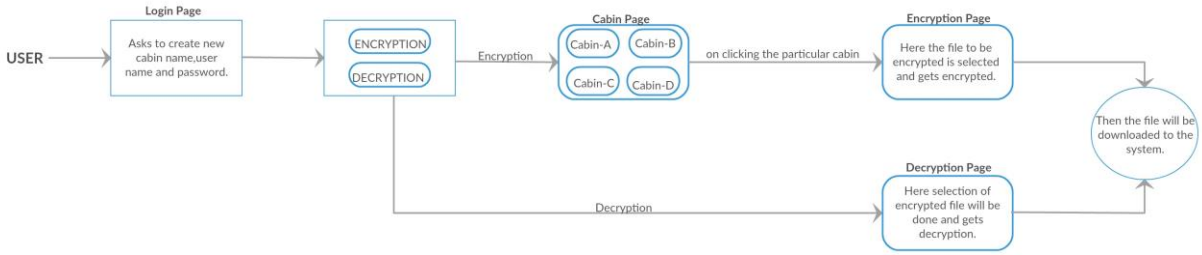
(c) *Hash function (one-way cryptography): Hash functions have no key since the plaintext is not recoverable from the ciphertext.*

Figure 1: Three types of cryptography: Symmetric-key, public-key, and hash function.

SOLUTION:

In this abstract we are going to propose secure messaging, file and image system that is implemented by an encryption technique which is faster, better immune to attacks, more complex, easy to encrypt and many more advanced security features included.

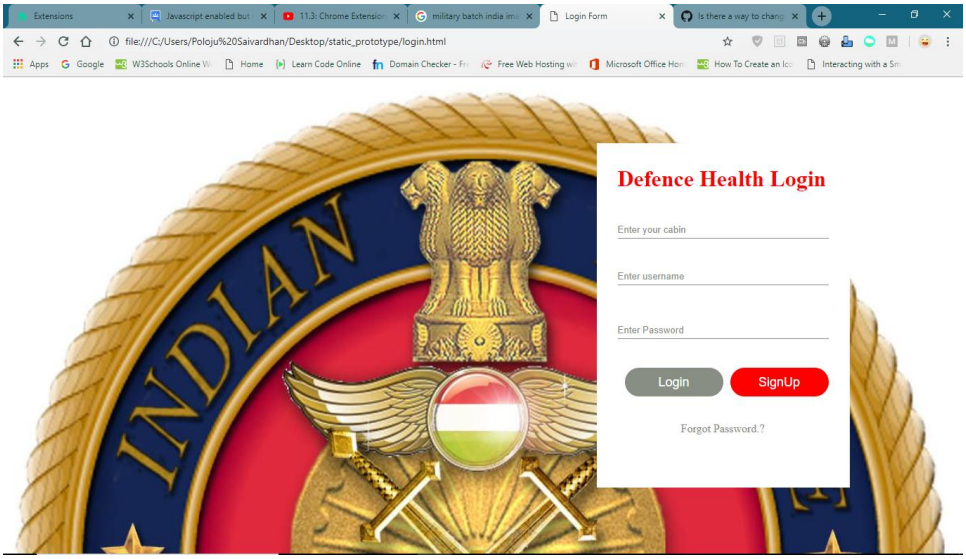
UML DIAGRAM:

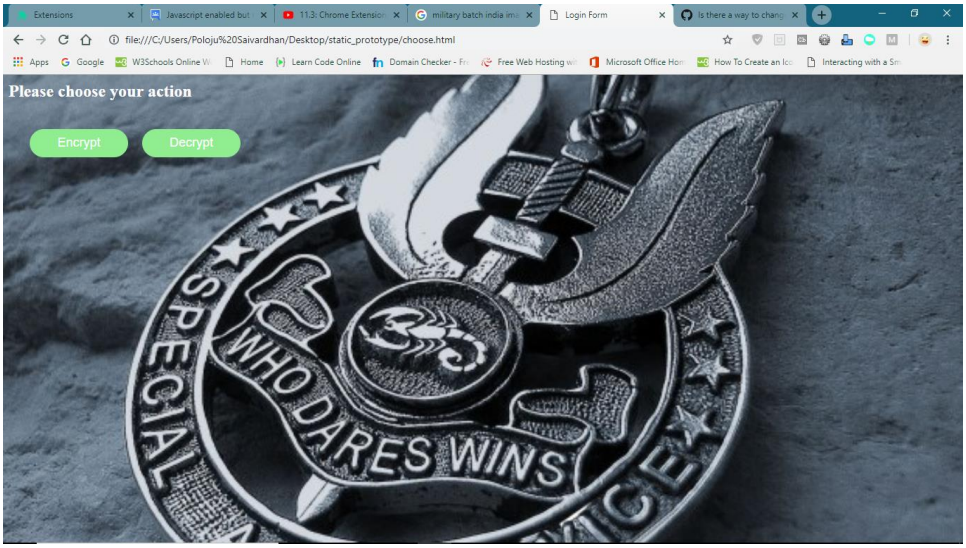


The defence user prompted to register cabin-name, username, and password. After registering is done, the user is provided with two options either encrypt or decrypt if the user selects encrypt option, a page will appear with different cabin-names, then the user has to

select an appropriate cabin-name to which the file has to be transmitted, the corresponding public key is fetched from the database. After this the user enters into a new page, where it requests the user to choose a file, by selecting the file it asks the user to set a password to make the encrypted file more secure and the password here again gets encrypted as a file. Now both the files get downloaded to the sender, the sender now sends the downloaded files to the receiver through the network. So, the receiver selects the decrypt option, then the page appears requesting the user to select the PGP password file, then Decrypts the file using the private key. To decrypt the file, Further accounts password is used to decrypt the message and the decrypted file gets downloaded.

WORKING PROTOTYPE:





***NOTE** The present working product is in alpha stage. Further the working product differs.