iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** IV **Month of publication:** April 2018

**DOI:** http://doi.org/10.22214/ijraset.2018.4090

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 6 Issue IV, April 2018- Available at www.ijraset.com*

# A Survey: Network Security and Cryptography Technique

Satish Kumar Yadav [1], Arpita Maji[2], Dr. Gitanjali Nikam [3], Mukta Dhiman[4]
[3]*Asst. Professor,* [4]*Asst. Professor*
[1, 2, 3, 4] *Dept. of Computer Application, National Institute of Technology (Kurukshetra)*

***Abstract:*** ***Cryptography can be defined as the science of writing in secret code and protecting the information by transforming it in a secure and inaccessible format for those who are not intended can't read and process it. Importance of digital communication has increased for a secure and unaltered transmission of data between sender and receiver. Security is of the great significance for exchange of information among the sender and receiver. This review paper contains the details of work done in the field of cryptography along with proposed algorithms. Asymmetric and symmetric algorithms are analysed in detail and included. In some algorithms, modulus operations are performed on the integral values followed by the ASCII value generation of the plaintext characters. In many algorithms substitution is also used along with the new methodology for text encrypts and decrypt using ASCII algorithm also the combination of vigener and Caesar cipher encryption techniques. The concept of intermediate text is also used. By studying various research papers, reviews are made and more secure ways are to be proposed in near future. After detailed analysis, comparison is done, conclusion is made and an algorithm is proposed using the ASCII values and the modified Vigener table for highly secure way of cryptographic practice along with an idea of less number of steps. Less number of steps directly affects the complexity of the algorithm and an efficient algorithm can be obtained.***
***Keywords:*** ***Network security, Cryptology, Encryption, ASCII value, Symmetric encryption, Asymmetric encryption Cipher***

## I. INTRODUCTION

*Cryptography*: It is a part of security. Security is much bigger than Cryptography, it is a part of security only. Cryptography is formed from cryptology. Cryptology is divided into two parts a) Cryptography and b) Cryptanalysis. And Cryptography has 3 parts…a) Symmetric algorithm & b) Asymmetric algorithm & c) Protocols. Some include protocols as a part of cryptography, where as some don't. Cryptanalysis is the hacking part and cryptography is the protecting part. The simple problem of when we communication over insecure channel. This communication could be anything like, open air or internet or airwaves GSM. Let, person A wants to send some information to the person B via e-mail. Now, suppose those kind of information are very important. And the 3rd person let C wants those information for bad use. Here, person A could give those information's to the B by hand or personal delivery, which is not possible for all time. So encryption was introduced to the person A side and what it does, it is a mathematical formula which calculates and transforms plain text to cypher text, so person C does not get information any more. In case of data person C will get random bits and in case of mail person C will get random characters. And the receiving side of person B has to decrypt to get the information! So we have encryption and decryption functions..! It is a conflict idea to do public Encryption and Decryption functions over internet. Some says it is a stupid idea to do public those functions, because person C will also get to know how to encrypt and decrypt. And some says it is actually secure to do public but it is not secure to use untested Cryptography .So, we use another parameter or input function key (k). Key becomes very important to the receiver side, if person B has the authorized key then he can decrypt information! Person A sends the text or information called plain text & person B sends the text or information called cipher or cypher text and E as encryption function, D as decryption function and K as key and |k| as key space (number of keys). Cryptography can be break by brute force key i.e., we use secure channel, could be anything like Telephone or a person travelling between person A to person B or internet which is connected to encryption and decryption key

## II. RELATED WORK

Mukund R. Joshi et al. [3] have provided a research review on network security and various techniques of the encryption used for cryptography. It mainly targets on the detailed study of the implementation of the different encryption techniques. They have done a literature survey on the methods of encryption and analysed more about network security and cryptosystem. The author have provided with the various cryptographic principle. First principle says that the encrypted message should contain some redundancy

i.e. to prevent message from being understandable the text should be redundant. Second principle says that there should be some methods to prevent the security attacks.

The authors have also provided details about various cryptosystem. The various cryptosystem is based upon the key used in the encryption. They are classified as symmetric or asymmetric key. In symmetric key encryption technique only one key is used for encryption and decryption procedure. In asymmetric key encryption two keys are used one is used encryption and other is used for decryption. One key is called private key which is used for encryption, other key is called public key is used for decryption. The keys are generated and managed through various key management techniques. Further the authors have discussed over various algorithm used for the encryption purpose.

*A. DES*

The data encryption standard algorithm works on 64 bit block of data. It uses a 64 bit key. The key is then again converted to 56 bit. The plain text is divided into two equal halves/blocks and key is used for encryption. Initial permutation is applied on plain text and then each half goes through 16 rounds of encryption. After encryption each half is combined and a final cipher text is formed.

