



Kabsography

¹Mr. Kaushik Karkera, ²Mr. Amit Chourasia, ³Mr. Sumit Ram, ⁴Mr. Bhavya Dobariya, ⁵Prof. Samarth Pandit

¹Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.

²Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.

³Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105

⁴Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayandar, Thane, India - 401105.

⁵Professor of Pravin Patil Polytechnic, Department of Information Technology, Bhayander, Thane, India – 401105

ABSTRACT-

There are many Increasing Threats to Data Privacy and Security During the Pandemic. More people than ever are being duped, and organizations are left more vulnerable to attacks as threats to data privacy and security noticeably continue to increase. This growing awareness is in response to increased incidences of cyber security attacks and data security breaches. This App allows a user to encrypt or decrypt text, images etc. After the files are encrypted, the user can download a .txt file of encrypted code and also generate QR Code for the encrypted text. A user can decrypt the encrypted text using a password used by a decryption Algorithms. To encrypt or decrypt any files the user must be logged into the system or a user must register himself into the system. The frontend of the app is designed using Android Studio and Firebase serves as a backend to store the user information.

INTRODUCTION

Cryptography is the process of encrypting messages and other data in order to transmit them in a form that can only be accessed by the intended recipients. It was initially applied to written messages. With the introduction of modern computers, cryptography became an important tool for securing many types of digital data. KABSography is a platform in which you can perform encryption and decryption of text and image on various tools such as Aes, Des, Binary and Caesar Cipher. Qr code Generator and Scanner to encrypt and decrypt text are available. You can also download encrypted text and image to your External Storage. By Using KABS Crypto You can also Learn Encryption and Decryption on various algorithm that is provided in our application KABSography also Provide you to Store your Encrypted Text in the Save encrypted text option.

LITERATURE SURVEY

Data at rest and in transit can both have their confidentiality and integrity guaranteed by cryptography. Moreover, it may prevent repudiation and authenticate senders and receivers to one another. Many endpoints, often several clients, and one or more back-end servers are common features of software systems. Data integrity is guaranteed by cryptography employing message digests and hashing methods. The receiver is ensured that the data received has not been altered during the transmission by supplying codes and digital keys to confirm that what is received is real and from the intended sender.

SYSTEM OVERVIEW

For implementation purpose, an application needs to be developed which will have a basic registration page asking for user personal information and a login page if the user changes his/her phone or uninstalls the application.

The user won't be asked to login every time except for the cases described above. Once the user logs in, our system will check whether the user is connected to a legitimate device installed at any student. Based on the device to which the user is connected our system would detect the source of the user.

When the user books for any services from our app, an appropriate amount will be displayed to the user account and if user books any service an acknowledgment would be sent to the service provider.

All the above information would be stored in a database which would be real-time i.e., altering every time the user reaches the destination the data entry of that particular seat would be changed.

Applications steps should be clear and actionable versus vague ideas or thoughts.

- Introduction Activity
- Created a Splash Screen
- Sign Up Activity
- Login Activity
- Main Activity

