Study on different Cryptography Algorithm a Critical Review

Mohammad Saleem Bari, Ahmad Talha Siddique

Abstract— **Encryption is the way towards scrambling a message so that the intended beneficiary can read it. Encryption can give a method for securing data. As more data is put away on PCs or conveyed by means of PCs, the need to guarantee that this data is insusceptible to snooping as well as altering turns out to be more applicable. With the quick movement of computerized information trade in an electronic way, Information Security is turning out to be considerably more imperative in information stockpiling and transmission. Data Confidentiality has an unmistakable hugeness in the investigation of morals, law and most as of late in Information Systems. With the advancement of human insight, the specialty of cryptography has turned out to be more perplexing keeping in mind the end goal to make data more secure. Varieties of Encryption frameworks are being conveyed in the realm of Information Systems by different associations.**

Index Terms— **AES, DES, RSA, Encryption, Decryption.**

I. Introduction

Cryptography is the method that makes information or system secure by giving security. Cryptography is the study of concocting strategies that permit data to be sent in a protected shape in a manner that the main intended user recovers this data without any difficulty. The profound utilization of systems administration prompts to the information trade over the system while conveying to one and another over the network. It is essential to scramble the message with the goal that interpreter can't read the message. [1] Fundamentally, Cryptography is a technique of concealing data by scrambling the message. The technique of ensuring data security by the techniques of encryption and decryption is called cryptography. [2]

A. Basic Terminology used in Cryptography

There are a few terms which we ought to know for better comprehension of encryption calculations. This phrasing is critical to comprehend on the grounds that in each calculation depiction, we will examine these basic terms:

i. Plain Text or Normal Text

The first content or message utilized as a part of correspondence in called as Plain text. Illustration: John sends "Hi" to Perry. Here "Hi" is Plain text or Original message.

ii. Cipher Text

The plain text is scrambled in a un-coherent message. This encrypted message is called Cipher Text. Case: "Hi" message is changed over in "- &tt%".This good for nothing message is Cipher Text.

iii.Encryption

Encryption is a procedure of changing over Plain text into Ciphertext. This non-meaningful message can safely be conveyed over the insecure medium. The encryption process is done utilizing encryption calculation.

iv. Decryption

The unscrambling procedure is the switch of the encryption process, the i.e. ciphertext is changed over into plain text utilizing specific encryption calculation.

v. Key

A key is a numeric or Alpha-numeric content (scientific recipe). It is applied to the plain text while encryption and on cipher text when decryption is done.

vi. Key Size

Key size is the measure of the length of the key in bits, utilized as a part of any calculation.

vii. *Block Size*

Key figure deals with settled length series of bits. This settle length of a string in bits is called Block measure. This square size relies on calculation.

viii. *Round*

Round of encryption implies that how much time encryption capacity is executed in total encryption prepare till it gives figure message as yield.

B. Main Objectives of Cryptography

Encryption or Cryptography has a few objectives that should be satisfied for client advantage. Cutting edge cryptography worries about the accompanying four targets:

i. Confidentiality

The rule of classification determines that exclusive the sender and the planned beneficiary ought to have the capacity to get to the substance of a message

ii. Integrity

The trustworthiness system guarantees that the substance of the message continue as before when it achieves the proposed beneficiary as sent by the sender.

Mohammad Saleem Bari*, Department of CS&IT, Maulana Azad National Urdu University,Hyderabad, Hyderabad, India*
7989997566
Ahmad Talha Siddique*, Department of CS&IT, Maulana Azad National Urdu University, Hyderabad,India*
7893035678

iii. Non-repudiation

Non-disavowal does not permit the sender of a message to disprove the claim of not sending the message.

iv. Authentication

Validation instruments set up proof of personalities. This procedure guarantees that the starting point of the message is effectively distinguished.

v. Access Control

Just approved clients can get to the information. This is done to maintain a strategic distance from an unapproved client.

vi. Availability

The standard of accessibility expresses that assets ought to be accessible to approved gatherings are only visible.