*B. HASH*

Hashing technique is applied for enumerate a complex illustration of a fix size message or file [13]. It is called a 'fingerprint' or a 'message digest'. it is of the huge digest size, it is less possible that two distinct messages will have the same SHA-1 message digest. Due to this logic it is approved over MD5.

*C. AES*

it is a widely adopted symmetric encryption technique. It is six times faster than triple DES. It works on 128 bit of data with key size used as 128 bit/192 bit/256 bit of length. The length of the key AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, 14 rounds for 256 bit keys. The encryption process consist of bytes substitution, rows shifting, mixing of columns with XOR operation. The last text which is obtained after the encryption is called cipher text.. Reverse process is applied for decryption.

*D. RSA*

RSA is a key generation and asymmetric encryption algorithm. For key generation two large prime numbers are selected. Both the prime numbers are multiplied and stored. Encryption key is produced by applying formula and decryption key is calculated. The encryption key is called public key and decryption key is called private key.

Nivedita Bisht et al. [1] Have provided a comparative study of various encryption algorithm. They have compared both the symmetric and asymmetric key cryptography on different factors. The utilization of key is characterised as far as encryption and decoding it is possible that it is same or extraordinary. The calculation utilization is characterized by its sort symmetric or deviated. The length of key is utilized by it's deem. The speed is portrayed as quick or moderate. The utilization of power takes less or high. The security is defined as great but not secure or minimum secure. The cost is more economic or un-reasonable. The execution as directed by its calculation utilization is either basic or complex.

Asymmetric Cryptography: In asymmetric key cryptography diverse keys for encryption and for readable, thus otherwise called open key encryption. The two keys, one is private key and another is an open key. The general population key is reported to people in general; though the private key is kept by the receiver. The sender utilizes the general society key of the beneficiary for encryption and the collector employments his private key for decoding. Here the quantity of keys are required is little however it isn't proficient for long messages. In unbalanced key encryption the RSA calculation and Diffie Hellman calculation diverse elements are broke down. Symmetric key Cryptography: In symmetric key cryptography, same key is shared to both sides, i.e. the one key is used for both encryption and decoding. Hence, otherwise it is also called single key or mystery key encryption. Symmetric key cryptography calculations are required less execution time. As per conclusion, these are normally utilization for long messages. There are two parts of symmetric key encryption modes, one is as piece figures and different as stream figures. Piece figures work on gatherings of bits and it is called as pieces and each parts or square is prepared in various number of times. The key is connected in each round in an interesting way. A stream figure works on a one piece at any given moment or time i.e. the information is isolated as little like single bits and after that the encryption is done. [12]In symmetric key encryption the AES and the DES diverse components are broke down.

The symmetric key and asymmetric key algorithms investigated that symmetric key calculations is seem to be great as compare to speed and power utilization while deviated key calculations in respect of tenability. In the symmetric key encryption, AES

calculation is observed, that is better as far as cost, security and usage. In topsy-turvy key encryption, RSA calculation is better regarding the rate and security.

Nath et al. [8] have proposed an algorithm for the symmetric key cryptography method containing encryption and decryption of different types of files like textual file, binary file or any other different types of files. They have come up with an algorithm called MSA for encryption and decryption. They have proposed a symmetric key method that works with generation of the random key matrix. The key is used for cryptographic encryption. For creating random key of size they have chosen any key text that is the secret key and whose size is less than or equal to 16 characters. The relative position of characters and the characters are important to calculate the random number and encryption number. To calculate the random number they took the key character and its length with a table that is based on length of the text and their corresponding base value. They have used a formula to calculate the random number from the sum of the formula used earlier. To calculate the encryption number they have used another formula that takes the sum used earlier and modulus function .They have used a substitution method that uses four characters as input from input file and search for same characters from random key matrix. For encryption process they have used a modified version of play fair encryption technique on their 4 X 4 key matrixes. They have processed the table in various cyclic shifting, up shift, right shift, down shift and left shift. The combined group of two plain text character is then matched with the characters of the table and correspondingly a new cipher text is generated. For encryption first it is checked if characters are in same row or same column or different rows and different columns and then replaced with other characters from the table. Final text that is formed with the replacement of characters is then used as cipher text. The present algorithm of the author is good for small files but for larger files it would be difficult which a major drawback of their algorithm is. If the number chosen as random key and encryption key is very large then the speed of the algorithm will decrease.

