Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparative Performance Analysis of Cryptographic Algorithms

Lalit Singh
(*C.S.E) BTKIT Dwarahat*
India

Dr. R.K. Bharti
(*C.S.E) BTKIT Dwarahat*
India

Abstract— Today is the era of Internet and networks applications. So the Information Security has been very important issue in data communication. Any loss to information can prove to be great loss to the organization. Encryption techniques are important in information security systems. This paper provides a fair comparison between five most common and used symmetric and asymmetric key algorithms: Two fish & Blowfish, IB_mRSA, RSA, RC. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption/decryption time, CPU process time in the form of throughput. These results show that IB_mRSA is more suitable than other algorithms. Simulation program is implemented using C#.NET programming.

Keywords— Cryptography, IB_mRSA, RSA, Blowfish, Two fish, RC2, Security, key management.

I. INTRODUCTION

Cryptography is an imperative element of avoiding private data from being purloined. Even if an intruder wants to split into your computer or intrude your messages it still won't be able to interpret the data if it is shielded by cryptography or if it is encrypted. Encryption is the process of converting data into some scribbled fashion. Its imperative function is to make sure secrecy by concealing the information from anybody for whom it is not proposed [3], even those who know how to read the encrypted data. Converse to encryption is decryption [13], i.e.; the conversion of encrypted data back into some sensibly readable form. Cryptography guarantees privacy since only a user with the proper deciphering algorithm or key can understand and identify the encrypted data [5]. Lastly, cryptography can safeguard the veracity of information by making sure that data has not been altered. Cryptology has been incorporated into smart cards for financial dealings, operating systems, web browsing, mobile phones and electronic identity cards.

Symmetric encryption algorithms are always deemed to be less complex as compared to asymmetric algorithm since only a single key is being employed in symmetric encryption [14]. Asymmetric cryptographic algorithms are dissimilar from symmetric algorithms in a manner that it requires two separate "keys" to encrypt and decrypt the data in contrast to the symmetric algorithm's single key encryption and decryption [1]. Asymmetric encryption, also known as public key encryption, employs two mathematically linked keys [2]: a public key for everyone for encrypting data and a private key, only for the receiver of the data for decrypting the data. Asymmetric cryptography is comprehensively utilized and brings about Transport Layer Security (TLS) and PGP (Pretty Good Privacy) protocols. A few general asymmetric algorithms include RSA and Diffie Hellman and some asymmetric algorithms include blowfish, two fish and RC2 etc.

II. COMPARED ALGORITMS

Blowfish, designed by Bruce Schneier in 1993, is a public domain and was explicitly used for performance-hindered situations for instance embedded systems [12]. Blowfish is a symmetric encryption algorithm, which implies that it employs the identical secret key for both encryption and decryption of data [8]. Blowfish is a block cipher as well, which means that it divides the data into some fixed length blocks at the time of encryption and decryption. Blowfish algorithm has the block length of 64 bits [4]. The Two fish encryption algorithm was designed in order to make the Advanced Encryption Standard (AES). Twofish is a symmetric block code which employs an identical key for encryption and decryption of data. The block size of a Twofish algorithm is 128 bits, and allows a key of length up to 256 bits [7]. RC2 is a block cipher designed in 1987 by Ron Rivest. "RC" stands for "Ron's Code" or "Rivest Cipher". Some other ciphers that are designed by Rivest comprise RC4, RC5 and RC6 [11] [13]. RC2 is a block cipher with the block length of 64-bits and uses an alterable key size which ranges from 8 to128 bits [1]. 18 rounds of RC2 are arranged as a source-heavy Feistel network, with 16 rounds of one type (MIXING) interposed by two rounds of other type (MASHING).

The major characteristic of identity-based encryption is the sender's capability to encrypt data by employing the use of public key which is derived from the receiver's identity and some other public information. The identity can be any information for instance receiver's email address, user id, contact number etc [10]. IB-mRSA is an easy and realistic technique of dividing an RSA private key in between the user and a Security Mediator (SEM). IB-m RSA is uncomplicated, safe and very proficient. The chief scheme behind IBM RSA is the division of an RSA private key into two portions as in threshold RSA. One portion is provided to a user while the other portion is provided to a SEM. If the user and the SEM collaborate, they utilize their individual half-keys in a manner which is functionally equal to the standard RSA. The verity that the private key is not held completely by any one is clear to the outside, i.e., to those who

employ the equivalent public key. In addition, information of a half-key cannot be utilized in deriving the whole private key. Hence, neither the user nor the SEM can decipher or decrypt or sign a message with no mutual permission.

