IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Secure Text Transfer Using Doubly Encrypted Chat Application Based on Cloud

Simi Jain[1], Vaishali Nirmalkar[2], Bhagyashri Rewatkar[3], Archana Nikose[4]
Students, Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science and Engineering[5]
Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
simijain2000@gmail.com[1], vaishalinirmalkar0@gmail.com[2], bhagyashri132001@gmail.com[3],
nikose.archu@rediffmail.com[4]

Abstract: *One of the most important ways to preserve information security is to use cryptographic techniques. It provides digital signature, authentication, secret sub-storage, system security, and other capabilities in addition to keeping the information confidential. As a result, the encryption and decryption solution can secure information secrecy, as well as information integrity and certainty, to avoid tampering, forgery, and counterfeiting. The security of encryption and decryption algorithms is determined by the algorithm's internal structure and mathematical rigour, as well as the key secrecy. The key in the encryption algorithm plays a crucial role; if the key is released, anybody may use the encryption system to encrypt and decrypt data, rendering the encryption process ineffective. As a result, the encryption and decryption solution can secure information secrecy, as well as information integrity and certainty, to avoid tampering, forgery, and counterfeiting. The security of encryption and decryption algorithms is determined by the algorithm's internal structure and mathematical rigour, as well as the key secrecy. The key in an encryption algorithm plays a critical role; if the key is released, anybody may use the encryption system to encrypt and decrypt data, rendering the encryption technique ineffective. As a result, throughout the encryption and decryption process, the type of data you pick to be a key, how you disseminate the private key, and how you preserve both data transmission keys are all critical considerations.*

Keywords: Cryptographic Techniques

I. INTRODUCTION

The transfer of digital information has a tremendous influence on the way we live our lives, whether it's in the form of fundamental communications, banking transactions, or even driving our automobiles. Access to secure ways of privately communicating information becomes increasingly crucial as more information from our daily lives gets digital. In fact, the commercialization of o digital footprint has transformed information into a type of currency - and if information is a currency, privacy is the difference between keeping your money in the bank and freely giving it away.

Because robust cryptographic systems that can be practically implemented are difficult to develop, the history of cryptography has seen a very small number of big advances. As a result, when breakthroughs occur, they attract a lot of attention. Though RSA cryptography is now considered an outdated approach and is frequently supplanted by newer methods based on elliptical curves, it is safe to claim that its development was one of the most significant discoveries in cryptography. Learning how RSA cryptography works is a useful exercise that will expand your toolkit and improve your understanding of the modern world, whether you're interested in how blockchains work, the general history of cryptography, or even the practical utility of seemingly esoteric number theoretic results.

The goal of this article is to present RSA's inner workings in a sufficiently self-contained manner. It is anticipated that readers who are interested in RSA will be able to go through the essay and feel sure that they have a good understanding of how it works. Multiple intriguing mathematical findings are used to prove that RSA cryptography is legitimate. The goal of this page is to compile all of the relevant background mathematics in one place, including clear proofs for key findings, so that readers may get a self-contained overview of RSA

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

II. Literature Survey

There has been a lot of research in the field of message sending security using Cryptography. In 2014 Honda Talked about structuring communication with session types in concurrent objects and beyond. Iwamoto came up with a new model of client server communication under information theory security.

They used a symmetric key encryption system for providing the security during the transfer of messages. Chauhan in 2013, Talk about using public key encryption techniques that provide extreme secure chat environment. They used an RSA encryption system to encrypt and decrypt messages between client and server. Anjaneyulu in 2012 discussed Use of directed digital signature over noncommunicating division simmering. But the challenge they face was that digital signature certificate for every user may not be available in a chat environment where users may be added or revoked.

In 2014 Desmet Discuss about real time security on the web using radius encryption system. They concluded that though symmetric key encryption system has maximum performance but on the other hand public key encryption systems are are much more secure. Khanezaei Provided a Framework based on RSA and AES encryption algorithms for cloud computing services. Here RSA was used to transfer the messages and AES algorithm was used to store the messages on the cloud.

