e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

PRIVATE MESSAGING SYSTEM WITH CHANNELIZING ENCRYPTION-DECRYPTION DOCTRINES

Abhay Patil*[1], Gopal R. Chandangole*[2]

*[1]Student, Department Of Computer Engineering, Zeal College Of Engineering And Research, Pune, India.

*[2]Asst. Professor, Department Of Computer Engineering, Zeal College Of Engineering And Research, Pune, India.

ABSTRACT

Encryption is the technique of swiveling a plaintext to ciphertext or the procedure of altering the confidential record/file to ciphered file to deter unauthorized individuals to gain passage to the classified information. Encryption is a greatly significant procedure for accomplishing data security. The technique of Encryption conceals the contents of a message in a manner that the original data is recouped only through a decryption procedure. The proposed module illustrates the Encryption/Decryption application of messages on android phones. For the working of this module, AES (Advanced Encryption Standard) algorithm is being employed. The proposed module works on the symmetric key mechanism i.e., for the encryption as well as for decryption methodology, the same key is being used. The sender creates a unique key to convert the message to its encrypted form and the receiver uses the same key to decrypt the ciphered message to its original form.

Keywords: Privacy Concerns, Encryption, Decryption, Plain Text, Cipher Text.

I. INTRODUCTION

The Data is the mortar that secures the presence of human existence. Consecutive information can be accomplished through encryption. The proposed paper is intended to cultivate message encryption and decryption on mobile phones. If we are ensuring classified data then encryption provides a high degree of secrecy for people and groups. However, the major objective of encrypting a message is not only to furnish confidentiality but also to procure outcomes for other dilemmas like data integrity, authentication, etc. Encryption is the technique that enables data to be transmitted in a secure form in such a way that the mere receiver can procure this data with the cypher key. To bring this section more significant, it must be associated with a distinct manifestation which is Mobile Phone. Mobile phones are employed for a variety of motives, including maintaining touch with family, administering businesses, and retaining access to a telephone in the event of a catastrophe. Many people carry an additional cell phone for different goals, such as for business and subjective uses. The fate of mobile computing is evolving even more exhilarating. There is an extremely elevated degree of attention in software development revolving around J2ME (Java 2 Micro Edition). J2ME is a slimmed-down edition of Java targeted at devices that have restricted recollection, memory, display, and refining power. However, this paper is concerned with a mobile phone as a beneficial tool in National Security Agency (NSA) Department. In cryptography, encryption is the modification of messages (or information) in cypher text in such a means that unauthorized users cannot browse it. In an encryption procedure, the memorandum or information (referred to as plaintext) is encrypted utilizing an encryption algorithm, swiveling it into an indistinct cypher text. This is usually done with the aid of an encryption key, which stipulates how the information is to be encoded. Any adversary that can glimpse the cypher text should not be competent to deduce anything about the initial message. An authorized party, however, can decode the cypher text using a decryption algorithm, which usually compels a secret decryption key that antagonists do not have a permit to. For specialized justifications, an encryption scheme usually requires a key-generation algorithm to randomly generate keys. There are two fundamental types of encryption schemes: symmetric key and asymmetric key encryption. In symmetric-key techniques, the encryption and decryption keys are similar. Thus, conveying parties must concede a private key before they wish to convey it. In Asymmetric-key methods, the encryption key and decryption key are diverse. One is a public key by which a sender can encrypt statements and the other is a private key by which a receiver can decrypt the information. However, only the receiving group has access to the decryption key and is competent in skimming the encrypted messages/files/data.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

II. LITERATURE SURVEY

The promising type of symmetric encryption is the Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), along the Rivest Cipher (RC4) algorithm. The past three are block cyphers while RC4 is an authentic cascade cypher [9]. The AES was invented as a substitute for DES and 3DES. It benefits key sizes of 128, 192, and 256 bits and a varying block length. AES is established on the Rijndael encryption algorithm. Rijndael is a block cypher approved as an encryption criterion by the U.S. administration, formulated by Joan Daemen and Vincent Rijmen. It has been evaluated largely and is now utilized internationally. During the examination of nominees for the AES standard, Rijndael was assessed by some of the world's promising cryptanalysts. It has substantiated to be very beneficial against known invasions, very worthwhile, and easy to enforce [6], [7], [9]. Rijndael funds a larger spectrum of block and key lengths; AES has a remedied block size of 128 bits and a key length of 128, 192 or 256 bits, whereas Rijndael can be specified with key and block lengths in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits [8]. This formulated research paper uses the AES cypher algorithm to conduct data encryption and decryption. The practice of the AES cypher algorithm enables us to catalogue the data in an abrupt encrypted form which consequently affects a small-size database. This implementation, therefore, deals with some of the wider problems put forward in the prior sending of an ordinary text message from one mobile phone to another mobile phone.

III. METHODOLOGY

The proposed methodology utilizes the Advanced Encryption Standard Algorithm (AES) for its working. The workflow involves the following steps:

- Sender opens the developed Android Application
- Message is being entered and the sender sets the unique 16-digit passcode as a key to encrypt the message content
- Sender clicks on the "SEND" button to send the message content to the designated mobile number
- The plain text message is converted to the encoded cypher text i.e., encrypted form and got delivered to the receiver's end side
- The receiver can only see the encoded message but not the plain text. To convert back to its original form, the receiver has to enter the same 16-digit unique key assigned by the sender
- Once key is loaded, the message gets converted back to its original form i.e., the message gets decrypt

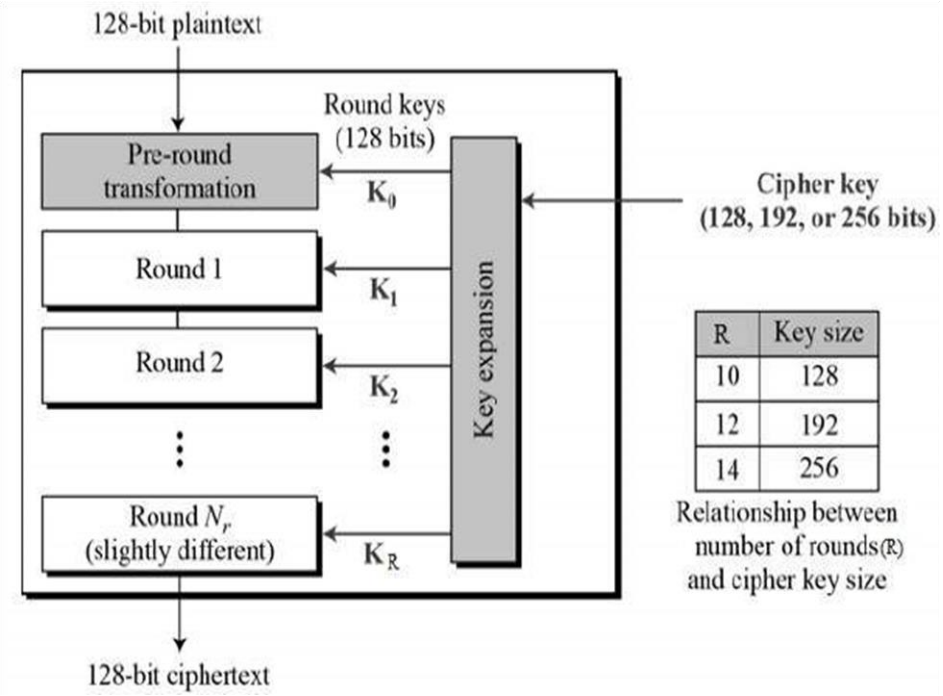

Fig 1: AES Algorithm Workflow

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

IV. MODELING AND ANALYSIS

The following are the screenshots of the proposed android project module:

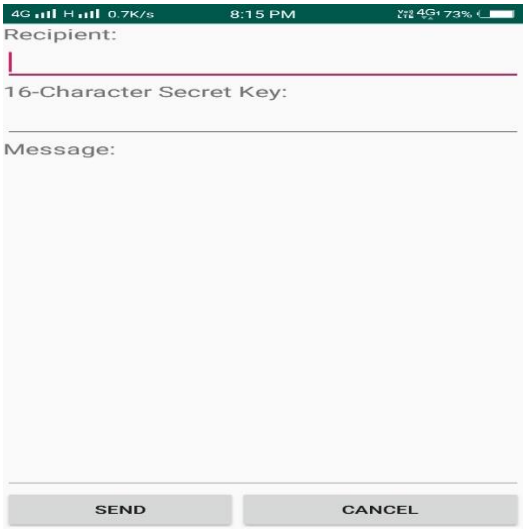

Figure 2: Opening Page UI

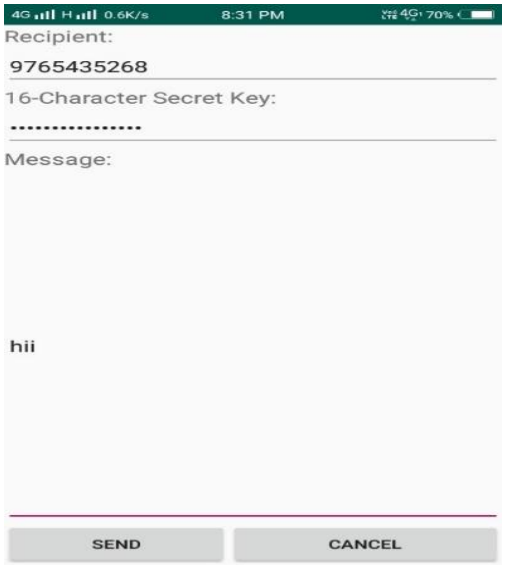

Figure 3: Entering Receiver Number and Key

Figure 4: Receiver's Side (Encrypted Message)

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

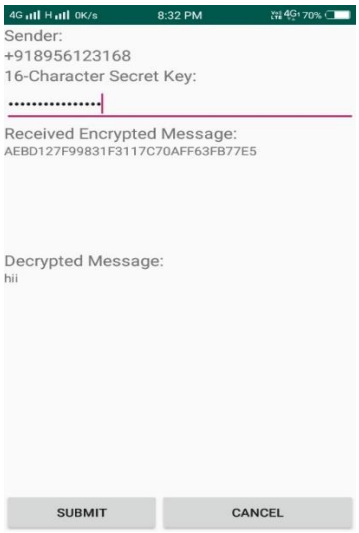

Figure 5: Receiver Entered Key (Decrypted Message)

V. CONCLUSION

This research endeavor has a ton of advantages to both private and public corporation and even people to protect their classified data on mobile phones. Based on the research so far, we bestow the subsequent recommendations:

- The formulated application/software should be utilized in a firm where their agency of sharing of data is primarily by text messages.
- Individuals should inaugurate this software on their mobile phones to compel the third party of accessing the private message.
- Those individuals that accomplish the transaction online via their mobile phones should install it on their phones for additional security.

ACKNOWLEDGEMENTS

Author wants to thanks all the professors of Zeal college of Engineering and Research, Pune for the support and assistance.

VI. REFERENCE

[1] Burnette, Ed. (2008). Hello, Android Introducing Google's Mobile Development Platform communications", Schweitzer Engineering Laboratories, SEL 2003 Inc. Pullman WA, USA.

[2] Heeks, R. (2008). Meet Marty Cooper – the inventor of the mobile phone, Accessed June,2013 from htpp://news.bbc.co.uk/2/hi/programmes, from IRKHS at International Islamic University Malaysia.

[3] Helen, F. (2009). "Cryptanalysis", Dover, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA

[4] John, M. (1973). Advance Development of handheld mobile telephone equipment, By Chicago Sun-Times, USA.

[5] Khurana, VG; Teo, C., Kundi, M., Hardell, L., Carlberg, M. (2009). "Cell phones and brain tumors: A review including the long-term epidemiologic data, US National library of medicine, national institute of health, USA.

[6] MMA,"Mobile Application", Mobile Marketing Association, Sept. 2008. 1670 Broadway, Suite 850, Denver CO, USA

[7] Murphy, L. (2009). A textbook "Beginning Android2", published by Apress L. P. USA.

[8] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. & Roback, E. (2000). "Report on the Development of the Advanced Encryption Standard (AES)" Computer security division information technology laboratory national institute of standards and technology administration, U.S. Department of Commerce, USA

[9] Risley, A. Roberts, J. & LaDow, J. (2003). "Electronic security of real-time protection and SCADA,

Western Power Delivery Automation Conference spokane, Washington, USA

[10] Sanadhya, S. & Sarkar, P. (2009). A new hash family obtained by modifying the SHA-2 family. ACM Symposium on Information, Computer and Communications Security, ASIACCS, Sydney, Australia Tetfund Sponsored Kwara State Polytechnic Journal of Research and Development Studies Vol. 5. No. 1 June 2017.

[11] Saylor, M. (2012). The Mobile Wave: How Mobile Intelligence Will Change Everything. Perseus Books/Vanguard Press, USA

[12] Yumbul, K. & Savas, E. (2009). Efficient, secure, and isolated execution of cryptographic algorithms on a cryptographic unit. ACM Proceedings of the 2nd international conference on Security of information and networks, Pages 143-151, Famagusta, North Cyprus.