RSA is an internet encryption and verification scheme and is the most commonly used algorithm. The mathematical information of the algorithm is employed in acquiring the public and private keys [9]. The algorithm engrosses multiplying two big prime numbers and by means of additional operations derives a set of two numbers in which one set comprises the public key and other set comprises the private key. Both the public and the private keys are desired for encryption and decryption purposes but only the holder of private key desires to recognize it. By using the RSA system, the private key by no means requires to be sent across the Internet [6].

Algorithm

Choose large prime numbers p and q such that p~=q.
Compute n=p*q
Compute ϕ (p q) = (p-1)*(q-1)
Choose the public key e such that
gcd (ϕ (n), e) =1; 1<e< ϕ (n)
Select the private key d such that
d*e mod ϕ (n) =1
So in RSA algorithm encryption and decryption are
Performed as-
Encryption
Calculate cipher text C from plaintext message M
Such that
C=M ^e mod n
Decryption
M=C^d mod n=M^ed mod n [6].

.

III. METHODOLOGY

The chief scheme behind IBM RSA is the division of an RSA private key into two portions as in threshold RSA. One portion is provided to a user while the other portion is provided to a SEM. If the user and the SEM collaborate, they utilize their individual half-keys in a manner which is functionally equal to the standard RSA. The verity that the private key is not held completely by any one is clear to the outside, i.e., to those who employ the equivalent public key. In addition, information of a half-key cannot be utilized in deriving the whole private key. Hence, neither the user nor the SEM can decipher or decrypt or sign a message with no mutual permission.

A. Procedure for signing

1. USER: h ← H (m)
   Where H () is a suitable hash function such as SHA-1 and |H ()| < k
2. USER: send h to SEM.
3. in parallel:
   3.1 SEM:
      (a) If USER revoked return (ERROR)
      (b) PS_{sem} ← hdsem mod n
      (c) Send PS_{sem} to USER
   3.2 USER:
      (a) PS_u ← hdu mod n
4. USER: h' ← $(PS_{sem} * PSu)^e$ mod n
5. USER: If h' ≠ h then return (ERROR)
6. S ← $(PS_{sem} * PS_u)$ mod n
7. USER: return (h,S)

B. Procedure for decryption function

1. USER: m' ← encrypted message
2. USER: send m' to SEM
3. in parallel:
   3.1 SEM:
      (a) If USER revoked return (ERROR)
      (b) PD_{sem} ← m'^{dsem} mod n
      (c) Send PD_{sem} to USER
   3.2 USER:
      (a) PD_u ← m'^{du} mod n
4. USER: m ← $(PD_{sem} * PD_u)$ mod n
5. USER: return (m)

IV. SIMULATION PROCEDURE

Main purpose here is to calculate the processing time of each algorithm for different file sizes. Their implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme .The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased .Similar procedure has been followed to calculate the throughput of decryption scheme.

For my experiment, I have used Pentium Core 2 Duo of 2.20 GHz CPU speed with 2 GB RAM. In this experiment the text files sizes range from 10 KB to 70 KB. The performance metrics are analyzed by the following:

(a) Encryption/decryption time.

(b) CPU process time – in the form of throughput.

The calculation and analysis purpose for above, customized computer application program is developed in C#.NET platform and after execution for analysis purpose the data is shown in MS Excel from there we can direct create graphs for visual analysis.

EXPERIMENTAL RESULTS Encryption / decryption algorithms have been tested with different text size files using application program developed.

Table No. 1

Comparison of Blowfish, Two fish, RC2, IB-mRSA and RSA Algorithm

Algorithm	**Designers**	**Key-size**	**Block size**	**Algorithm structure**	**Rounds**
Blow fish	Bruce Schneier	32–448 bits	64 bits	Feistel network	16
Two fish	Bruce Schneier	128, 192 or 256 bits	128 bits	Feistel network	16
RC 2	Ron Rivest	8 to128 bits	64 bits	Feistel network	18
IBm-RSA	Xuhua Ding, Gene Tsudik	1,024 to 4,096 bit	Any byte length	----------	1
RSA	Rivest, Shamir, and Adleman	1,024 to 4,096 bit	Any byte length	----------	1