In 2017 Vollala Designed and RSA processor for concurrent cryptographic transformations. This was a mixture of Software and Hardware implementation of algorithm for faster encryption and decryption and key generation processors. In 2019 Rajesh and Sairam Used RSA algorithm based on cloud to implement big data and health care system.

III. System

To code messages modified with the projected chat entrance manner, an encryption algorithmic rule is used. This research is focused on creating a fresh new model for forming a personal electronic messaging network to send message contents between client terminals through a network/computer network. The chat electronic messaging environment demonstrated a high potential for hosting a real-time interactive interaction system that is protected by the RSA coding process.

Choosing the key size in RSA coding is critical because as the key size grows, the system's security level, the quality, and the resistance of encrypted text grows as well.

These advantages make it difficult to decode encrypted messages and crack passwords. Nonetheless, in addition to those, he time it takes to create a coding key, the time it takes to code text, and the amount of RAM used by the mobile device all rise. These drawbacks are issues that will have an impact on the application's effectiveness. As a result, the advantages and disadvantages of different key sizes should be evaluated, and the best-suited key size should be the most popular. The need for authentication mechanisms and coding algorithms will be critical to complete the talking and satisfy the aims of this client/server design research. The three primary steps of the RSA algorithmic rule for cryptography are Key Generation, Coding, and Coding. The procedure of creating keys for cryptography is known as the key generation stage. The keys created during this step will be used to code plaintext in the coding stage and decode cipher-text in the coding stage. The coding (encryption) stage is the process of encrypting messages so that only authorised individuals may read them. The message gets reincarnated as cipher-text as a result of encryption. The procedure of deciphering the cipher-text to generate the initial message is known as the coding stage.

3.1 Modules of Doubly Encrypted Chat Application

1. RSA And Double Encryption Module
2. GUI(Graphical User Interface) Module
3. Cloud Based Module

A. RSA and Double Encryption Module

It covers four types of RSA (Rivest-Shamir-Aldeman) algorithms: key generation, key distribution, encryption, and decryption. It is the process of transforming plaintext (ordinary information) into incomprehensible text (called ciphertext). Decryption is the opposite of encryption, i.e., going from incomprehensible ciphertext to plaintext. A cypher is a set of algorithms that work together to generate encryption and decryption. The algorithm and, in each case, a "key"

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

are in charge of the cipher's detailed execution. This is a secret (preferably known only by the communicants) that is used to decode the ciphertext. It is commonly a short string of characters.

It accepts user input for all key generation factors as well as the message. Long Message Lengths are achievable with this technique since it gives additional security. The RSA Model is based on the Discrete Logarithmic Problem (DLP). Encryption between user to user and user to cloud i.e Double Encryption which secure the Text from External hacker and cloud which can read private message.

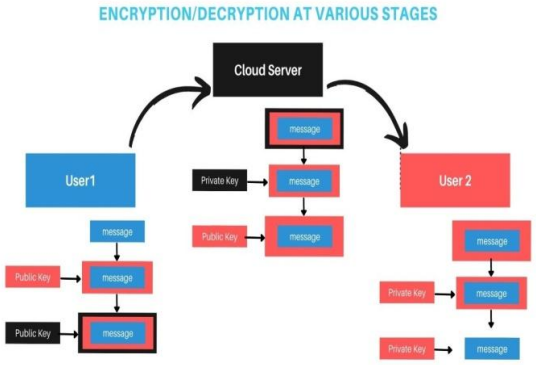


Figure: Encryption and Decryption At Various Stage

B. GUI (Graphical User Interface) Module

Instead of text-based user interfaces, written command labels, or text navigation, the graphical user interface (GUI) lets people to interact with electronic devices using graphical icons and auditory indicators such as primary notation. Command-line interfaces (CLIs), which require instructions to be entered on a computer keyboard, were established in response to the perceived steep learning curve of command-line interfaces (GUIs).

In the field of human–computer interaction, designing the visual composition and temporal behaviour of a GUI is a significant component of software application programming. Its purpose is to improve the efficiency and usability of a stored program's underlying logical design, a design discipline known as usability. To guarantee that the visual language used in the design is well-tailored to the tasks, user-centered design methods are utilised.

