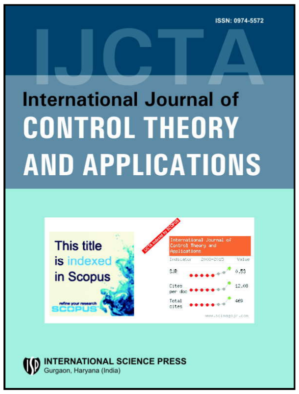

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 15 • 2017

Image Substitution Technique for Secret Message Transmission in Digital Communication

Devendra Prajapati[1], Anjana Pandey[2] and Varsha Sharma[3]

[1,3] Department of School of Information Technology RGPV, Bhopal, MP, India, Email- devendra.prajapati76@gmail.com, varshasharma@rgtu.net
[2] Department of Information Technology UIT RGPV, Bhopal, MP, India, Email- anjanapandey@rgtu.net

Abstract: Cryptography is a way to provide the security for secret message transmission. it provide several kind of techniques for secret message transmission such as substitution, transposition etc. these techniques has some drawback as when secret message travel on network that time it may be taken by someone and may be decrypted by crypto Analysis tools, because message contains the keys and encrypted message. In this research we provide a new mechanism which completely reduces that way of cryptography in which transmission message contains keys and encrypted message. By proposed technique, when secret message travel on network that time message has no information about keys for decryption and even not actual message. This technique used one spatial substitution method for encryption and two level encapsulation securities for cipher security. Main object is to develop strong technique for secret message transmission.

Keywords: Cryptography, Cipher, Substitution , Transposition, Asymmetric key Cryptography

1. INTRODUCTION

Cryptography [1] is a technique which provides the encryption for secure transmission of information on network. It converts the message format from readable to unreadable form or not understandable format. Cryptography used encryption message, keys, digital sign etc. for security purpose. It has a large collection of algorithms for cipher text generation such as substitution & transposition techniques, symmetric key & asymmetric key cryptography techniques etc. This cryptography is under development from its origin, because when it got some new way then it will more secure but after some time that will became general for others. Key Cryptography is two types of cryptography, symmetric and asymmetric key cryptography. symmetric key cryptography used only one key for encryption but there is one problem of key sharing between sender and receiver. In the asymmetric key cryptography there is used two keys for encryption public key and private key, when sender want to send message then sender used the private key for encryption and receiver's public key, receiver use private key for decryption.

Substitution technique [2] replaced plain text by other letters or any number or symbols. For Example Caesar cipher, hill cipher, mono alphabetic cipher etc. These types of techniques used the replacement of letter or symbols. This may used the word replacement in place of character replacements and may on several levels.

In Transposition technique[2-3], some sort permutation is performed on plain text. For Example rail fence method, columnar method etc. these types of techniques used the permutation on characters according to method, it may be line by line or place of letters and may be used some padding for encryption etc.

Steganography is a technique of cryptography which used the images, audio/videos for hiding the secret data behind it. In other words, this technique hides the data in images, audio, video etc for security purpose, for example if there is secret sort message then it may be encrypted in High Definition images when any one got this image that can see only image directly not the data or secret message.