Table No. 2

EXECUTION TIME DIFFERENCE IN DIFFERENT CRYPTOGRAPIC ALGORITHMS

Input file size in KB	Execution time in ms for IB_mRSA	Execution time in ms for RSA	Execution time in ms for Blowfish Algorithm	Execution time in ms for Two fish Algorithm	Execution time in ms for RC2 Algorithm
10	4.0726	8.3955	7.2735	6.7436	6.8977
20	3.0968	10.8416	7.4227	6.8677	6.2239
30	5.7024	10.9732	6.9133	7.0539	6.8128
40	6.7936	11.4532	7.0938	6.0353	6.287
50	4.7477	11.9341	7.2026	6.8966	6.4204
60	9.3924	12.8256	7.0998	6.0675	6.272
70	8.7654	11.7645	7.2184	6.611	6.5945

V. SIMULATION RESULTS AND DISCUSSION

All The results show below in graphs and above in Table No.2 the superiority of IB_mRSA algorithm in terms of the processing time. More the throughput, more the speed of the algorithm & less will be the time used. Again, we can conclude that Blowfish is also the second best of all.

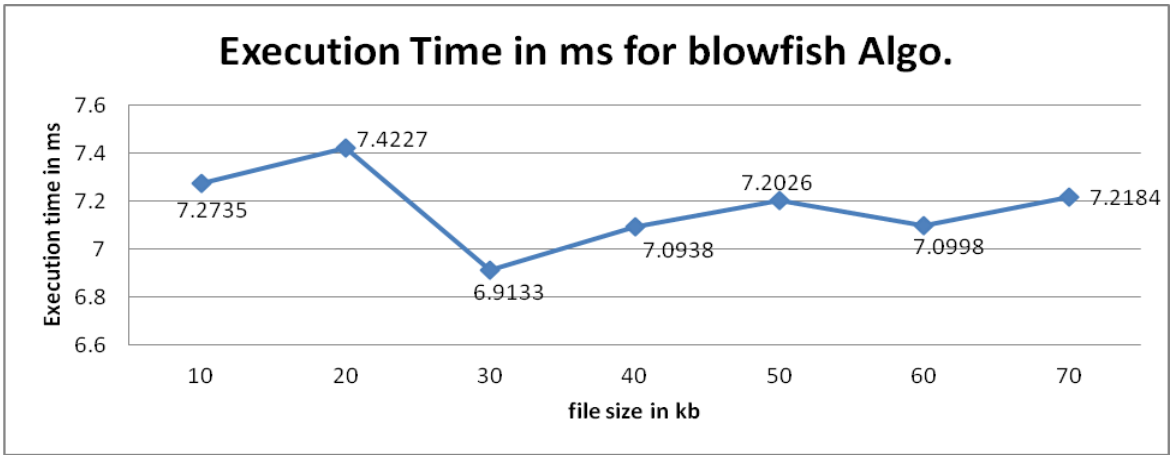

Fig (1) Execution Time Vs File Size in Kb for Blowfish

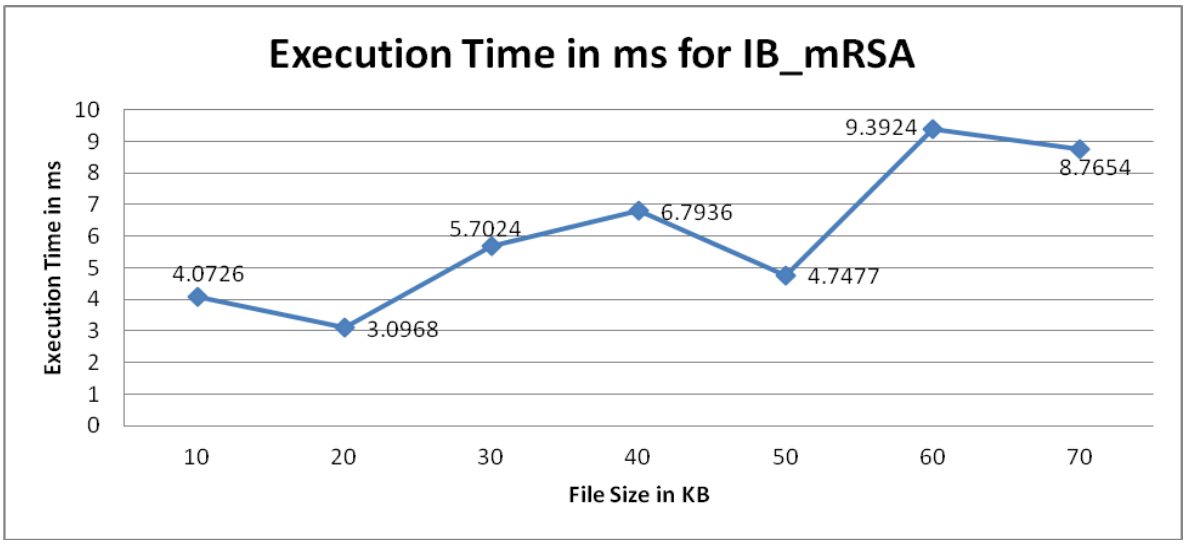

Fig (2) Execution Time Vs File Size in Kb for IB_mRSA

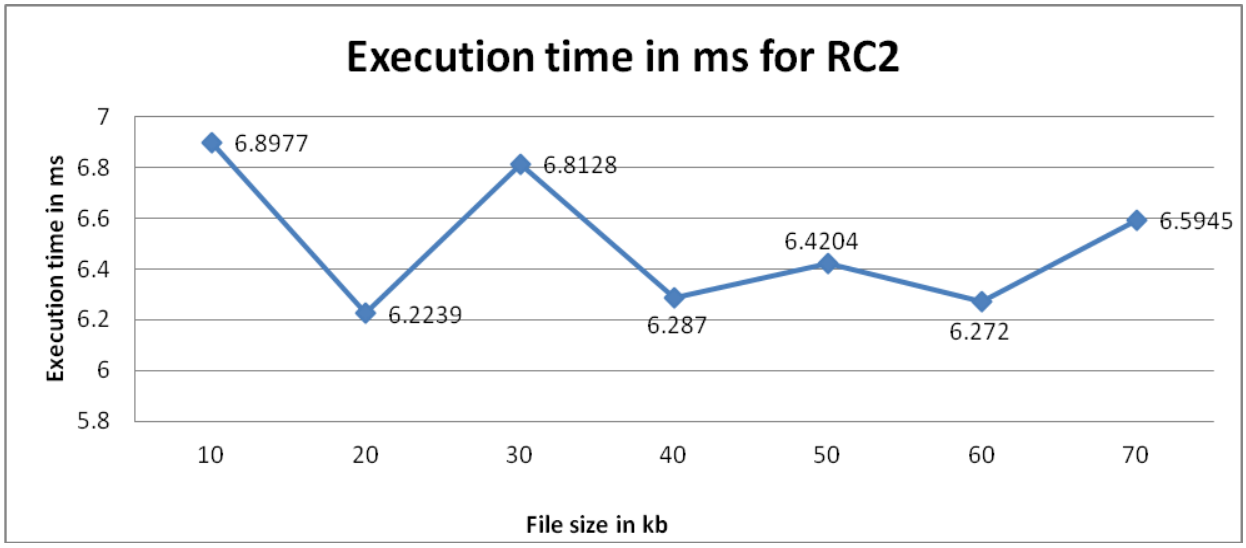

Fig (3) Execution Time Vs File Size in Kb for RC2