In this paper, we analyze three encryption standard AES, DES and RSA.

II. DATA ENCRYPTION STANDARD

DES is a piece figure that utilizes shared master key for encryption and unscrambling. DES calculation as portrayed by Davis R. [3] takes a settled length string of plaintext bits and changes it through a progression of confused operations into figure content piece string of a similar length. On account of DES, each square size is of 64 bits. DES additionally utilizes a key of 56 bits to redo the change, with the goal that decoding must be performed by the individuals who know the specific key used to scramble the message. There are 16 indistinguishable phases of preparing, named rounds. There is likewise an underlying and last stage, named IP and FP, which are inverses (IP "fixes" the activity of FP, and the other way around). The Broad level strides in DES are as per the following [4]:

1. In the initial step, the 64-bit plain instant message is given over to an Initial stage (IP) work.
2. The underlying stage is performed on the plain content.
3. The IP produces two parts of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4. Presently, each of LPT and RPT experiences 16 rounds of an encryption process.
5. At last, LPT and RPT are rejoined and the last stage (FP) is performed on the consolidated square.
6. The consequence of this procedure produces 64-bit figure content. Rounds: Each of the 16 rounds, thus, comprises of the expansive level strides. [5]

III. ADVANCED ENCRYPTION ALGORITHM

The AES (Advanced Encryption Standard) [6] is an encryption standard as a symmetric piece figure. It was declared on 26thNovember 2001 by National Institute of Standards and Technology (NIST)) as U.S. FIPS PUB 197 (FIPS 197).The focal outline guideline of the AES calculation is the appropriation of symmetry at various stages and the productivity of preparing.

The AES works on 128-piece squares of information. The calculation can encode and unscramble squares utilizing mystery keys. The key size can either be 128 pieces, 192 pieces, or 256 pieces. The real key size relies on upon the coveted security level. The distinctive renditions are regularly signified as AES-128, AES-192, AES- 256.

A.AES round transformation:

The round change [7] adjusts the 128-piece State. The underlying State is the information plaintext and the last State is the yield figure content. The State is sorted out as a 4 X 4 network of bytes. The round change scrambles the bytes of the State either independently, push shrewd, or section astute by applying the capacities Sub Bytes, Shift Rows, Mix Columns, and Add Round Key successively.

i.Sub-Byte Transformation

Sub Byte is a substitution work in the Cipher round. In the Sub Bytes step, every byte in the state is supplanted with its entrance utilizing a non-linear byte substitution table (S-box) that works on each of the State bytes freely.

ii. Shift Rows transformation

Move Rows is a changing work in the Cipher round. In the Shift Rows step, bytes in every line of the state are moved consistently to one side. The abundance of spots every byte is moved varies for every column. Move Rows step is made out of bytes from every section of the info state.

iii. Mix Columns Transformation

Blend Columns is a Mixing capacity in the Cipher round. In the Mix Columns venture, In the Mix Columns step, the four bytes of every segment of the state are consolidated utilizing an invertible straight change. The Mix Columns work takes four bytes as info and yields four bytes, where every information byte influences each of the four yield bytes. Together with Shift Rows, Mix Columns gives dissemination in the Cipher

iv. Add Round Key Transformation

Include Round Key is a key including capacity in the Cipher round. In the Add Round Key stride, the subkey is consolidated with the state. For each cycle, a subkey is gotten from the primary key utilizing Rijndael's key calendar, every subkey is an indistinguishable size from the state. The subkey is included by consolidating every byte of the state with the relating byte of the subkey utilizing bitwise XOR.

AES Decryption registers the first plaintext of an encoded figure content. Amid the unscrambling, the AES calculation turns around encryption by executing backward round changes backward request. The round change of decoding uses the capacities Add Round Key, Inv. Blend Columns, Inv. Move Rows and Inv. Sub Bytes [8].