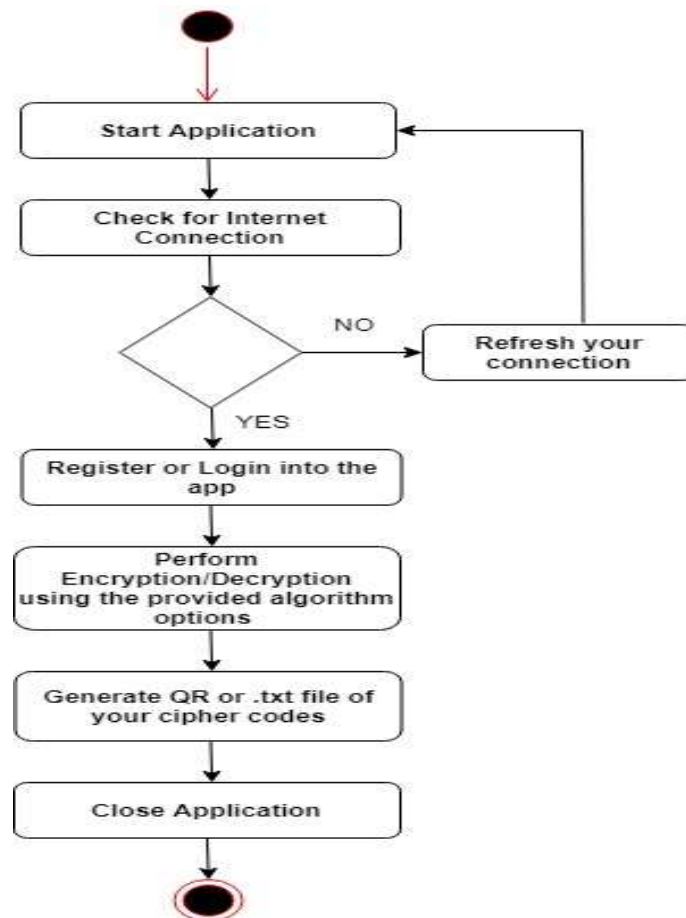
Making of Application Steps:

1. First we created a splash screen for user interaction and then we added registration activity by using firebase and then we added login activity
2. Now our Registration Activity is ready the data also get stored in firebase.
3. Now we created a Main Activity in which we have added different services like electrician, plumber, mechanic, Food Ordering, Hospitals, Animal Defense, etc.
4. After this we added booking activity in which user can book for their services.
5. An Acknowledgement will send to user as well as service provider.

METHODOLOGY

We have proposed an android KABS-Crypto Application which will secure user texts files and images from getting harmed or attacked by someone. It will help user to keep his/her text files safe and encrypted, so that unauthorized user can't go through the data. The app will have file encryption facilities for texts, files and images. This System will help a user securing his data from outside world and also allow him to share the encrypted data safely.

Activity Diagram :



PROBLEM STATEMENT

There are several encryption and decryption methods available today, particularly in the communication systems offered in a wide range of applications. Military communications and dependable security data to safeguard for transmission have a special influence on encryption and decryption. This cypher text is used in the military to transmit information such as orders, strategies, secret codes, and other data that the enemy country cannot obtain during hostilities. Making this system is the method by which the national enemy cannot detect information. Because this system uses a procedure to encrypt and decode data, the information cannot be recognised by a national enemy.

PRODUCT SCOPE

- Advanced cryptography algorithms for encryption.
- Image Encryption.
- Encryption/Decryption of user entered text
- QR Code generator of encrypted text
- QR Scanner to Scan encrypted Text.
- User can download a .txt file of his/her encrypted code.
- Guide for encryption/decryption algorithms / cryptography.
- User can save his/her encrypted text in the application.

SOFTWARE DESCRIPTION

ANDROID STUDIOS-

The official integrated development environment (IDE) for creating Android applications is called Android Studio. It integrates the code editing and developer tools from IntelliJ IDEA, a Java integrated development environment for applications.

Android Studio employs a Gradle-based build system, an Android emulator, code templates, and GitHub integration to assist application development for the Android OS. In Android Studio, every project contains one or more modalities that include source code and resource files. These modalities consist of Google App Engine modules, Library modules, and modules for Android apps.

To publish code and resource changes to an active application, Android Studio employs the Apply Changes functionality. A code editor offers code completion, refraction, and analysis in addition to helping the developer write code. The software created using Android Studio is assembled into the APK file and uploaded to the Google Play Store.

JAVA-

Millions of devices, including laptops, smartphones, gaming consoles, medical equipment, and many more, employ the object-oriented programming language and software platform known as Java. Java's syntax and principles are derived from the C and C++ languages.

The portability of Java is a key benefit while creating applications. It is relatively simple to transfer Java application code from a notebook computer to a mobile device once you have done so. The fundamental intention of the language's creation in 1991 by James Gosling of Sun Microsystems (later bought by Oracle) was the ability to "write once, run anywhere."