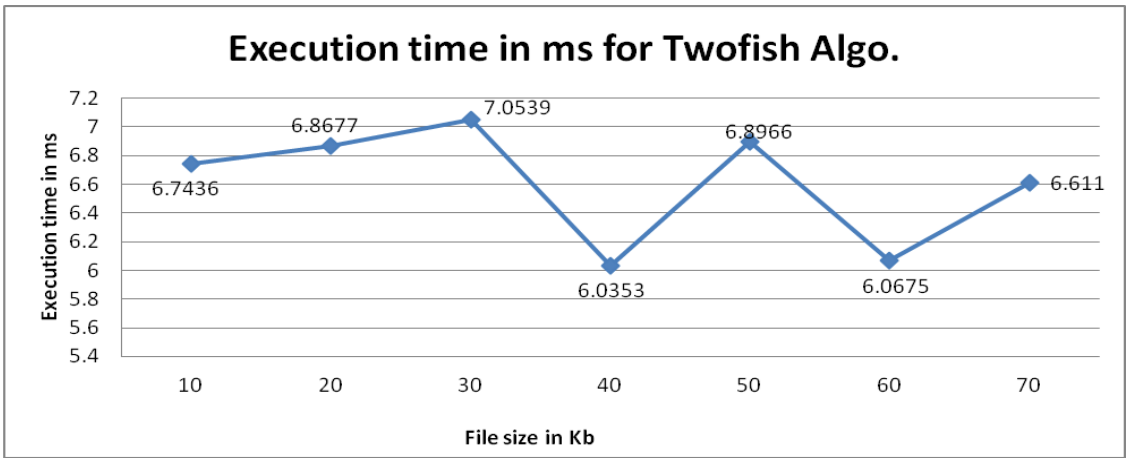

Fig (4) Execution Time Vs File Size in Kb for Two fish

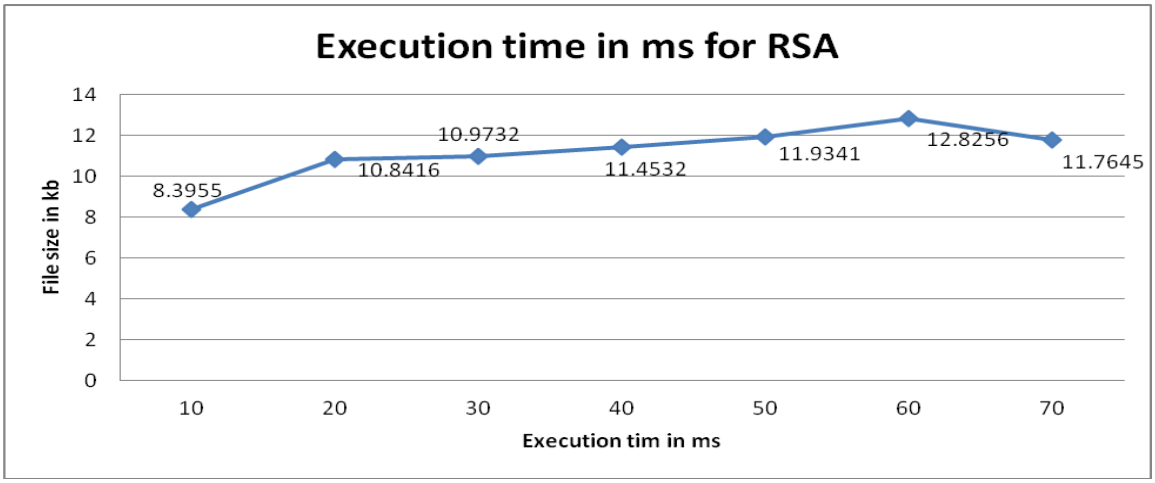

Fig (5) Execution Time Vs File Size in Kb for RSA

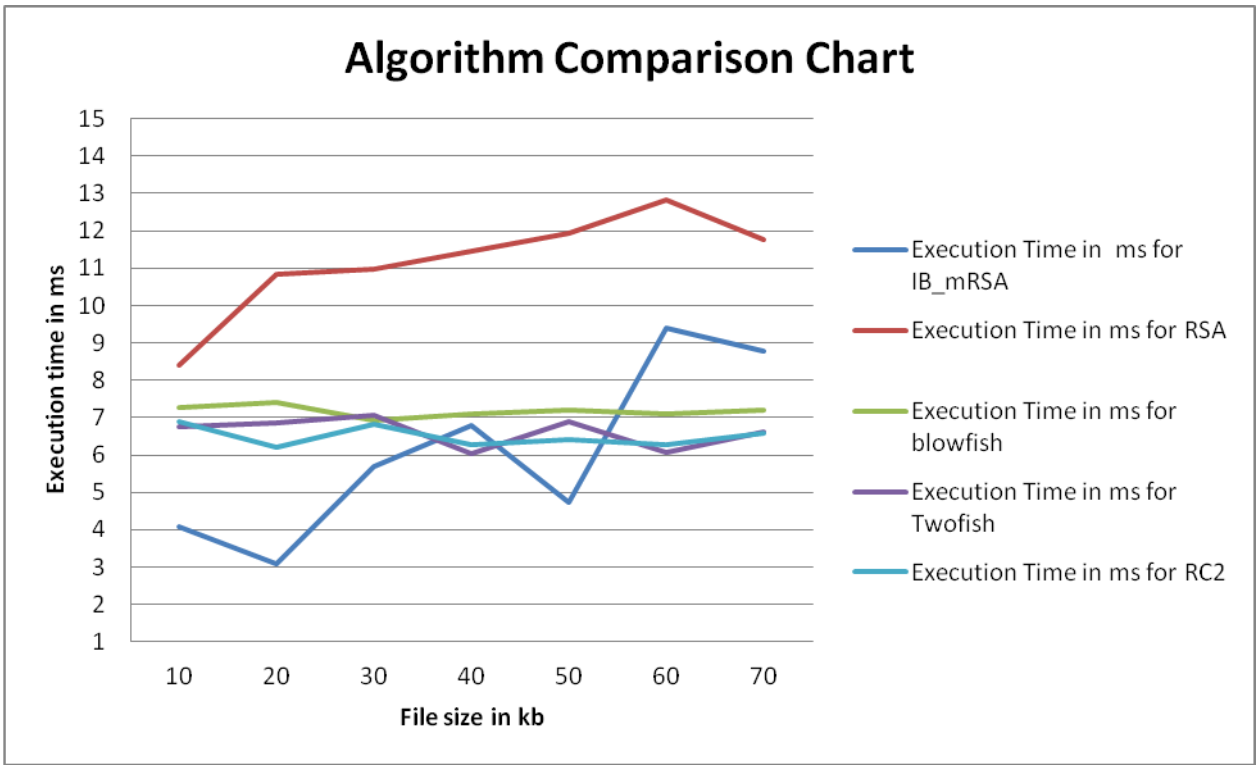

Fig (6) Execution Time Vs File Size in Kb for Comparison for Algorithms

VI. CONCLUSION AND FUTURE SCOPE

This paper presents the performance evaluation of selected cryptographic symmetric and asymmetric algorithms for various file sizes. From the presented simulation we can conclude that IB_mRSA is the first best algorithm and Blowfish is the second best has better performance than other algorithms. Secondly, IB_mRSA has advantage over the other algorithms in terms of throughput & processing time except Blowfish. Third point is that RSA has the least performance among all the algorithms mentioned here. In future the work may be extended by including the schemes and techniques over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and minimum time consumption.

REFERENCES