IV. RSA

This is open key encryption technique created by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It is most well-known and unbalanced key cryptographic technique. It might use to give both secrecy and digital signature. [9] It utilizes the prime number to produce people in general and private key in light of scientific actuality and duplicating substantial numbers together. It utilizes the piece measure information as a part of which plaintext and figure content are numbers between 0 and n1 for some n values. The size of n is viewed as 1024 bits or 309 decimal digits. In this two diverse keys are utilized for encryption and unscrambling reason. As sender knows encryption key and collector knows decoding key. [10]

A. *Key generation*

For the RSA cryptosystem, we first begin off by creating two substantial prime numbers, "p" and “q”, of about a similar size in bits. Next, figure "n" where n = pq, and "x" with the end goal that, x = (p - 1)(q-1). We select a little odd number not as much as x, which is moderately prime to it i.e. gcd(e,x) = 1. At long last, we discover the one of a kind multiplicative backward of e modulo x and name it 'd'. At the end of the day, ed = 1 (mod x), and obviously, 1 < d < x. Presently, general society key is the combine (e,n) and the private key is d.

B. *RSA Encryption*

Assume Bob wishes to communicate something specific (say 'm') to Alice. To scramble the message utilizing the RSA encryption conspire, Bob must get Alice's open key combine (e,n). The message to send should now be encoded utilizing this combine (e,n). Nonetheless, the message "m" must be spoken to as a whole number in the interim [0, n-1]. To scramble it, Bob just figures the number "c" where c = m ^ e mod n. Weave sends the figure ext c to Alice.

C. *RSA Decryption*

To unscramble the figure content c, Alice needs to utilize her own private key d (the decoding type) and the modulus n. just figuring the estimation of c ^ d mod n yields back the decrypted message (m). [11]

Mathematically

The RSA calculation [10] depends on the scientific part that is anything but difficult to discover and various two substantial prime numbers together, however, it is amazingly hard to consider their item.

Pick vast prime numbers p and q with the end goal that p~=q.

Process n=p*q

Process φ (n) = (p-1)*(q-1) Where φ(n) is Euler Totient Function

Pick people in general key e with the end goal that

gcd (φ (n), e) =1; 1<e< φ (n)

Select the private key d with the end goal that

d*e mod φ (n) =1

So in RSA calculation encryption and decoding are executed as-

Encryption

Compute figure content C from plaintext message M with the end goal that

C=M ^e mod n

Decryption

M=C^d mod n=M^ed mod n

V. RELATED WORK

This sub-section describes and examines previous work done in the field of an encryption algorithm.

Dr.Prerna Mahajan et. al. [12] Encryption calculation assumes the critical part in transmission security. Our examination work reviewed the execution of existing encryption strategies like AES, DES and RSA calculations. In light of the content records utilized and the trial result, it was presumed that AES calculation expends minimum encryption and RSA devour longest encryption time. We likewise watched that Decryption of AES calculation is superior to different calculations. From the reproduction result, we assessed that AES calculation is greatly improved than DES and RSA calculation..

Mini Malhotra et. al. [13] It is restated that the RSA is utilized broadly. An extensive variety of research is done in RSA. It utilized an inquiry of catchphrase lists and article titles. This paper displays the present situation and can give a heading to gullible clients.

Gurpreet Singh et. al. [14] This paper introduces a nitty gritty investigation of the well known Encryption Algorithms, for example, RSA, DES, and AES. The utilization of web and system is developing quickly. So there are more prerequisites to secure the information transmitted over various systems utilizing diverse administrations. To give the security to the system and information diverse encryption techniques are utilized. In this paper, a review of the current deals with the Encryption procedures has been finished. To sum up, every one of the methods are valuable for ongoing Encryption. Every strategy is one of a kind in its own particular manner, which may be reasonable for various applications and has its own advantages and disadvantages. As per research was done and writing study it can be found that AES calculation is most productive as far as speed, time, throughput and torrential slide impact.