A graphical user interface (GUI) is a set of interactive visual components for computer applications. It shows items that provide information and reflect actions that the user may do. When the user interacts with the items, they change colour, size, and visibility. GUI (Graphical User Interface) is a visual experience builder for Java programmes that is simple to use. It is mostly made up of graphical elements such as buttons, labels, and windows that let the user to interact with a programme. The use of a graphical user interface (GUI) is critical for creating user interfaces for Java programmes.

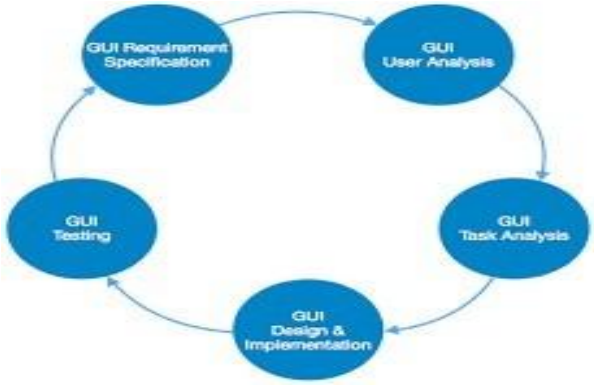


Figure: GUI Model

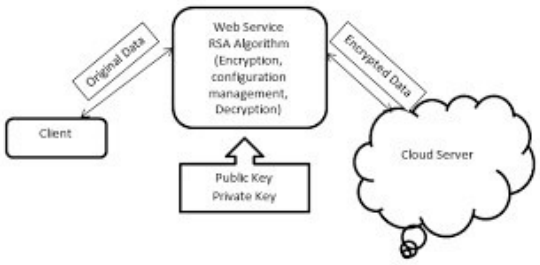
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

The main work is done in the client handler. It's difficult to send messages through a TCP socket. TCP does not have message boundaries; it is simply a stream of data. If you write 50 bytes to the stream, the application on the other end may read it as two groups of 25 bytes or 50 single bytes. There are two approaches to this issue. One method is for the client and server to be aware of the type of data being sent at any given moment and to read the right amount of bytes. Normally, you'd send the message type first, then the message bytes. The length and content of the information would be determined by the software reading data based on the message type.

The third option is to prefix any message sent via the socket with a message length. If you wish to send 223 bytes, for example, you write 223 as a 4-byte integer number, then the 223 bytes of data. On the other end, the application examines the 4-byte length and determines that it is 223 bytes.

Each method has its own set of benefits and drawbacks. When sending messages as bytes arrays, you must add the extra step of putting the data into the array rather than publishing it to the socket immediately. If you use context to determine the length of data, be sure that both sides of the connection are using the same format. In other words, if one side sends a message with an integer and a string, the other side should anticipate an integer and a string in return. It's impossible to recover if you transmit a message type that the other party doesn't comprehend. It has no notion how many bytes the message data contains.

Each technique has its own set of advantages and disadvantages. You must add the extra step of placing the data into the array rather than publishing it to the socket immediately when delivering messages as bytes arrays. If you're going to utilise context to figure out how long a piece of data is, make sure both ends of the connection are using the same format. In other words, if one side transmits an integer and a string in a message, the other side should expect an integer and a string back. If you send a message type that the other party doesn't understand, it's difficult to recover. It has no idea how many bytes are in the message data.



IV. METHODOLOGY

To code messages modified with the projected chat entrance manner, an encryption algorithmic rule is used. This research is focused on creating a fresh new model for forming a personal electronic messaging network to send message contents between client terminals through a network / computer network. The chat electronic messaging environment demonstrated a high potential for hosting a real-time interactive interaction system that is protected by the RSA coding process.

RSA (Rivest-Shamir-Adleman) Algorithm

The RSA algorithm (Rivest-Shamir-Adleman) is the foundation of a cryptosystem (a collection of cryptographic algorithms used for certain security services or purposes) that permits public key encryption and is commonly used to secure sensitive data, particularly credit card information. When it's sent via an insecure network, like the internet
Ron Rivest, Adi Shamir, and Leonard Rivest published the first public description of RSA in 1977.