Nisha Rani et al. [5] have proposed a new system for detecting suspicious email using triple DES algorithm. The system detects for any type of security attacks or suspicious email. In the paper the authors have proposed the use of cryptographic techniques for suspicious email detection. The cryptographic technique used is triple DES (Data encryption standard) algorithm which is a private key cryptography system. The system detects suspicious message sent from the sender that are registered on the website. The website provides sign up facility for new user to send and receive email. In this paper, they have connected Cryptography systems to identify suspicious messages, i.e., an email that alarms of forthcoming fear based oppressor occasions. We have connected Triple DES (Data Encryption Standard) calculations, underlining at first on Given a plaintext message, the main key is utilized to DES-encode the message. The second key is utilized to DE decode the scrambled message. (Since the second key isn't the correct key, this decoding just scrambles the information further.) The twice-mixed message is then encoded again with the primary key to yield the last figure content. This three advance technique is called triple-Triple-DES is simply DES done three times with two keys utilized as a part of a specific arrange. (Triple-DES should likewise be possible with three separate keys rather than just two. In either case the resultant key space is around 2^112.) Triple DES Algorithm utilized by administrator to scramble the messages sent to the clients or sent a few notices about alternate client's suspicious movement. In this work, suspicious words lexicon is utilized to recognize the suspicious words which are not really utilized as a part of the ordinary informing or correspondence.

They have created two modules for their system. First is the admin module and second is the user module. Both modules have their sub-modules.

dmin Module: In Admin module, administrator can check all the suspicious mail which is send by suspicious clients. He can see the information lexicon, see the client detail which is enrolled in this framework and in addition send the message to client.

User module: In this, client can send message to another client and that message will be encode somehow by utilizing some key. Whenever user (sender) send message to another client he needs to enter their name, subject, key, and sort their message. Email id is now enlisted at the season of client enrolment. At that point that key will be send to the user (receiver) Gmail inbox. He can see their key and then unscramble their message and see the message. In this way, the principle advantage of this framework it gives security and also suspicious sends and suspicious client can without much of a stretch distinguished. The limitation with this system is that only fixed number of words are present in the dictionary as suspicious words. If any other suspicious word will be used other than that present in their given dictionary the system will fail in detecting the suspicious mail.

## III.COMPARATIVE ANALYISIS

### *A. General*

The above approach will be use for the secure communication. The algorithms should perform the encryption and decryption of the input text/other multimedia file. For that some of the parameters and measures are to be considered. They are encryption computation time, decryption computation time, encryption, decryption security keys and block size.

Table 1: Comparison of various encryption techniques

| Factor | AES | DES | RSA | DH |
|---|---|---|---|---|
| Key used | Only one key is used for encryption and decryption [12] | Only one keys are used for encryption and decryption [12] | two key is used one is used for encryption other is used for Decryption [13] | Two keys are used one is used for encryption other is used for decryption[13] |
| Algorithm | symmetric algorithm | Symmetric algorithm | Asymmetric algorithm | Asymmetric algorithm |
| Key length | 128/192/256 bit keys | 56 bits keys | 1024 bits keys | Key exchange management |
| Speed | Fast | Fast | Fast | Slow |
| Power consumption | Low | Low | High | High |
| Security | Excellent secure | Not secure enough | Excellent secure | Less secure than RSA |
| Cost | Cheap | Expensive | Expensive | depends on key |

## IV. CONCLUSION

An efficient and robust encryption and decryption methodology is essential for secure communication more specifically in various fields via cookies, email detection system, group communication. Investigation of encryption strategies regarding symmetric key and asymmetric key calculations have been carried out and found that symmetric key calculations is better in speed and power utilization. However AES algorithm of symmetric key encryption seems to be promising, cost and security. AES provides full satisfaction and design details. In asymmetric key encryption RSA calculation is better as far as speed and security. The strength of encryption of RSA algorithm increase exponentially. RSA algorithm easy to implement and understand.[9] Cryptography ensures that data is not manipulated or altered during the transmission of data.

## REFERENCES

[1] Nivedita Bisht, “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms”, International Journal of Innovative Research in Science, Engineering and Technology , Volume 4, Issue 3, March 2015

[2] Gurjeevan Singh, Ashwani Single, K S sandha”, “Cryptography algorithm comparison for security enhancement in wireless intusion detection system”, “International journal of multidisciplinary research, volume .1 issues 4, august 2011.

[3] Mukund R. Joshi, “Network Security with Cryptography” IJCSMC, Vol. 4, Issue. 1, January 2015.

[4] Diffie, W., and Hellman, M.: ‘New direction in cryptography’, IEEE Trans., 1976, IT-22, PP.644-564

[5] Nisha Rani,” Suspicious Email Detection System via Triple DES Algorithm: Cryptography Approach” IJCSMC, Vol. 4, Issue. 5, May 2015, pg.552 – 565

[6] P.S.Keila and D.B.Skillicorn, “Decting unusaland Deceptive Communication in Email,” Technical reports June, 2005.

[7] S.Appavu and R.Rajaram, “Supicious Email Detection via Decesion Tree: A Data Mining Approach’, in Journal of Computing and Information Technologies.

[8] Nath,Joyshree,” A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA Symmetric key algorithm” 2011 International Conference on Communication System and Network Technologies.