B. Padmavathi et.al. [15] In Data transmission, encryption calculation assumes a critical part. Our exploration work reviewed the current encryption procedures like AES, DES and RSA calculations alongside LSB substitution system. Those encryption procedures are contemplated and dissected well to advance the execution of the encryption techniques likewise to guarantee the security. In light of the trial result it was presumed that AES calculation expends minimum encryption and decoding time. In any case, RSA expands more encryption time and buffer use is additionally high. We likewise watched that decoding of AES calculation is superior to different calculations. From the reproduction result, we assessed that AES calculation is greatly improved than DES and RSA calculation.

ShashiMehrotra Seth et. al. [16] Encryption calculation assume a vital part in transmission security where encryption time, Memory utilizations yield byte and battery power are the real issues of concern. They chose encryption schemes like AES, DES and RSA and utilized their calculations for execution assessment. In light of the content records utilized and the exploratory outcome it was presumed that DES calculation devours slightest encryption time and AES calculation has minimum memory utilization while encryption time distinction is minor in the event of AES calculation and DES calculation. RSA expend longest encryption time and memory utilization.

RajdeepBhanot et. al. [2] In this paper, they have analyzed different encryption calculations. They have found that every calculation has its own particular advantages as indicated by various parameters. From the work finished in this paper, it is watched that the quality of the every encryption calculation relies on the key administration, sort of cryptography, number of keys, number of bits utilized as a part of a key. All the keys are based upon the numerical properties and their quality abatements regarding time.

S.Pavithra et. al. [18] Cryptography calculation is the science in mystery code. Quickly rising digital wrongdoing and the developing prospect of the web being utilized as a medium for assaults make a noteworthy test for system security. In this paper, they concentrated the different cryptographic calculations and significantly the encryption and unscrambling process for ensuring the content records and pictures utilizing a portion of the cryptographic calculations show a tradeoff.

Madhumita Panda [19] This paper displays the execution assessment of some symmetric and asymmetric calculations. From the exhibited results, it was presumed that AES has preferred execution over different calculations regarding both throughput and encryption-unscrambling time. A proposed bearing for the future work could be to play out similar analysis on sound and video also. Likewise for speedier encryption, we can first go for some pressure calculation and after that encryption.

Mitali et.al.[5] In this remote world these days, the security for the information has turned out to be exceptionally critical since the offering and purchasing of items over the open system happen every now and then. In this paper, the current techniques regarding encryption systems have been reviewed. Those encryption procedures are contemplated and examined well to advance the execution of the encryption strategies additionally to guarantee the security procedures.

RanjeetMasram et. al. [21] In this paper distinctive symmetric key calculation have been examined for different record highlights like diverse information sort, information thickness, information size and key size, and divided the variety of encryption time for various calculations. It is presumed that encryption time does not require sorted information about the document.

VI. COMPARISION

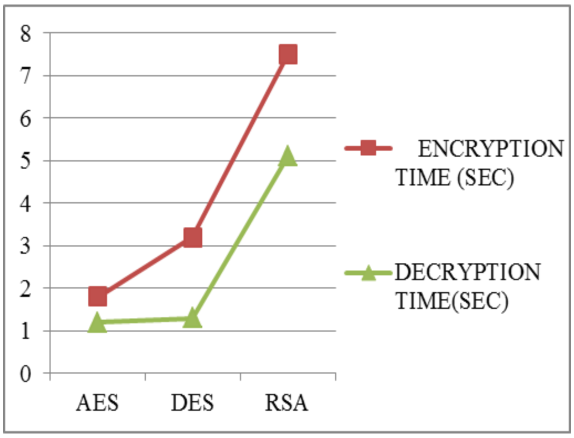
In the table underneath a relative audit between AES, DES and RSA is brought into eighteen factors, which are Key Size, Block Size, Ciphering and Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds, Stimulation Speed, Trojan Horse, Hardware and Software Implementation and Ciphering and Deciphering Algorithm[12]