The Massachusetts Institute of Technology's Adleman, through the introduction of a new department in 1973,the British mathematician Clifford Cocks' public key algorithm was kept secret by the NSA.GCHQ was the United Kingdom's intelligence agency until 1997.Asymmetric cryptography, often known as public key cryptography, employs two distinct yet complementary methods. One public and one private key are mathematically related. It is possible to distribute the public key with everyone, in contrast to the private key must be kept secret.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

How does the RSA Algorithm Work?

Alice chooses two prime numbers for her RSA keys: p=11 and q=13. n=p*q=143 is the modulus n. (n)=(p1)x(q1)=120 is the totient decides on 7 for her RSA public key(e) and uses the Extended Euclidean technique to calculate her RSA private key gives her a score of 103 Bob needs Alice's RSA public key (n, e) in order to send her an encrypted message, M. (143, 7). His plaintext message is simply the number 9 and is encoded as follows in ciphertext, C:

$M^e \bmod n = 9^7 \bmod 143 = 48 = C$

When Alice receives Bob's communication, she uses her RSA private key (d, n) to decode it as follows:

$C^d \bmod n = 48^{103} \bmod 143 = 9 = M$

To digitally sign a message with RSA keys, Alice would need to generate a hash — a message digest of her message to Bob — encrypt the hash value with her RSA private key, and include the key in the message. By decrypting the hash value with Alice's public key, Bob may verify that the message was sent by her and has not been tampered with. If this value matches the hash of the original message, then the message was sent by Alice alone (authentication and non-repudiation), and it is exactly as she wrote it (integrity). Of course, Alice might encrypt her message with Bob's RSA public key to ensure its confidentiality before transmitting it to Bob. A digital certificate contains the owner's public key as well as information that identifies the certificate's owner. Certificates are signed by a third party.

They are issued by a certificate authority, and they can make the process of obtaining one easier confirming the owner's public keys.

The RSA algorithm uses two keys: public and private. The public key is used during the encryption process, whereas the private key is utilised during the decryption phase. The computed 'N' value is used in both keys.

The steps in Stage 1: Key Generation are as follows.

- STEP 1: Choose any two huge prime numbers, P and Q, as your starting point.
- STEP 2: Using N = P * Q, calculate the values of N.
- STEP 3: Determine (r) = (P-1) *. (Q-1).
- STEP 4: Select E as the Public Key, with GCD(E, (r)) = 1.
- STEP 5: D * E = 1 * mod((r)) is used to calculate the Private Key D.

As a result, the Public Key component has the letters E and N, while the Private Key has the letter D.

Encryption Process (Stage 2) C = M E mod C = M E mod C = M E mod C = M E mod C = M E mod C = M E mod C = M E mod C = M E mod C = M E mod C (N).

Decryption Process (Stage 3) M can be used to locate plain text.

AES (Advanced Encryption Standard) Algorithm

AES is used for Message Encryption and Decryption.

The Advanced Encryption Standard (AES) is a symmetric block cypher that the United States government has chosen to safeguard confidential information. AES is used to encrypt sensitive data in software and hardware all over the world. It's critical for government computer security, cybersecurity, and data security.

When the National Institute of Standards and Technology (NIST) recognised the need for an alternative to the Data Encryption Standard (DES), which was becoming vulnerable to brute-force attacks, AES was born the newer, powerful encryption method would be unclassified, according to NIST, and would have to be "capable of protecting sensitive government information well into the [21st] century." It was designed to be simple to implement in both hardware and software, as well as in constrained settings. - such as a smart card — and provide adequate defences against a variety of attack methods. AES was developed for the US government, but it is also freely available for use in public or private, commercial or noncommercial encryption programmes. However, nongovernmental groups that choose to employ AES are subject to export control restrictions imposed by the United States.

How AES Encryption Works

Three block cyphers are included in AES:

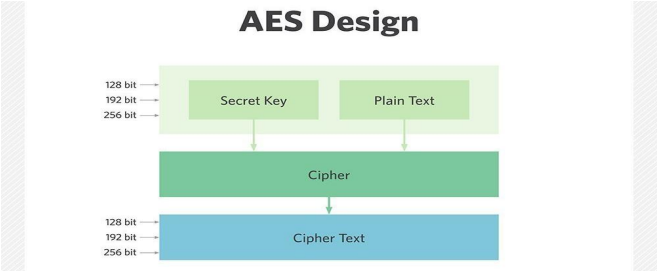
- AES-128 encrypts and decrypts a block of messages with a 128-bit key length.
- AES-192 encrypts and decrypts a block of messages with a 192-bit key length.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

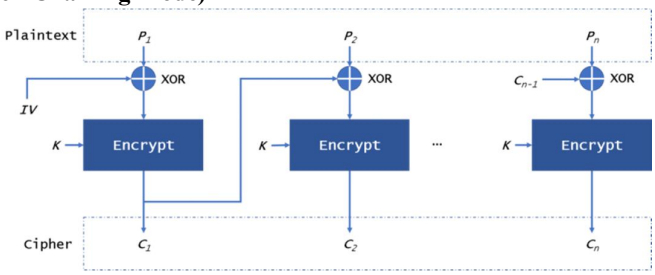
- AES-256 encrypts and decrypts a block of messages with a 256-bit key length.
- Each cypher encrypts and decrypts data in 128-bit blocks with 128, 192, and 256-bit cryptographic keys, respectively.

Symmetric cyphers, often known as secret key cyphers, encrypt and decode using the same key. Both the sender and the receiver must have access to the same secret key.Information is classified by the government into three categories: confidential, secret, and top secret. The Confidential and Secret levels can be protected with any key length. Key lengths of 192 or 256 bits are required for top-secret information.

For 128-bit keys, there are 10 rounds, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round consists of numerous processing steps that change the input plaintext into the final output of ciphertext, including substitution, transposition, and mixing.



CBC Mode(Cipher Block Chaining Mode)



The plaintext is separated into blocks, as shown in figure, and padding data is required. We'll start with the plaintext block xor and the IV. The result is then encrypted and written to the ciphertext block by CBC. We'll xor the encryption result with the plaintext block in the next block until we get to the last block. Even if we encrypt the same plaintext block in this mode, the ciphertext block will be different. We can decrypt data in simultaneously, but we can't encrypt data in parallel. A faulty plaintext or ciphertext block will affect all subsequent blocks.

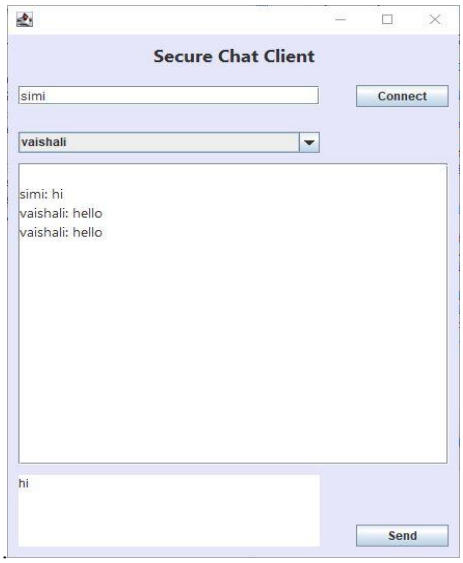
To attack the system, a Mallory can modify the IV. Even if a little part of the IV is incorrect,The data is incorrect. Mallory can use a padding oracle attack as well. They can pad the ciphertext block with a piece of ciphertext. This will return some plaintext-related messages. It's immune to CPA, but it's susceptible to CCA and PA.

