International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 1227-1229 www.ijaem.net ISSN: 2395-5252

Crypto Cipher

Bayyana Mahmood, Ekta Verma
Bachelor of Technology Student, Department of Information Technology.
Shri Ramswaroop Memorial College Of Engineeringand Management,Faizabad Road,Lucknow, Uttar Pradesh.
Bachelor of Technology Student, Department ofInformation Technology.
Shri Ramswaroop Memorial College ofEngineering and Management, Faizabad Road,Lucknow, Uttar Pradesh.

Submitted: 20-03-2022 Revised: 27-03-2022 Accepted: 30-03-2022

ABSTRACT
Smart Phone has become an important aspect of human life. Android is the most widely used operating system. Android operating system is an open source and freely accessible to everyone. Nowadays, mobiles contain various important android apps that are being used by people every now and then.With the enhancement of technology day by day, new apps are being launched daily in the market for varied purposes as per the increasing human demand. Human beings have made their life totally smartphone-centric. Having the least important things to the most important data,the users also havecertain data on the android devices that is to be handled with utmost security. Sometimes, the user has to transfer such data from his device to some other device.This data transfer has to be performed in such a way that the receiver receives the data without being tampered, in a completely protected manner.
The design and development of the android-based app named as 'CryptoCipher' enables the user to encrypt the data in the base-32 and base-64 format which can later on be decrypted by the desired receiver. This would make the data secured.

I. INTRODUCTION

In today's digital world, the data is being exchanged on the internet with so much exposure. It has consequently led to the serious problems of privacy of the data.

So, to solve this serious problem, security of the data is necessary. This is being done to prevent the data from being misused by third parties for fraud like scamming and identity thefts. For this purpose, encryption and decryption of the text can be done.

Here we introduce an android based application named CryptoCipher which has been specially designed to protect and secure the data from unauthorized users.

Encryption plays a significant role in securing various kinds of information technology (IT) sectors. Encryption is generally done to protect and secure the data in transit and data at rest. The main objective of encryption is to secure the confidentiality of digital data stored on computer systems or transferred over the internet or computer network. Encryption is the technique by which information or data is converted into secret and unreadable code that conceal or hide the information's pure meaning.[4]

The encrypted data can be converted into its original and readable form and this process is called as Decryption. Decryption is the reverse process of encryption. The encrypted information is decoded by the authorized users only because it requires a secret key or password to decrypt. This whole procedure of encrypting and decrypting of data and information is referred to as cryptography.

II. PROPOSED SOLUTION

A mobile application that's user centric and might be accustomed systematicallyaccess different functionalities. The user has to register once so can login anytime to whenever he/she wishes to use any of the features.

The app has interactive interface so as enhance the user experience and to draw in a bigger number of users. This app can connect with the database for storing the user record.

This is an Android application based on the idea of cryptography that will encrypt a text message and generate a QR Code out of it. The message would be encrypted as base-32 or base-64 text. This would convert the message in an unreadable format.

The receiver would receive the message in the form of codes which later on, could be transformed into a readable form by decrypting it.

The objectives of this android application are as

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 1227-1229 www.ijaem.net ISSN: 2395-5252

follows:

- To make the information secure by **encryption** and **decryption** to the **base-32** and **base-64** text.
- Generating a **QR code** for the data would also make it accessible to the desired people only
- To prevent the unauthorized access of data.

III. BASE-32 ENCRYPTION

Base-32 can be defined as a numeral system that makes use of 32 digits, each of which can be represented by 5 bits.
Base32 uses a way such that much smaller set of characters which has three main advantages:

- The resulting set of characters can be all in one case, which is favorable to case-insensitive environments.
- The resulting list of characters can be properly chosen to avoid similar-looking pairs of various characters, like 1 and l, so that resulting strings can be efficiently transcribed by hand.
- The resulting character set are often properly selected to avoid using any additional encoding or encryption when used as URL strings.

CryptoCipher application will encrypt the normal text into the base-32 format which could be later on decrypted by the same application after it reaches safely to its desired destination.

IV. BASE-64 ENCRYPTION

Base64 is said to be a binary-to-text encoding scheme. It represents binary data in an ASCII string format, that is printable, by translating it into a radix-64 representation.

Base64 encoding works with a 65-character subset of the US-ASCII charset. The first 64 characters out of the 65-character subset are mapped to the same 6-bit binary sequence (26 = 64). The additional 65th character (=) is employed for padding.

The Base64 encoding algorithm accepts an input stream of 8-bit bytes. It processes the input from left to right and arranges the input into 24-bit groups by concatenating three 8-bit bytes. These 24-bit groups are then taken as four concatenated 6-bit groups. Finally, each 6-bit group is converted to one character within the Base64 alphabet.

Base64 encoding is generally used when there is a need to transmit binary data over media that do not correctly handle binary data. Moreover, it is designed to deal with textual data belonging to the 7-bit US-ASCII charset.

After encrypting the text successfully into the base-64 format by using this android application, the text can be sent anywhere over the network without being tampered.

V. BASE-32 DECRYPTION

Base-32 decryption is same as themathematical base change. Each and everycharacter is referred to its 5-bit value in order to create a binary string. Then read the binary string as per the encoding used.
A Base32-encoded message

- comprisesonly of the characters 'ABCDEFGHIJKLMNOPQRSTUVWXYZ23 4567 =' (no 0,1,8,9)
- theoretically has a number of character multiple of 8.
- ends with 0,1,3,4 or 6 characters = (equal).
- has a length greater than 40 to 60% of the original message

VI. BASE-64 DECRYPTION

When decrypting Base64 text, four characters are naturally converted back to three bytes. The only exceptions are when padding characters are present. A single = specifies that the four characters will decode to only two bytes, while == indicates that the four characters will decode to only one byte.

Without padding, after ordinary decoding of four characters to three bytes over and over again, fewer than four encoded characters may remain. In this situation, only two or three characters can be left. A single remaining encoded character is not possible, because a single Base64 character has only 6 bits, and 8 bits are required to form a byte, so a least of two Base64 characters arerequired: The first charactercontributes6 bits, and the second character contributes its first 2 bits.

This process is embedded within the app that is used to decrypt or decode back the data when it reaches to the authorized receiver.

VII. QR CODE

A Quick Response (QR) code is a matrix barcode that is comprehendible by smart phones and mobile phones with cameras. They are sometimes called as 2d codes, 2d barcodes, or mobile codes. The QR code generally seem to be as a small white square with black geometrical shapes. Nowadays, colored and even branded QR codes are

being employed.

VIII. CONCLUSION

Mobile Phones have become an integral part of human life. Communication over the internet through various devices has become basic necessity of every individual, where the reliability of this data is to be maintained at any and every cost.
The android application entitled 'CryptoCripher' Will render to the security of data that is transmitted from one to another over the network. This app adheres to data guarding and user authorization so as to prevent the data vulnerability.

IX. FUTURE WORK

The future scope of this application consists of the following implications:

- Apart from text, the images, audios and videos can also be encrypted and decrypted in future.
- Along with base-32 and base-64, encoding to various other bases can be performed.
- The efficiency and the time complexity of the application can be enhanced.
- Can also be developed for iOS using Swift programming language.

REFERENCES

[1]. https://developer.android.com/guide/topics/security/cryptography
https://en.wikipedia.org/wiki/Base32
e32
[3]. https://developer.android.com/reference/android/util/Base64
[4]. https://www.ibm.com/docs/en/i/7.4?topic=functions-base64-decode
[5]. https://firebase.google.com/
[6]. Android Studio documentation for app developers –
[7]. https://developer.android.com/docs
[8]. Firebase Documentation - https://firebase.google.com/docs
[9]. https://en.wikipedia.org/wiki/QR_code