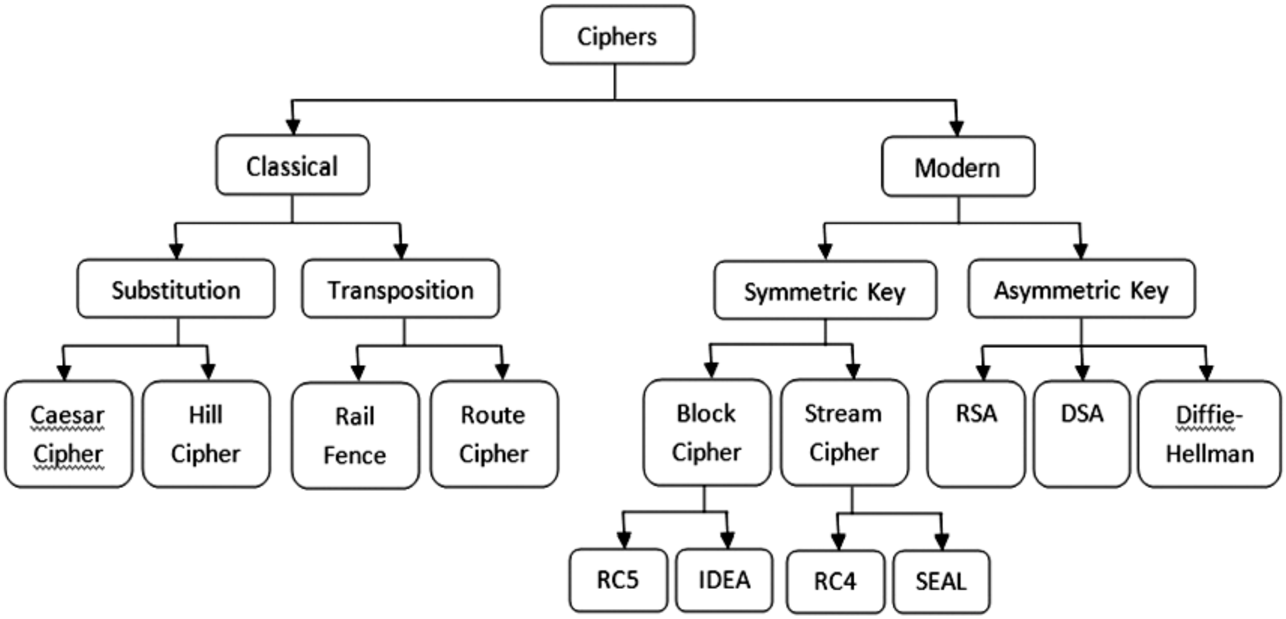

Figure 1: Classification of Encryption methods

1.1. Major Drawbacks of Convention Cryptography

1.1.1. Key Sharing & Size

Key [4] size is varying according to algorithms. The techniques which are using as asymmetric or symmetric cryptography, if key size is small then it may be cracked easily if long then it may take more time. Sharing is also a big problem in symmetric key cryptography because it required secure channel for sharing and in asymmetric key no one can absolutely sure about public key belongs to the person, and if private key is determined then attacker can read all messages.

1.1.2. Substitution & Transposition

In both techniques cipher text is a actual message and currently that is being the unreadable or non understandable but after cryptanalysis expert attacker may decrypt it.

The rest of the paper is organized as follows. Literature survey explained in section II. Proposed methodology and Experimental results are presented in section III. Concluding remarks are given in section IV.

2. LITERATURE SURVEY

*R. Bhanot and R. Hans [1]***:** Data security is exceptionally testing issue that touches numerous regions including PCs and correspondence. As of late, we ran over numerous assaults on digital security that have played with the privacy of the clients. These assaults simply broke all the security calculations and influenced the secrecy, verification, uprightness, accessibility and recognizable proof of client information. Cryptography is one such approach to ensure that classification, validation, uprightness, accessibility and distinguishing proof of client information can be kept up and in addition security and protection of information can be given to the user. Encryption is the way toward changing over ordinary information or plaintext to something endless or figure message by applying scientific changes or formulae. These numerical changes or formulae utilized for encryption procedures are called calculations. We have broke down ten information encryption calculations DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA and so forth. Among them DES, Triple DES, AES, RC5, BLOWFISH, TWOFISH, THREEFISH and IDEA are symmetric key cryptographic calculations. In this paper, investigated different encryption calculations on the premise of various parameters and contrasted them with pick the best information encryption calculation so we can utilize it in our future work.

T. Rubya, N. Prema Latha, B. Sangeetha [2]: Cryptography is the study of keeping private data from unapproved access of guaranteeing information honesty and confirmation, and it is the most grounded device for controlling against much sort of security dangers. Part of cryptography shows up in numerous secured regions like government offices, expansive banks, media communications organizations and different companies who handle delicate or military information. Quantum cryptography is a rising innovation in which two gatherings may at the same time produce shared, mystery cryptographic key material utilizing the transmission of quantum conditions of light. This paper comprises of the fundamental parts of quantum cryptography and it researches the data about where and all quantum cryptography happens.