[9] Divya Shree and Seema Ahlawat, “A review on Cryptography, Attacks and Cyber Security”, International Journal of Research in Computer Science, June 2017

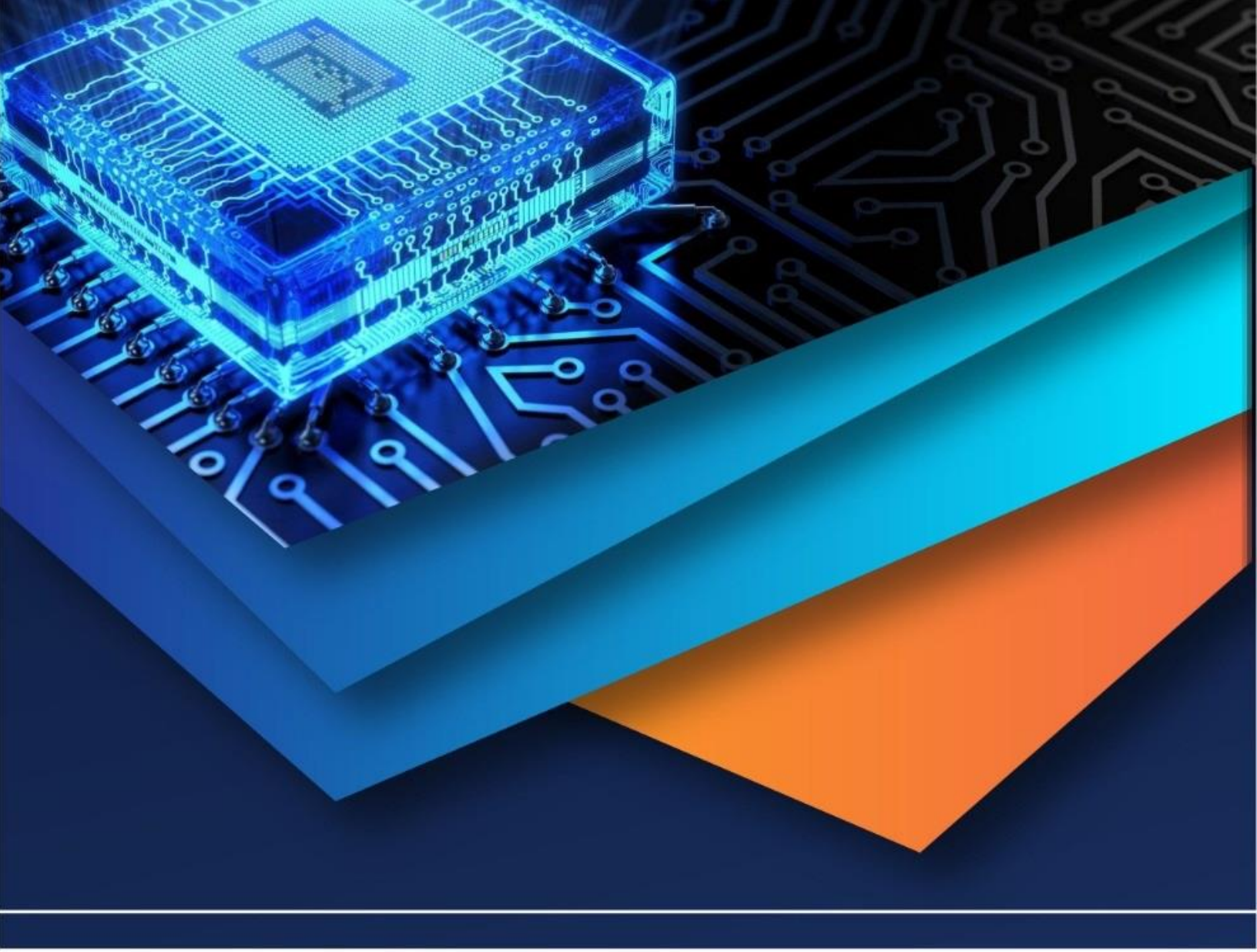
[10] Gurjeet Kaur and Babita, “A Review: Network Security based on Cryptography and Steganography Technique”, International Journal of Advanced Research in Computer Science, 4 may 2017

[11] Swati Kashyap and Er, Neeraj Madan, “A review on: Network Security and Cryptography Algorithm”, International Journal of Advanced Resarch in January 2014

[12] Divya Sukhija, “A Review Paper on AES and DES Cryptographic Algorithm,” International Journal of Electronics and Computer Science Engineering.

[13] Paul C.Kocher, “Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and other Systems”, Cryptography Research Inc., USA

[14] N. Priya and M. Kannan, “Comparative Study of RSA and Probabilistic Encryption, “International Journal of Engineering and Computer Science, January 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY