**CRYPTOGRAPHY ASSIGNMENT PHASE-2**

**SECURITY OF END-TO-END ENCRYPTION IN MESSAGING SERVICES**

|  |  |  |
| --- | --- | --- |
| DEEPANSHU SAXENA | 2018A7PS0206U | Abstract, Conclusion,  Literature Survey, Implementation |
| ANUKRITI JAISWAL | 2018A7PS0254U | Problem Statement & Solution, Literature Survey, Implementation |
| AADILA JASMIN | 2019A7PS0801U | Introduction, Literature Survey, Formatting & References, Implementation |

**SECURITY OF END-TO-END ENCRYPTION IN MESSAGING SERVICES**

Aadila Jasmin, Anukriti Jaiswal, Deepanshu Saxena

Department of Computer Science Engineering,

Birla Institute of Technology and Science – Pilani, Dubai Campus

Academic City, Dubai, UAE­­­­­

# **ABSTRACT**

The growth of messaging applications and sharing multimedia is increasing at a great pace. With many convenient resources and advancements in technology, different messaging apps are made available and have replaced the traditional methods of communication. But along with advanced technology, the malware practices have also increased and no data is safe. Therefore, with the trend of instant messaging applications and growth in their use, security and confidentiality of data being transferred is very crucial. It is the right of the user that the information which is being shared, should remain confidential between the sender and receiver, and no third party should have access to them. End-to-End encryption is used to secure data, this method allows only the sender and designated receiver to view the information in plain-text form while the message is sent in encrypted form blocking the third parties from viewing or manipulating it. Our solution aims at solving the existing issues such as backup intrusions and spreading of fake news. In this paper, we have tried to find the security issues with end-to-end encryption techniques and have explored solutions to make the method more efficient in order to get more reliable results.

**1. INTRODUCTION**

In today’s world, it has become almost impossible to live without messaging applications. From sharing images to sharing information about work, we use several messaging applications every single day of our lives and have become dependent on them. There is a massive surge in the popularity of Internet data-based messaging applications like WhatsApp, Signal, Telegram etc. Text messaging has become the preferred mode of communication when compared to calls and in-person communication. The reason for the increasing usage of messaging applications could be the convenience of the applications, the ease of communication, widely available internet access etc. [1]. Instant messaging applications are undoubtedly one of the most popular applications among users. Hence, the security of these applications and the confidentiality of the messages sent using them is extremely important. With improving technology, hacking and stealing of data has become very common and messaging applications are not exempted from this. Besides this, several applications falsely claim that the user’s data is secured and governments of several countries also track their citizen’s information [2]. Several Cryptographic algorithms can be used to secure the data (in order to protect the different aspects of information security) that is being sent in these messaging applications. End-to-End encryption is a popular method that is used by several applications for security reasons. In end to end encryption, only the sender and the designated receiver can view the plain text data, the message is transmitted in the encrypted form which cannot be understood by intermediate or third parties. End-to-End encryption on systems depends on the mode of communication followed in the system. For example, the aim of end-to-end encryption on a client-user system would be to protect the data from the server that is making the communication possible. The commonly used encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest Shamir Adleman (RSA) [3].

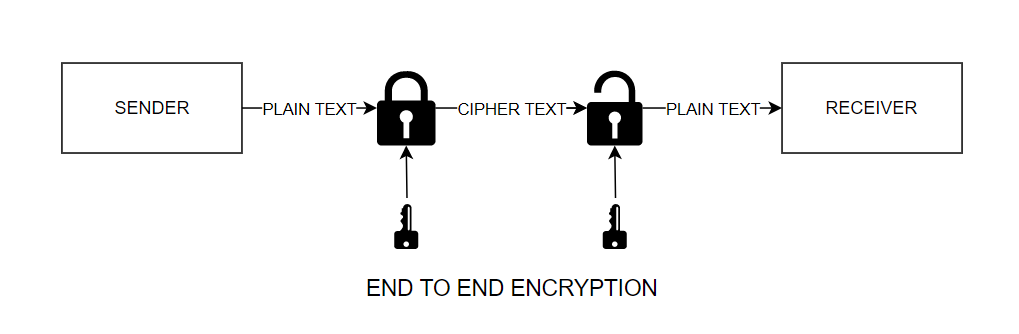


Figure 1 END-TO-END ENCRYPTION BLOCK DIAGRAM

In this paper, we analyse the security issues associated with end-to-end encryption in messaging applications and propose an application that has high level security. In section 2, we have performed a literature survey of the related work. In the section following it, we have explored the problems and possible solutions to improve messaging services.  Section 4 discusses the implementation and results obtained from our work. The last section will conclude the work with final observations and future work.