FIREBASE-

A backend-as-a-service is Firebase (Baas). It offers a range of tools and services to developers so they can create high-quality apps, expand their user base, and make money. It is created using Google's technical framework.

A NoSQL database application, Firebase stores data in documents that resemble JSON.

Different algorithms used in Encryption and Decryption.

1. TRIPLE DES

The original Data Encryption Standard (DES) algorithm was intended to be replaced by Triple DES, but hackers soon figured out how to easily break it. At one point, the most popular symmetric algorithm in the market and the recommended standard were both Triple DES.

The three separate keys of Triple DES each have a length of 56 bits. Although the entire key length is 168 bits, experts contend that a key strength of 112 bits is more realistic. While being gradually phased down, the Advanced Encryption Standard has largely taken the role of Triple DES (AES).

2. AES

The [Advanced Encryption Standard \(AES\)](#) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.

AES is largely considered impervious to all attacks, except for brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

3. CEASER CIPHER

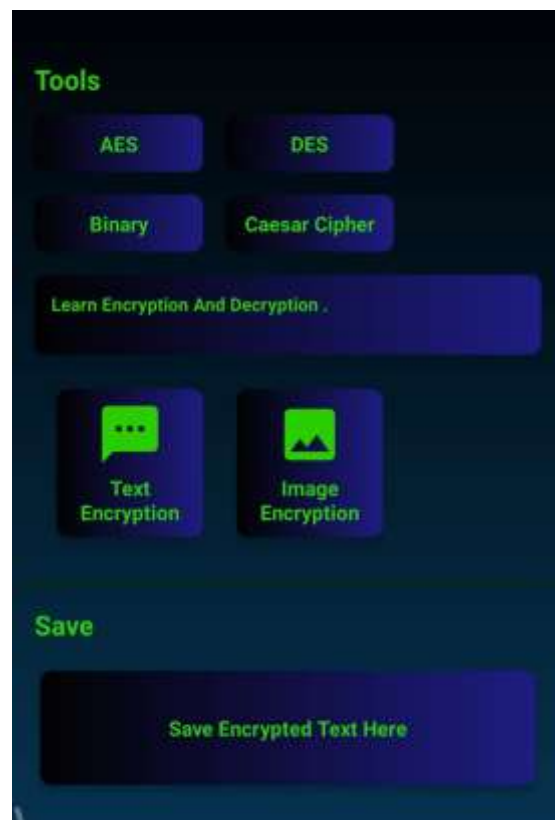
A well-known example of early cryptography is the Caesar cypher, which Julius Caesar is rumoured to have utilised. As demonstrated in Figure 5.1, the Caesar cypher is based on transposition and entails moving each letter of the plaintext message by a specific number of letters, typically three. Using the equal quantity of shifts in the opposite direction will enable the decryption of the ciphertext. Due to the continuous replacement of one letter with another, this sort of encryption is known as a substitution cypher.