[1] Pratap Chnadra Mandal Asst. Prof, Dept of Computer Application B.P.Poddar Institute of Management & technology, West Bengal, India "Superiority of Blowfish Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 9, September 2012 ISSN: 2277 128X.

[2] T.D.B Weerasinghe "Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms" International Journal of Information & Network Security (IJINS) Vol.1, No.2, June 2012, pp. 77~87 ISSN: 2089-3299.

[3] G. Ramesh, Dr. R. Umarani "Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers" I.J. Information Technology and Computer Science, 2012, 12, 60-66.

[4] Dr. Sandeep Sharma and Rishabh Arora "Performance Analysis of Cryptography Algorithms" International Journal of Computer Applications (0975 – 8887) Volume 48– No.21, June 2012.

[5] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud" Evaluating the Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.

[6] Mohit Marwaha, Rajeev Bedi, Amritpal Singh and Tejinder Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS" International Journal of Advanced Engineering Technology E-ISSN 0976-3945.

[7] Irfan Landge, Tasneem Bharmal and Pooja Narwankar "Encryption and decryption of data using two fish algorithm" World Journal of Science and Technology 2012, 2(3):157-161 ISSN: 2231 – 2587.

[8] Purnima Gehlot, S. R Biradar and B. P. Singh "Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL" International Journal of Computer Applications (0975 – 8887) Volume 70– No.13, May 2013.

[9] Shashi Mehrotra Seth and Rajan Mishra" Comparative Analysis of Encryption Algorithms for Data Communication" IJCST Vol. 2, Issue 2, June 2011. I S S N: 2229-4333 (Print) |ISSN0976- 8491 (Online).

[10] Dan Boneh, Xuhua Ding, and Gene Tsudik "Identity-Based Mediated RSA" Department of Information and Computer Science, University of California, Irvine.

[11] Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud "Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009.1793-8201

[12] Pratap Chandra Mandal "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" Journal of Global Research in Computer Science Volume 3, No. 8, August 2012.

[13] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622. Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[14] Samuel King Opoku" A Robust Cryptographic System Using Neighborhood-Generated keys" International Journal of Research in Computer Science Volume 2 Issue 5 (2012) pp. 1-9.