L.Jothi [3]: Cryptography is that the watch and investigation of strategies for secure correspondence inside the nearness of outsiders. It furthermore plays essential of remote sensor systems. The cryptography disadvantage has tended to in a few connections and by specialists in a few orders. This expositive paper presents review of some of the freshest advancements on cryptography calculations in system security and moreover gives some of the answers for remote sensor arrange close by the outcomes.

Ijaz Ali Shoukat1, Kamalrulnizam Abu Bakar and Mohsin Iftikhar[4]: Movement in figuring forces and parallelism innovation are making deterrent for tenable security particularly in electronic data swapping under cryptosystems. A huge arrangement of cryptographic plans hold on in which each has its own particular positive and weak qualities. A few plans convey the utilization of long bits key and some bolster the utilization of little key. Commonsense cryptosystems are either symmetric or deviated in nature. In this meticulous look, the precise determination of right encryption plot matters for craved data swap to meet upgraded security targets. This study thinks about popular encryption strategies for persuaded determination regarding both key and cryptographic plan. Furthermore, this study presents two new encryption determination obliges which are ignored in past studies. At long last this far reaching study whip outs the most recent patterns and research issues upon cryptographic components to finish up prospective necessities identified with cryptographic key, calculation structure and improved security particularly in exchanging the sight and sound data.

Anupama Mishra [5]: the author proposed Caeser Cipher enhancement in this paper. The multilevel encryption is used to make cryptography more secure. Some techniques are used like multilevel row transposition ciphers , Encryption with some key with each level, Encryption with different key at each level etc. These techniques are more secure than other common techniques and when the messages will travel over networks, it is difficult to encrypted by Brute force attach and not possible to decrypted. Caeser cipher is simple type of cipher and mostly used transposition method. it is mostly combined with other technique the substitution and transposition, both methods are easily perform the encryption. The combination of these techniques provide more security and strong cipher so the final cipher text is more strong and difficult to break.

Kasish Goyal [6]: In this paper author present a modified caeser cipher algorithm. The algorithm required encryption key and plain text to encrypt the messages. It is based on modulo twenty six airthmetic. Decryption process follows reverse operation of encryption process. This process required a encrypted text and decryption key to provide the network security and data encryption techniques are used. The proposed technique is unique and further enhanced with combination of other algorithm.

Orooba Ismaiel [7]: In this paper author present a new algorithm based on substitution and transposition cipher for encryption. The algorithm delete some bits from plain text during conversion in binary code. After that the bits put in other place. The proposed algorithm is easy and it can be run in all programming languages. It worked with short and long text patterns.

Atish jain [8]: the author present a approach with shifted randomly by using the substitution and permutation techniques. These are implemented in modern encryption techniques such as blowfish, DES etc. the proposed algorithm encrypt a large range of characters in place of ceaser cipher. In this paper author present the weaknesses of ceaser cipher and transposition. A modified ceaser algorithm are proposed to reduced the limitations of traditional encryption algorithm.

3. PROPOSED METHODOLOGY AND EXPERIMENT RESULT

In existing techniques there are various variants of cryptography are presented. But in these techniques public and private keys are considered to provide encrypted message. Thus these techniques have the problem of key sharing between sender and receiver over network.

A new technique is proposed which resolves all the problem issues in existing techniques. The proposed technique is Image substitution technique which called ICipher or ImageCrypt.

In this proposed technique replace the letters by some other symbols as image (which is difficult to identify easily) and that will be the actual data in message rather than codes. These image symbols will travel on the network, in the place of real message or encrypted messages, it's a two level security so there is no information is available to the intruders or hackers for decryption purpose. If someone get the message than there is no option to decrypt it, because actual message will never travel on network.

3.1. Algorithm Steps

Step 1- Generate Real time data set of bitmap Images (I_i) { i=1,2,3……….n}

Step 2- Generate a table which contains all Letters (L_i) of a language. { prefer English language so generate a table which contain all alphabets of English language }

Step 3- Assign an Image (I_i) to each Letter (L_i) { Create a database which contain the letter with its corresponding bit map image }

Step 4- Compare the letter with its corresponding image if it is true than encrypt the message otherwise check letter with its image value.

Step 5- Generate ICipher (ImageCrypt) message {Encrypt the message by replacing the letters of code with its corresponding image}

Setp 6- Convert ImageCrypt message in zip format and Send ImageCrypt message in place of encrypt code.

Step 7- Stop the procedure

Example:

If there is message as "meet me tomorrow"

After the encryption message will be " "

Table 1
Example of Equalent Codes of Symbols

Collection of Symbols with Equalent Codes										
List of Symbols	0	1	2	3	4	5	6	7	8	9
Equalent Codes										

The process will start from message which is in readable form for example the message is “123” and we want to send it in encrypted form, so firstly, we will write this message and submit for encryption process. it will converted to encrypted message by encryption process and code images size are dot size , so it will look like as “ ” and finally we got the encrypted code or cipher code, this is not readable to others. After this encryption process we will convert it in rar or zip file for sending purpose. And finally we will send it to receiver then receiver will got (this sending and receiving process used the asynchronous key cryptography for security of message on network). this cipher text is in zip form so first it converted to unzip form and then by the decryption algorithm receiver can decrypt it in readable format as “123” with the help of imageCrypt.

The flow diagram gives the complete scenario of the experiment that how it is performed .

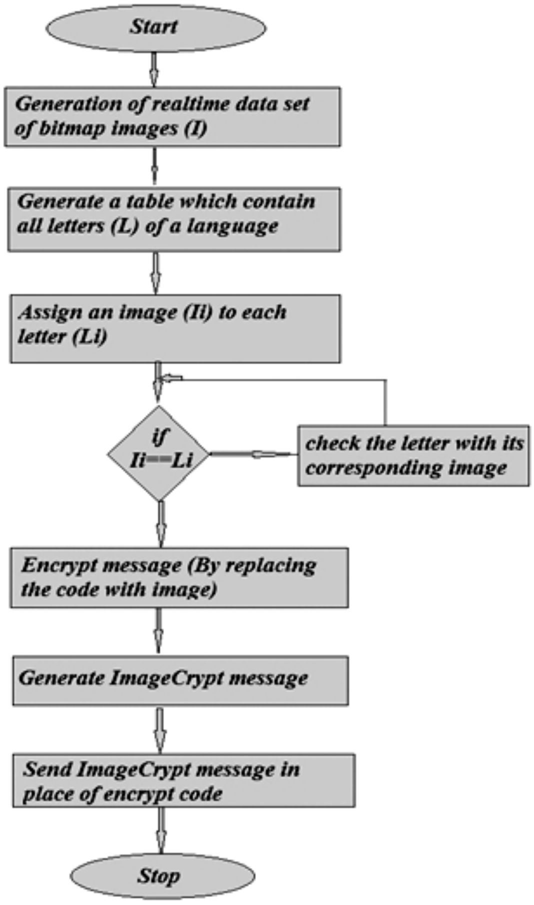
Start
Generation of realtime data set of bitmap images (I)
Generate a table which contain all letters (L) of a language
Assign an image (Ii) to each letter (Li)
if Ii==Li
check the letter with its corresponding image
Encrypt message (By replacing the code with image)
Generate ImageCrypt message
Send ImageCrypt message in place of encrypt code
Stop

Figure 2: Complete Scenerio of Proposed Technique

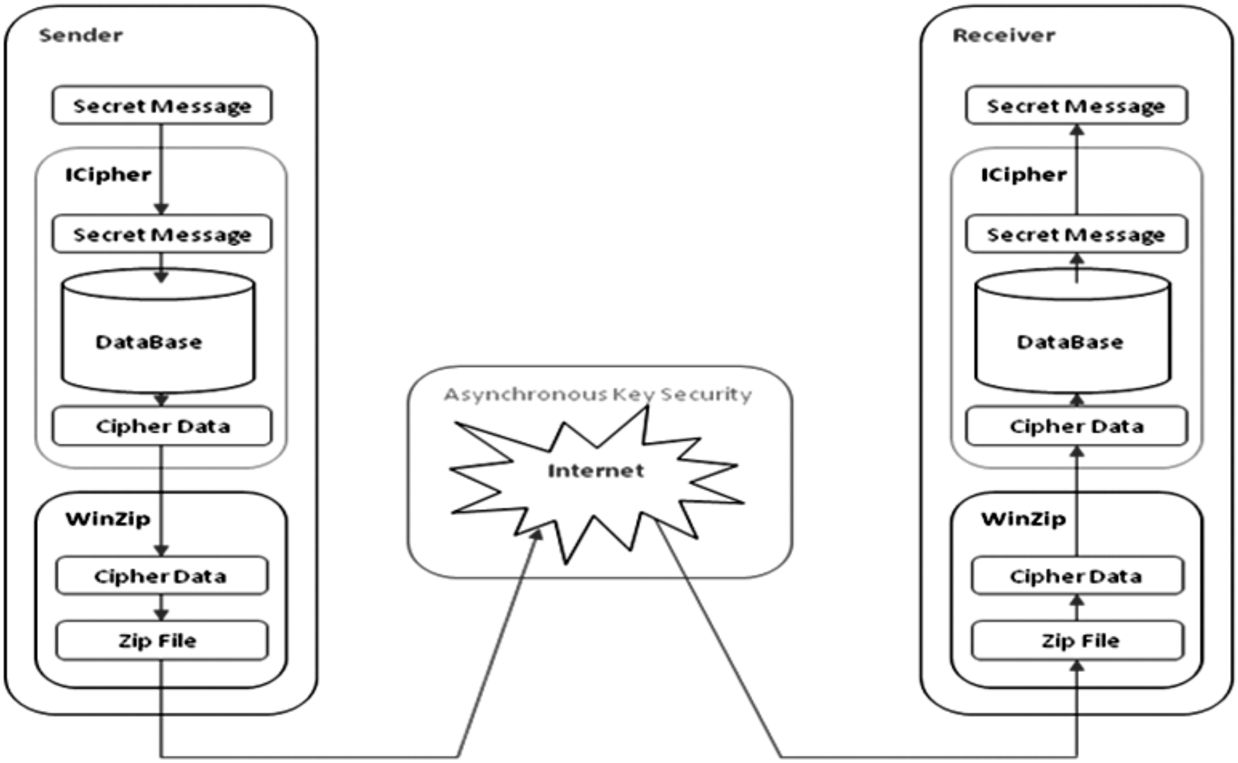

Figure 3: Process of ICipher (ImageCrypt) From Sender to Receiver

This figure contains the three steps, first part is senders who responsible for encryption by ICipher (ImageCrypt) then convert to zip form and finally send it to receiver on internet. Second part is internet, this phase used the second level security called asynchronous key cryptography which provide the key level security for message to reduce the risk of intruders. this cryptography techniques used two types of keys for message encryption public key and private key sender used private key and receiver public key for encryption, receiver used his private key for decryption.

We may include another level of security on zip level; zip files can use password protection of secret message before asymmetric encryption. Zip file is able to include any encryption techniques. The ICipher (imageCrypt) technique consist following three processes.

Preprocess: According to Icipher this take all the secret message for encryption and it will convert in the cipher data.

Midprocess: In This process, secret data is converted in zip or rar file format for transmission process & finally sent to target.

Finalprocess: Firstly, it takes the code in zip form & then unzip it, and final process coverts the secret code to uncipher message that is easily readable to receiver.

These all three process steps take place in this Icipher tool, preprocess is done at the sender side and Midprocess also take place at the sender side and the Finalprocess is processed at the receiver side.

3.2. Efficiency

1. This algorithm is best for small secret messages, but it will be useful for all size of messages if network speed is appropriate.

2. This algorithm is safe from confidentiality, integrity and availablity problems.
3. It will very hard to decrypt.
3. Complete solution from intruders or hacker.