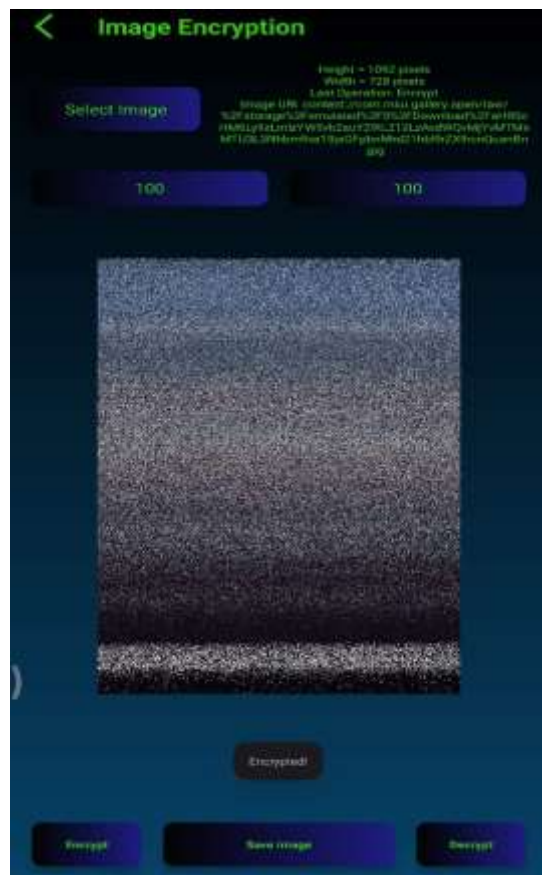
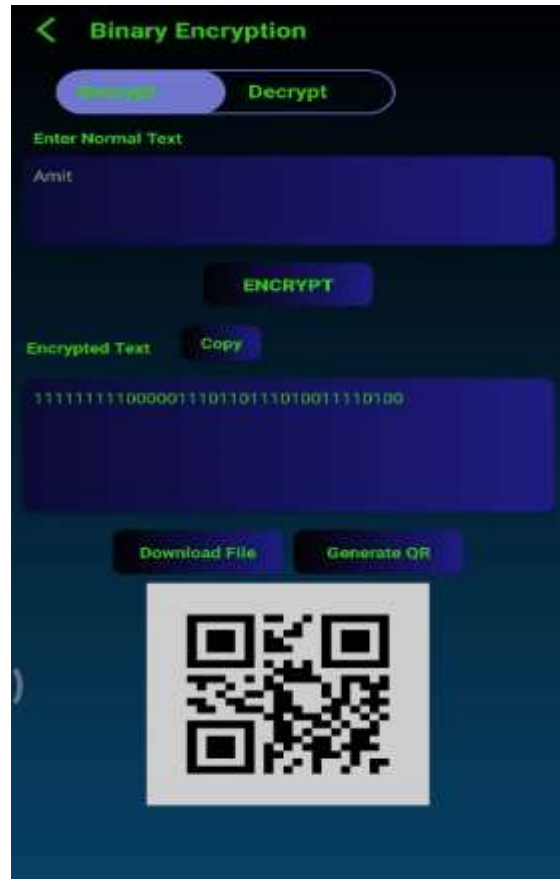
4. BINARY

On sorted arrays, binary search operates. An element in the centre of the array is first compared to the target value in a binary search. The element's location in the array is returned if the target value matches the element. The search continues in the lower half of the array if the target value is smaller than the element. The search moves to the top half of the array if the target value is larger than the element. This eliminates the half in which the goal value cannot lie throughout each iteration of the programme.

RESULT ANALYSIS

The KABSography's user interface has been developed. Individual can now encrypt and decrypt their data with full authentication. Their data is simultaneously kept in the database, and helps user to protect data from unauthorized user.





CONCLUSION

In this project we have designed an application which allows user to encrypt and decrypt text and images using cryptography algorithms. A user can learn how cryptography works through this app and will get basic knowledge on how for data hiding or encrypting works in security. It's a very good application which can be operated by any individual with a smart phone and KABS-Crypto installed in it.

FUTURE SCOPE

- File Encryption
- Cloud Storage
- Ray Crypto will be Available for IOS device.

REFERENCES

1. Beutelspacher, J. Schwenk, and K. D. Wolfenstetter. *Moderne Verfahren in der Kryptographie*. Vieweg, Wiesbaden, 1995.
2. E. Biham and A. Shamir. *Differential Cryptanalysis of the Full 16-Round DES*, Lecture Notes in Computer Science 740. Springer, 1993.
3. D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Well. *Coding Theory and Cryptography, the Essentials*. Marcel Dekker, New York, 2000.
4. D. Hankerson, A. Menezes, and S. A. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, New York, 2004
5. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996 (<http://www.cacr.math.uwaterloo.ca/hac>).