Factors	**AES**	**DES**	**RSA**
Developed	2000	1977	1978
Key Size	128,192,256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Same
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and block size	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of Keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Force Attack	Brute Forced, Linear, and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	The same key used for Encrypt and Decrypt	The same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Simulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

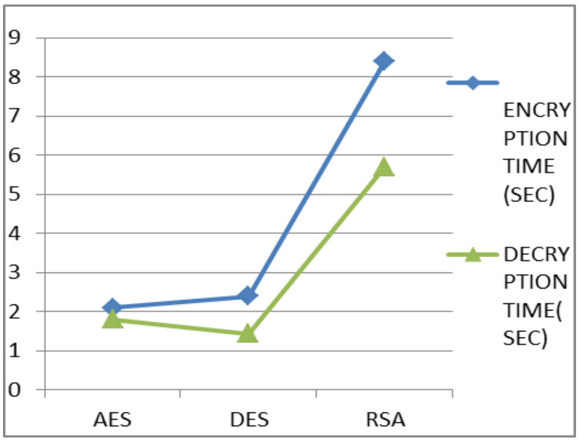
VII. EXPERIMENTAL ANALYSIS

Experiment analysis for Encryption algorithm AES, DES and RSA are shown in the table which shows the comparison of three algorithm AES, DES and RSA using the same text file for four experiments.

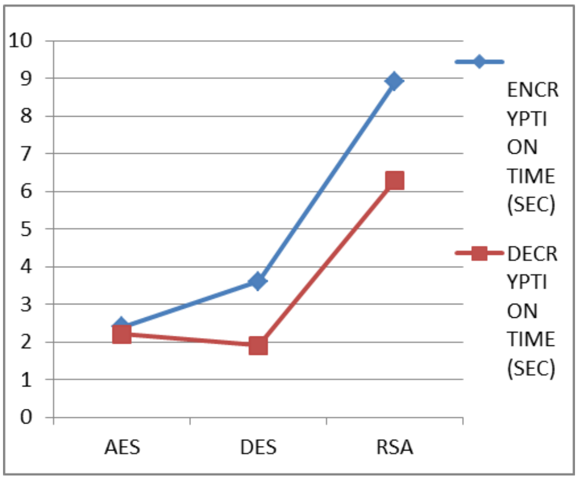
S.No.	Algorithms	Packet Size (KB)	Encryption Time (Sec)	Decryption Time (Sec)
1	AES	180	1.8	1.2
	DES		3.2	1.3
	RSA		7.5	5.1
2	AES	240	2.1	1.8
	DES		2.4	1.44
	RSA		8.4	5.7
3	AES	372	2.4	2.2
	DES		3.6	1.9
	RSA		8.9	6.3
4	AES	953	2.8	2.6
	DES		4.8	2.0
	RSA		9.0	5.9



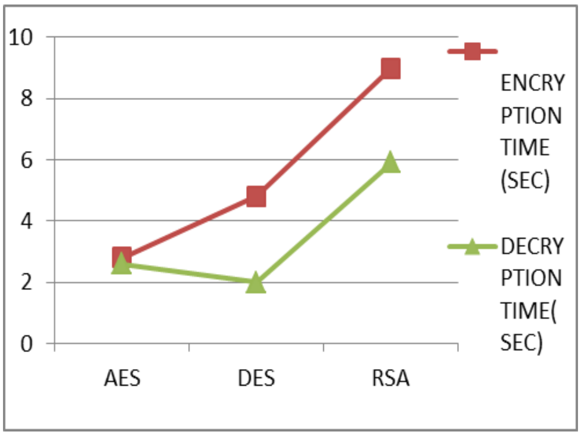
Packet size 180 Encryption and decryption



Packet size 240 Encryption and decryption



Packet size 372 Encryption and decryption



Packet size 953 Encryption and Decryption

VIII. CONCLUSION AND RESULT

Cryptography algorithm is the science in secret code In this paper We studied the various cryptographic algorithms and majorly deals the encryption and decryption process for protecting the text file based on packet sizes. In this paper, we have analysis various algorithm. We have found that each algorithm has its own benefits according to different factors and different packet sizes used. From above analysis, we have found that AES and DES, these two algorithms are leading with encryption and decryption time with respect to packet sizes. So, from this review and analysis that AES algorithm requires minimum time as compared to other two algorithms.