The relation between the image size and the data weight are two important factor which depend on each other, because when the images size is changed to upper limit or lower limit, the weight of data on the network is also change. Let If image size is increase then data weight also increase on network during message traveling, on other hand when image size reduced then data weight is also reduced.

Table 2
Comparison between traditional method and Image Crypt

S. No.	*Techniques/ Methods*	*Problems*	*Solution by ImageCrypt*
1.	Steganography	Steganography is techniques which used other data as image, audio/video for hiding the original or secret data behind them, but this contains the secret data in mixed form if some got this data and if intruder knows that this contain some critical data then they may decrypt it.	Image Crypt contains the bit map images in behalf of secret data or message, so there is no risk of analysis.
2.	Substitution	Traditional Substitution techniques used some replacements of characters to another characters, but if someone analyses the substitution pattern then it may decrypted.	Image Crypt used special types of substitution which is in a changeable objects form as images etc. which is harder to analyses pattern.
3.	Transposition	Transposition is techniques which used the place or position changing method as we can use c in place of a and d in place of b and so on, this is also contains some more hard method for this, but still it may be decrypted by analysis.	Image Crypt used substitution in place of transposition and another layers of security for strong algorithm etc.

4. CONCLUSION

Cryptography is a way to write a secrete message. It uses the public and private keys for encryption and decryption of the message. The proposed technique is Image substitution technique which completely reduced the drawback of conventional cryptography. This technique does not contain any information related to secret message, so there is no way to decrypt the encrypted message back to secret message or understandable form, Thus secret encrypted message is completely secure and there is no relation between secret message and encrypted message. This technique is enveloped in three layers. it can be used with combination of present algorithms as any one of substitution or transposition for encryption

REFERENCES

[1] R. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms" International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306

[2] T. Rubya, N. Prema Latha, B. Sangeetha, "A Survey on Recent Security Trends using Quantum Cryptography" International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3038-3042

[3] L.Jothi, "A Literature Review: Cryptography Algorithms for Wireless sensor networks",IJCSET Vol. 4 No. 10 Oct 2013

[4] Ijaz Ali Shoukat1, Kamalrulnizam Abu Bakar and Mohsin Iftikhar, "A Survey about the Latest Trends and Research Issues of Cryptographic Elements" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011

[5] Anupama Mishra "Enhancing security of Caesar cipher using different methods" , International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308

[6] Kashish Goyal " Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013

[7] Orooba Ismaeel Ibraheem Al-Farraji "New Algorithm for Encryption based on substitution cipher and transposition cipher" International Journal of Current Research Vol 7, Issue, 12, pp.23610-23612, December, 2015

[8] Atish Jain, Ronak Dedhia, Abhijit Patil " Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication" International Journal of Computer Applications (0975 – 8887) Volume 129 – No.13, November2015

[9] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad Odeh, "Survey Paper: Cryptography Is The Science Of Information Security" International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011

[10] A. Joseph Amalraj, Dr. J. John Raybin Jose, "A SURVEY PAPER ON CRYPTOGRAPHY TECHNIQUES" IJCSMC, Vol. 5, Issue. 8, August 2016, pg.55 – 59

[11] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008

[12] D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in Advance in Cryptology (CRYPTO'01), LNCS 2139, Springer Verlag, 37, 213-229, 2011

[13] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978

[14] Gábor Erdé Lyi, Tim Meyer, Tobias Riege, And Jö Rg Rothe Quantum Cryptography: A Survey Dagmar Bruss, ACM Computing Surveys, Vol. 39, No.2, Article 6, Publication date: June 2007

[15] ICAO, "Manual of technical provisions for the aeronautical telecommunications network (atn) - standard and recommended practices (sarps)," Mars 2001.

[16] E.Thamiraja ,G.Ramesh,R.Uma rani "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[17] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal Of Computing, Volume 2, Issue 3, March2010,Issn2151-9617

[18] Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar "comparative analysis between DES and RSA algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[19] C. J., Ulasi A. G "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December