# **2. LITERATURE REVIEW**

Initially, WhatsApp sent messages as plaintext, i.e. without encryption that led to serious security issues. This led them to adopt a 256-bit algorithm for encryption in 2012 [4]. In 2016, WhatsApp followed the Signal protocol to implement End-to-End encryption(E2EE). This ensured that no third parties, not even the provider itself could access transmitted messages. All government interference and surveillance of information flow was also dropped [5]. Downsides of end-to-end encryption include the inability to moderate content. Many law enforcement firms across the globe have expressed their concern over the rising issue of child exploitation and abuse over texts. Hence, tech giants such as Google and Facebook now use machine learning classification algorithms to detect harmful content on applications [6]. While E2EE safeguards against eavesdropping and ensures privacy, it restricts government organizations from intercepting anti-national and terrorist communications. In 2013, Skype was revealed to have a “backdoor”, contrary to its claim of a secure end-to-end encryption [7]. Several cryptographic tools such as Tor and off-the-record messaging have emerged and failed due to failure in message delivery and complex key usage. In [8], a pre vs. post MME (Mass Messenger Encryption) survey was conducted to compare human sentiment towards SMS and WhatsApp in 2015. An Advanced Secure Messaging Application(ASMA) was proposed in [9] that would allow users to control the usage of data by specifying exactly how it can be shared or modified by future recipients. Moreover, a fact-checking mechanism would ensure all forwarded messages and news to be credible, hence limiting the spread of fake or harmful content. Another method used for encoding is the Most Significant Bit (MSB) method used to insert a message from the sender into the leftmost bit of the image pixel. The text is inserted using a Linear Congruential Generator and the image is further compressed using a Fibonacci code algorithm. However, this is not feasible for large input texts as a significant increase in running time and image distortion may be observed [10]. Data security is one of the most important concerns of people around the globe using the internet in this era. It makes sure that the content which is being transferred by the sender is accessed only by the intended recipient and there are no modifications or alterations in data on the path. In conditions like these cryptography algorithms are used that help to encrypt the files which cannot be read by human eye without the help of decryption algorithms and maintaining security [11]. Encryption is the process of converting plain-text into cipher text so that it cannot be understood or altered easily by people other than the designated ones. It is also referred to as the science in mathematics of encryption or decryption operations. There exist many different algorithms to perform this and encrypt or decrypt the data [12]. The conversations on messaging applications not only include texts but many other forms like images, videos, gifs etc. and hence we need to encrypt them as well for security reasons and there are different techniques of doing that. First one is (3, 3)*-* Extended Visual Cryptography Techniques (*EVCT)* in which first share contains *Red* component, second contains *Green* component and third contains *Blue* component of the secret image. These shares on the receiver side are needed to reconstruct the secret image sent. Second technique is (2, 3)*-EVCT,* in which any 2-out-of-3 shares are needed to recover the original secret image on the receiver side. Out of these shares, the first share contains the *Red-Green* components, second contains *Green-Blue* components and third contains *Red-Blue* components of the secret image. The techniques proposed above are safe, less complex and lossless in nature. The shares in both the techniques are most important as they are used to discover the original image on the receiver side [13]. There are different applications of cryptography in different aspects and a technique called Elliptic Curve Cryptography (ECC) is trending various application fields like sensor network, network security, authentication, signature verification and in the different applications of the internet of things (IOT). In message encryption ECC is useful but not for large input texts and hence a couple of algorithms are proposed in this paper that convert input message to elliptic curve point for efficient computational cost and communication cost [14]. With advancements in technology there are requirements of better and secure algorithms for most security of data being exchanged through electronic systems. In the growth of multimedia, image security is a major issue and many complex techniques have been used in cryptography. There is one technique proposed for image security with random selection and Blowfish algorithm. The results calculated are better than the standard methods [15]. Similarly, like security, storage is also an issue with the growth of multimedia. Another technique is Visual Cryptography (VC) which is used to hide the information available in images. It is a special technique of encryption which is decrypted with the help of human visual systems. This method uses simple Least Significant Bit (LSB) substitution which is an essential concept of the technique. The method proposed in the paper uses Cuckoo Search (CS) that finds an optimal solution to cover the entire image that is presented by transforming the message in every block as opposed to finding a single optimal matrix for substitution. The results outperformed all the Joint Photographic Experts Group (the JPEG) and the Joint Quantization Table Modification (JQTM) based method in terms of quality of image, security level and embedding capacity [16]. There are a few hybrid methods also used for encryption of data which have given secure results. The technique uses a multi-layer encryption of hybrid Advanced Encryption Standard (AES) 256-bit algorithm and Hidden in Plain Sight (HIPS) image hiding technique. The application has been verified and rated by ISO proving the technique to be really useful in encryption technique [17].  Several cryptographic algorithms are used in order to achieve end-to-end encryption, and they can be broadly categorized into two categories, Symmetric and asymmetric protocols. Data Encryption Standard (DES) designed by IBM is one of the most widely used symmetric algorithms in encryption procedures. DES is considered very strong against several analytical attacks. Ryndel V., Ariel Sison, and Ruji Medina suggested a method in their paper to further strengthen the DES algorithm by replacing XOR with another function [18]. However, due to its small key space, it is considered vulnerable and is being replaced by Advanced Encryption Standard (AES).  AES is considered as one of the most reliable ciphers, and is used widely in wireless communications [19]. Hardware based services can also be used to end-to-end encryption. A plugin was incorporated into Converse.js, an open source instant-messaging application. It triggers a web extension which determines the encryption and decryption of data and establishes a connection between the hardware cryptographic system and the software [20]. Prior to internet-based messaging applications, Short message services (SMS) were more commonly used. With the current scenario of advanced hacking, Rivest–Shamir–Adleman (RSA), AES, and International Data Encryption Algorithm (IDEA) are used to perform cryptographic manipulation on messages sent by SMS [21]. Signal messaging protocol, widely used in several messengers such as Facebook messenger, WhatsApp, etc. follows the concept of “perfect forward secrecy” and “post-compromise secrecy”. It follows the “ratcheting” technique where keys are updated in intervals to improve security [22]. Applications like WhatsApp, Viber and Signal follow different security protocols and have variations in their usability. Signal has high security, which can be improved by additional features such as notification on end-to-end encryption and two step verification. WhatsApp can avoid unauthorized access by adding the requirement for a passcode to open the application. Viber doesn’t notify the users when a change in cryptographic key occurs, this problem can be fixed by labelling the status of messages and notifying users when resets take place [23]. With information security being one of the biggest concerns in today’s world, strong cryptographic algorithms are essential to protect valuable and personal information from cyber criminals [24]. The paper [25] Nature discusses how WhatsApp uses algorithms and maintains high security between the users which cannot be breached by any outside interference or even the application itself. In paper [26], Nature  the major encryption techniques are discussed and their performance is compared for data security. The algorithms that have been studied and compared are AES, DES and RSA. The study shows that asymmetric algorithms are way faster than the symmetric encryption techniques and AES is the best algorithm among all 3 techniques.  Using algorithms such as MD5, RSA and Blowfish along with Structured Systems Analysis & Design (SSADM) and Object-oriented analysis and design method (OOADM) methodologies, a brute-force resistant encryption standard can be created that developers must use for end-to-end encrypted messaging services [27].

**3. PROBLEMS AND PROPOSED SOLUTIONS**

Although End-to-End encryption has levelled-up the concept of security in message applications extensively and has by far surpassed all its protocol counterparts, some major issues concerning security and content continue to arise. The first problem- E2EE protocol ensures that the sender’s message is encrypted as soon as the send button is clicked and is decrypted only at the receiver’s end. This way, the WhatsApp server never has access to the original message. However, if the recipient is offline, the message is decrypted and stays in the sender's device but is now accessible to the server and hence vulnerable to any kind of server breach [28], All Eve has to do is gain access to the cellular network and clone the sender’s WhatsApp. We can resolve this by using a single shared key that is not communicated through the server hence maintaining integrity as well as the messages will be decrypted once the receiver comes online and then stored in the backup storage so that even if it is some confidential data, it can be deleted from there and then accessed later in the storage. The second problem- most users tend to back-up their chats into some device location like drives. This data is stored in decrypted form and can be available to anyone with access to the user’s device. To avoid data compromise in such a situation, the application or the user must ensure that data is either stored in a secure inaccessible location or is stored in an encoded form or both. We have proposed a solution for the mentioned problem to create a storage option in the application itself so that the data will be stored there itself in the encrypted form and also the backup can be accessed only with a PIN that will be set by the user so that no one else can use that data even if the device is lost. Similarly, if someone tries to hack into the account for the storage database, the person will not be able to gain any information as the text will be stored in encrypted form and will change to plain-text only once the PIN is provided. We have also displayed this concept in our illustration through User Experience (UX) design. The third problem- although message transmission is done in the most secure way, there is no way to know how the recipient would use the data received. WhatsApp allows screenshots, screen recordings and message forwarding all of which threaten the very concept of privacy. In order to ensure that no data is used against the sender’s wishes, messaging applications must bring in a feature to notify both ends of screenshots taken and screen recordings to make sure they are aware of data being copied and saved. We have adopted a user specific approach to deal with this problem in our UX Design. In our prototype the users are made sure to be aware of every action that is taking place with their data or every activity they are performing on the received data. Hence both the sender and receiver gets the notification when any message is forwarded or a screenshot is taken. This maintains transparency between the users and accountability of information that is being shared. The fourth and last problem pertains to content moderation which is basically a downside of the E2EE protocol. Since, channels are unable to intercept transmitted messages, it becomes impossible for service providers to read or moderate content flow. This sort of freedom has led to the immense misuse of messaging applications and social media leading to child abuse, body shaming, fake news, etc. Such messages are forwarded time and again and therefore reach a larger crowd exponentially. To curb this, applications must enable features such as fact-checking and message hashing.  A fact-checker would run the forwarded messages against actual true news and allow forwarding only if it was true. Our prototype allows the app to take up the data only when the message is double clicked hence providing access only when the user allows it and hence the app verifies if that message is true or not as shown in the mock up. This helps improve authenticity of information and avoids false information transfer. Message hashing would store related content under the same hash key and stop the flow of information related to prohibited topics. Of course, this can only be done if the application is able to decrypt the messages on or during transmission, which would basically dissolve the idea of end-to-end encryption. Our prototype uses encryption techniques like AES and RSA algorithms that make the conversation secure and reliable for the users while it becomes very difficult for the eavesdroppers to access or manipulate the data that is being shared.

**4. SIMULATION, IMPLEMENTATION & RESULTS**

The implementation consists of two parts: A UX simulation of our suggested solution application and an RSA key generation, encryption and decryption code.

The UX simulation used the FIGMA design tool for prototyping and creating the application scenario (as shown in Figure 2). The code implementation was done in Python3 on the Google Colab platform. Python comes with a number of in-built cryptographic libraries with various functions. For our purpose, the Pycryptodome library version 3.10.1 was used. Our code generates a random number for the number of bits in the keys, done by the randomN() function. There is also a provision for the user to input the number. Other libraries imported include random, RSA, binascii and PKCS1\_OAEP. Next, both public and private are generated through RSA and extracted to be converted into ASCII (as shown in Figure 3). The encryptor takes as input a byte encoded plain text string and outputs the hexadecimal form of cipher text. The decryptor decrypts in the same format. The decryptor uses the initial public and private key pair in order to decrypt the cipher-text. The resulting plain text is in byte-encoded format. Our prototype shows the various security features that can be added to messaging applications. It includes a database storage to store the back-up data in decrypted form for higher security. It also shows how the encrypted data will look in the back-end. The prototype also gives the mock-up of how it will look when fake news is being circulated.

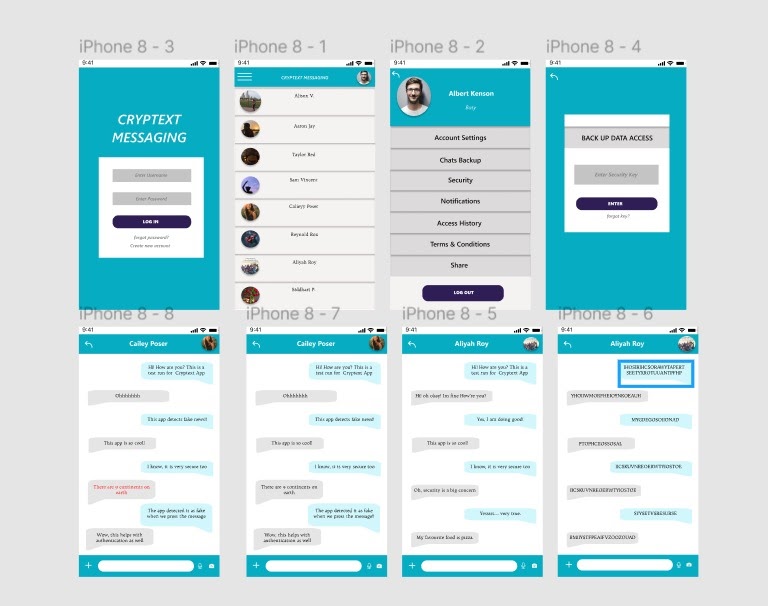


Figure 2 The UX Design for our Model “Cryptext” Messaging Application with various security features.

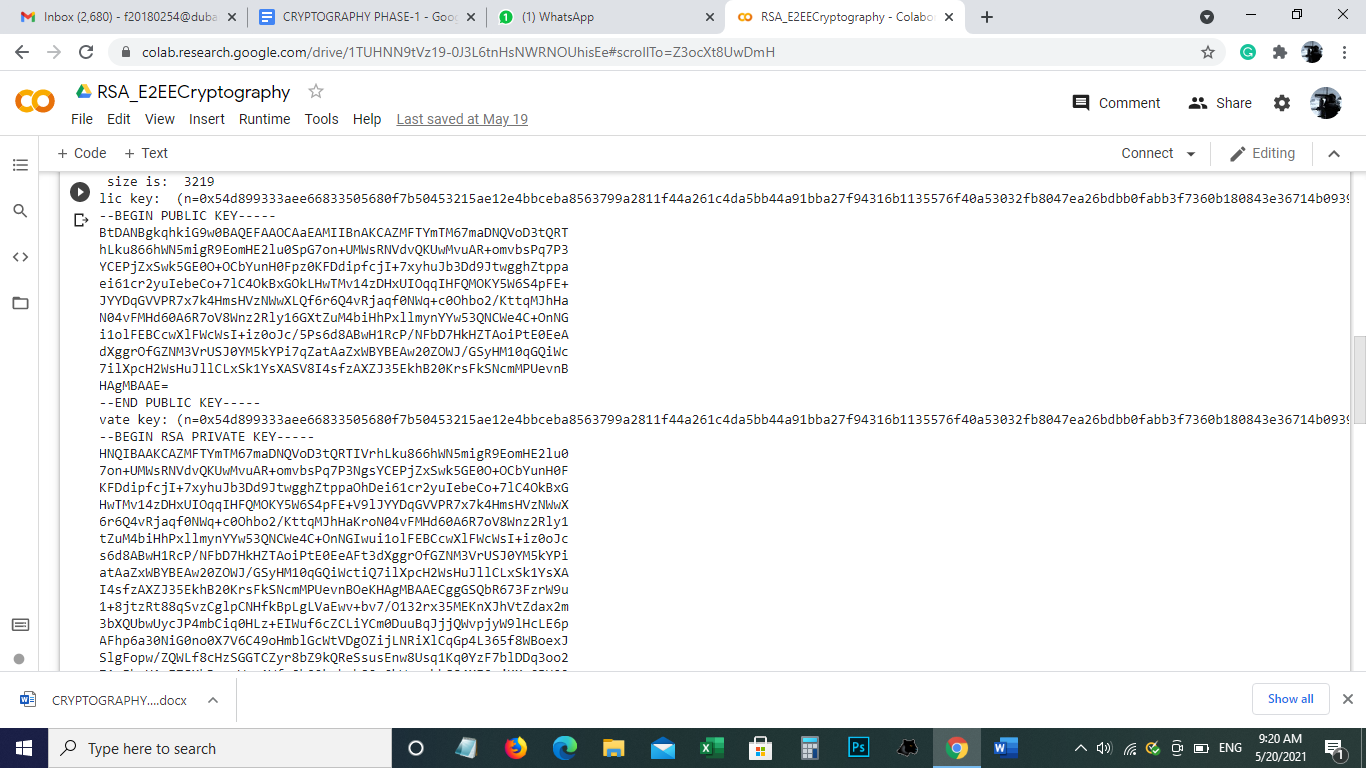


Figure 3 RSA Cryptography Algorithm Python Implementation showing Public & Private key in ASCII.

**5. CONCLUSION**

The technique of End-to-end encryption has improved their security concepts and surpassed the protocols for more secure passage of information transmission but there are still some aspects which threaten the confidentiality of the data being sent and received by the users. We have analysed and proposed solutions to these problems. The technique needs to maintain the security of information after it is sent till the time it is received by the receiver, hence we make sure the message gets decrypted only when the user is online. There are loopholes in storage and accessibility of the information even after it is received. Therefore, we created an in-built storage system which keeps the data safe and secure, always guarded with a PIN code. The sender will be more aware of the actions that are being taken on the information sent, and will have control over these actions. There is another major problem in this technique which is monitoring of content flow, checking it is not an easy task. It has been resolved with the help of methods like “fast-checking” and “message hashing” but these algorithms also impose a threat to the concept of end-to-end encryption technique. They basically allow the server to access the messages after once received so that a fast check can be run over and to verify the authenticity of the message. This threatens the motive of the end-to-end encryption system but we have also given a feature that this fast-check will be done only with the user’s permission.  At the global level, with increase in technology and simultaneous increase in cyber-attacks, measures should be taken to improve the security and storage results, as data integrity is really important but also on the other hand E2E encryption system is really strong in itself and provides high security to the data that is transferred through this encryption technique. In conclusion, end-to-end encryption has good security, however, there is always scope for improvement.