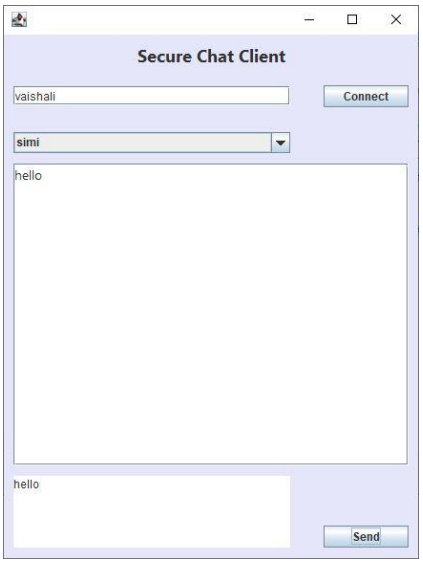
When encrypting 2((n+1)/2) we must modify the key to ensure security (n is the length of a block).

V. Experimental Results

Jframe is used to create a GUI (Graphical User Interface) interface model. When you're finished, right-click on the project and choose New — > Project. Select JFrame Form fromthe drop-down menu. Create two Jframe forms, one for the client and one for the server. Jframe is a programming language that is used to create a design for your application. It offers a straightforward configuration, comparable to that of ASPX pages. It also comes with a nice toolkit that includes drag-and-drop capability. Create two Jframes, Client.java and Server.java, and name them accordingly. Following that, the design is presented

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252





VI. Future Work

In our Feature Scope is to implement Group Messaging Chat Application by using JAVA Platform (Multicast Socket)

VII. Conclusion

This project will look at using the RSA (Rivest-Shamir-Adleman) algorithm to securely send text over the internet. To protect user-to-user and user-to-cloud data sharing in such a way that neither an external attacker nor the cloud itself can read the messages passed between the two users, key generation and encryption-decryption will be required twice.

References

[1]. Honda, K., Hu, R., Neykova, R., Chen, T. C., Demangeon, R., Deniélou, P. M., Yoshida, N. (2014). Structuring communication with session types.In Concurrent Objects and Beyond, pp.105-127,Springer Berlin Heidelberg.

[2]. Iwamoto, M., Omino, T., Komano, Y., Ohta, K. A new model of Client-Server Communications under information theoretic security. In Information Theory Workshop (ITW), pp. 511-515, 2014.

[3]. Chouhan, K., Ravi, S. (2013). Public Key Encryption Techniques Provide Extreme Secure Chat Environment. International Journal of Scientific & Engineering Research, 4(6), pp. 510-516

[4]. Anjaneyulu, G.S.G.N., Reddy, U.M. (2012). Secured directed digital signature over non-commutative division semirings and Allocation of experimental registration number,International Journal of Computer Science, Vol. 9, Issue 5, No. 3, pp:376-386.

[5]. Desmet, L.,Johns, M. (2014). Real-time communications security on the web. IEEE Internet Computing, 18(6), pp.8-10.

[6]. Khanezaei, N., Hanapi, Z. M. A framework based on RSA and AES encryption algorithms for cloud computing services. In Systems, Process and Control (ICSPC), 2014 IEEE Conference on, pp. 58-62, 2014.

[7]. Vollala, S., Varadhan, V. V., Geetha, K., Ramasubramanian, N. (2017). Design of RSA processor for concurrent cryptographic transformations. Microelectronics Journal, 63, pp.112-122.

[8]. Rajesh, M., Sairam, R., Big data and health care system using mlearningJournal of Recent Technology and Engineering, Volume-7 Issue-6S3 April, 2019.

[9]. Chandramouli, R., Iorga, M., Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In Secure Cloud Computing , pp. 1-30, Springer New York

[10]. Goshwe, N. Y. (2013). Data encryption and decryption using RSA Algorithm in a Network Environment. International Journal of Computer Science and Network Security (IJCSNS), 13(7), pp.9-13.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

[11]. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19), pp.33-38.

[12]. Rajanbabu, D. T., Raj, C. Implementing a reliable cryptography based security tool for communication networks.

[13]. In Science Engineering and Management Research (ICSEMR), 2014 International Conference on, pp. 1-4, 2014.

[14]. Lent, C. S. (2013). Learning to program with MATLAB: Building GUI tools. John Wiley & Sons.

[15]. Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Das, R. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm.In 33 Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual, pp. 332-337, 2017.

[16]. Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). Modified RSA encryption algorithm (MREA).In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pp. 426-429.