.

REFERENCES

[1] Textbook William Stallings, Data and Computer Communications, 6eWilliam 6e, (2005).

[2] Rajdeep Bhanot and Rahul 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

[3] Davis, R., "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

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

[5] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 4, July-August 2014

[6] FIP 197: Announcing the Advanced Encryption Standard, Nov. 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[7] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," IEE Proc. Inf. Security, vol. 152, IEE, pp. 13-20, Oct. 2005

[8] Hyubgun Lee, Kyounghwa Lee and Yongtae Shin "AES Implementation and Performance Evaluation on 8-bit Microcontrollers" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6 No. 1, 2009

[9] Aman Kumar, Dr.Sudesh Jakhar, Mr. Sunil Maakar "Distinction between Secret key and Public key Cryptography with existing Glitches" IJEIM- 0067, vol.1, 2012

[10] Mohit Marwaha, Rajeev Bedi, *Amritpal Singh, Tejinder Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS" Singh et al., International Journal of Advanced Engineering Technology

[11] A FAST IMPLEMENTATION OF THE RSA ALGORITHM USING THE GNU MP LIBRARY Rajorshi Biswas Shibdas Bandyopadhyay Anirban Banerjee IIIT-Calcutta

[12] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES, and RSA for Security" Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[13] Mini Malhotra & Aman Singh "Study of Various Cryptographic Algorithms" International Journal of Scientific Engineering and Research (IJSER) ISSN: 2347-3878 Volume 1 Issue 3, November 2013

[14] Gurpreet Singh & Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[15] B. Padmavathi & S. Ranjitha Kumari "A Survey on Performance Analysis of DES, AES, and RSA Algorithm along with LSB Substitution Technique" International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[16] Shashi Mehrotra Seth & Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication " International Journal of Computer Science and technology Vol. 2, Issue 2, June 2011 ISSN: 0976-8491(Online)

[17] Mansoor Ebrahim , Shujaat Khan & Umer Bin Khalid "Symmetric Algorithm Survey: A Comparative Analysis " International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013

[18] S.Pavithra & Mrs. E. Ramadevi "STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS" International Journal of Advanced Research in Computer Engineering & Technology Volume 1, ISSN: 2278 – 1323 Issue 5, July 2012

[19] Madhumita Panda "Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[20] Pritesh Kumar Prajapati, Nehal Patel, Robinson Macwan, Nisarg Kachhiya & Parth Shah "Comparative Analysis of DES, AES, RSA Encryption Algorithms" International Journal of Engineering and Management Research Volume-4, Issue-1, February-2014, ISSN No.: 2250-0758

[21] Ranjeet Masram, Vivek Shahare, Jibi Abraham & Rajni Moona "ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014

[22] Das Debasis, Misra Rajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 204.

[23] D. S. Abdul. Elminaam, M. Abdul Kader, M. M. Hadhoud "Performance Evaluation of Symmetric Encryption Algorithms" Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765

[24] E. Thambiraja, G.Ramesh, Dr. R. Umarani, "A survey on various most common encryption techniques," International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.

[25] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems"z. Communications of the ACM, Feb 1978

Mohammad Saleem Bari
M.Tech(CS), B.Tech(IT)
Mtech931517@gmail.com
Student M.Tech, Department of CS&IT,
Maulana Azad National Urdu
University,Hyderabad, India

Ahmad Talha Siddique.
M.Tech(CS),
Published International Journal
papers:8
Conference Proceedings(published:5)
Conference/Workshop Attended:2
ahmedtalha207@gmail.com Assistant
Professor, Department of CS&IT,
Maulana Azad National Urdu
University, Hyderabad, India.