# **REFERENCES**

|  |  |
| --- | --- |
| [1] | B. L. S. D. E. W. &. V. K. S. U. o. C. F. Shannon K.T. Bailey, "Perceptions of Mobile Instant Messaging Apps Are Comparable to Texting for Young Adults in the United States," roceedings of the Human Factors and Ergonomics Society, 2016. |
| [2] | P. Dashtinejad, "Security System for Mobile Messaging," KTH Information and Communication technology, Department of ICT, Stockholm, Sweden, 2017. |
| [3] | H. Mohamed Nabeeltitute, "The Many Faces of End-to-End Encryption and Their Security Analysis," Qatar Computing Research Ins, 2017. |
| [4] | D. V. R. A. G. R. K. Maganti Manasa, "Encryption Techniques for Different Messenger," International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019. |
| [5] | S. S. M. S. K. Vamsi Krapa, "WhatsApp Encryption- A Research," International Journal of Recent Technology and Engineering (IJRTE), 2019. |
| [6] | J. Mayer, "Content Moderation for End-to-End Encrypted Messaging," Princeton University, USA, October 6, 2019. |
| [7] | R. E. Endeley, "End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger," Journal of Information Security , Capitol Technology University, Laurel, MD, USA , January 2018. |
| [8] | S. Dechand, A. Naiakshina, A. Danilova and M. Smith, "In Encryption We Don’t Trust: The Effect of End-to-End Encryption to the Masses on User Perception," IEEE, Stockholm, Sweden, 2019. |
| [9] | P. P. A. S. Ankur Gupta, "SMA: An Advanced Secure Messaging Application," Model Institute of Engineering & Technology, India, October 2020. |
| [10] | R. S. I. J. a. I. A. M Elveny, "Implementation of Linear Congruential Generator (LCG) Algorithm, Most Significant Bit (MSB) and Fibonacci Code in Compression and Security Messages Using Images," ICCAI, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Padang Bulan 20155 USU, Medan, Indonesia, June 2020. |
| [11] | A. M. Qadir and N. Varol, "A Review Paper on Cryptography," The Institute of Electrical and Electronics Engineers (IEEE), 7th International Symposium on Digital Forensics and Security (ISDFS), 2019. |
| [12] | S. K. G. Omar G. Abood, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, Department of Information Technology Institute of Graduate Studies and Researches, Alexandria University, Egypt., 2020. |
| [13] | S. S. K. Kirti Dhiman, "Extended visual cryptography techniques for true color images," ELSEVIER, Computer Science and Engineering Department, Thapar University, Patiala, Punjab-147004, INDIA, 2018. |
| [14] | P. Das and C. Giri, "An Efficient Method for text Encryption using Elliptic Curve Cryptography," IEEE 8th International Advance Computing Conference (IACC), Greater Noida, India, 2018. |
| [15] | A. Kaur and G. Singh, "A Random Selective Block Encryption Technique for Secure Image Cryptography Using Blowfish Algorithm," Second International Conference on Inventive Communication and Computational Technologies (ICICCT) , IEEE, Coimbatore, India, September 2018. |
| [16] | S. P. R. K. Gurunathan, "A stegano - visual cryptography technique for multimedia security," Multimed Tools Appl 79, 3893–3911 (2020), Springer. |
| [17] | N. M. M. I. P. D. L. T. Gemma D. Belga, "Hybrid Encryption Algorithm towards Secured Instant Messaging Application," International Journal of Advanced Trends in Computer Science and Engineering, April 2020. |
| [18] | A. M. S. R. M. Ryndel Amorado, "Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques," ICISS Proceedings of the 2nd International Conference on Information Science and Systems., 2019. |
| [19] | S. R. M. S. H. M. D. Md. Shafiul Alam Forhad1, "An Improvement of Advanced Encryption Standard," IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.11, November 2018. |
| [20] | R. D. O. A. G. D. O. A. F. L. L. D. M. W. G. R. T. D. S. J. ,. A. S. O. ABRIEL ARQUELAU PIMENTA RODRIGUES1, "Securing Instant Messages withHardware-Based Cryptography andAuthentication in Browser Extension," IEEE, 2020. |
| [21] | R. M. V. B. A. P. Shaik Quadar Janbee, "MS Encryption on Android Application," International Journal of Computer Sciences and Engineering, Andhra Pradesh, India, 2019. |
| [22] | C. C. B. D. L. G. D. S. Katriel Cohn-Gordon, "A Formal Security Analysis of the Signal Messaging Protocol," IEEE EuroS&P , Natural Sciences and Engineering Research Council of Canada (NSERC), July 2019. |
| [23] | A. M. H. A. J. N. Christian Johansen, "The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications," University of Oslo, 2018. |
| [24] | M. T. Gençoğlu, "Importance of Cryptography in Information Security," *IOSR Journal of Computer Engineering (IOSR-JCE),* Vols. ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 21, Issue 1, Ser. II, March 2019. |
| [25] | M. R. R. M. S. J. ,. M. ,. M. V. S. M. Y. M. N. P. S. Miss. Rachna Agrawal, "CASE STUDY ON WHATSAPP END TO END ENCRYPTION," International Research Journal of Modernization in Engineering Technology and Science Volume:02/Issue:04, April - 2020 , April 2020. |
| [26] | A. S. Dr. PRERNA MAHAJAN, " A Study of Encryption Algorithms AES, DES and RSA for Security," Global Journal of Computer Science and Technology, [S.l.], dec. 2013. ISSN 0975-4172.. |
| [27] | "Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm," Journal of Software Engineering and Applications 13(03):25-40, January 2020. |
| [28] | S. S. M. S. K. Vamsi Krapa, "WhatsApp Encryption- A Research study," International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019. |