Enhancing the Speed of Encryption and Decryption

Rajneet kaur
Electronics and communication engineering,
ACET, Amritsar,
Punjab, India

Prof. V K Banga
Electronics and communication engineering,
ACET, Amritsar,
Punjab, India

***Abstract* : Security is one of the most challenging aspects in the internet and network applications. Encryption algorithms play a main role in information security systems .Internet and networks applications are growing very fast, so the needs to protect such applications are increased. This paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, RC6 and RSA. In this paper, we compare the various cryptographic algorithms. On the basis of parameter taken as time various cryptographic algorithms are evaluated on different size. Simulation results are given to demonstrate the effectiveness of each algorithm.**

Key Words: Encryption, Decryption, AES, DES, RC2, 3DES, Blowfish, RC6, RSA.

I. INTRODUCTION

In the last quarter of the 20th century, especially in the 90's, the field of cryptography has faced a new problem beyond privacy, which had been the main goal until that time. "We stand today on the brink of a revolution in cryptography" said Diffie and Hellman in 1976. After 2 years in 1978, an elegant implementation of the public-key cryptosystem came from Rivest, Shamir and Adleman, named as the RSA Public-Key Cryptosystem [1]. Today, because of the high-security provided, RSA is still known as the most widely used public-key cryptosystem in the world. Cryptography is concerned with keeping communication secret [3]. Today's Cryptography is more than secret writing. Cryptosystem such as authentication, integrity, and non- repudiation.

Cryptography generally refers to the method of making data invisible to any third party who the availability of such data could be potentially harmful to the original parties the data needs to be available to [2]. It deals mostly with the aspect of information security that includes data integrity, authentication and data confidentiality. This means that the parties exchanging information do not necessarily know each other; they may not even know the location of one another, but still need to exchange information or data, depending on the reason for communication existing between both parties.

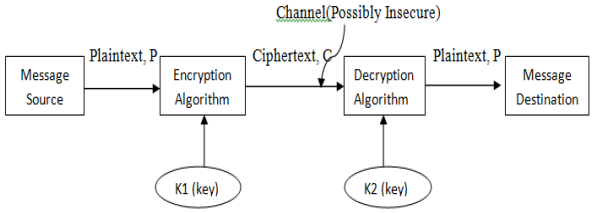

Fig 1: The components of Cryptography

An encrypted message is cipher text, denoted as *C***.** The process of recovering the original message from the encrypted data is called decryption [4]. It is the inverse function of the encryption. This general model shows that there are four basic tasks in designing a particular security service.

There are two categories of cryptography which includes symmetric key, also called secret–key cryptography, where the key is a shared secret between two communicating parties. Encryption and decryption both use the same key. and in asymmetric key, also known as public–key, cryptography a pair of keys is used in the communication process [7]. One of the keys, the private key, used by the receiver only, kept secret and not shared with anyone. The other key, the public key, used by the sender of the message, is not secret and can be shared with anyone.

Brief definitions of the most common encryption techniques are given as follows [5][6]:

A. DES (Data Encryption Standard)

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key length DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). DES consists of 16 steps, each of which called as a Round.

B. 3 DES

It is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. The

plain text block P is first encrypted with a key K1, then encrypted with second key K2, and finally with third key K3, where K1, K2 and K3 are different from each other. To decrypt the cipher text C and obtain the plain text, we need to perform the operation P= DK3 (DK2 (DK1(C))). It is a known fact that 3DES is slower than other block cipher methods.

C. *RC2*

It is also a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts.

D. *Blowfish*

Blowfish is block cipher 64-bit block - can be used as a replacement for the DES algorithm. It takes a variable-length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish.

E. *AES*

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. it encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

F. RC6

RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128,192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard .

G. RSA

The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA system in 1977. RSA stands for the first letter in each of its inventor's last names. RSA is now widely been used in electronic commerce protocols and is believed to be secure for sufficiently long keys . The typical size of n which is the product of the two prime numbers for RSA algorithm is 1024-bits or 309 decimal digits. The block size must be less than $\log 2n$.

II. RELATED WORK

This section discuss the results obtained from other resources alongwith the performance of the compared algorithms. The energy consumption of different symmetric key encryption is evaluated [8]. Using 3-DES for encryption of 5 MB file for 600 times the battery left is 45% and further encryption is not possible as battery dies. AES is considered faster as compared to other symmetric key schemes [11].

When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). While data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. Which is not noticeable. Number of rounds can be reduced to save power but it leads to insecure protocol for AES which is to be avoided. But for some cases to save power seven or more rounds can be considered. A study in [12] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [13].

In [14] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption.

III. EXPERIMENTAL DESIGN

For experiment, we use a laptop 2.4 GHz CPU, in which performance data is collected. In this experiments, encryption of different file size ranges from K byte to Mega Byte is done. Several performance metrics are collected: encryption time, decryption time, and total time [16]. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [15][26]. The decryption time is considered the time that an decryption algorithm takes to produce a plaintext from a cipher text. Then finally overall time of the input plaintext is calculated.

The following tasks that will be performed are shown as follows:

- A comparison is conducted between the results of the selected different encryption and decryption.
-A study is performed on the effect of changing data types - such as text or document and images-for each cryptography
- A study is performed on total time taken by algorithm.

IV. SIMULATION RESULTS

The results are given in Fig. 2 and Fig. 3 for the selected six algorithms of different sized files. Fig. 2 shows the results of encryption of different sized files while Fig. 3 gives the results of decryption analysis of different sized files. We can notice that these different size files are encrypted and decrypted by different cryptography techniques. Thus same files are encrypted by different methods.

The graph shows the Experimental result for Encryption algorithm AES, DES, 3 DES, RC6, BLOWFISH, RC2 and RSA are shown in table, which shows the comparison of various algorithm AES, DES, 3 DES, RC6, BLOWFISH, RC2 and RSA using same text file for experiment.

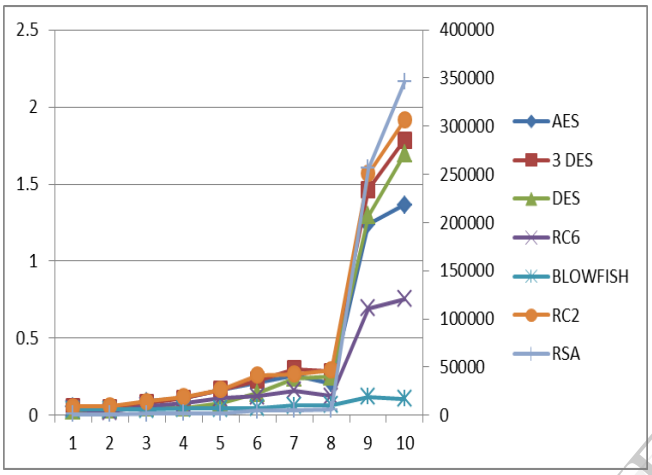

Fig 2: Encryption time of different cryptography algorithm

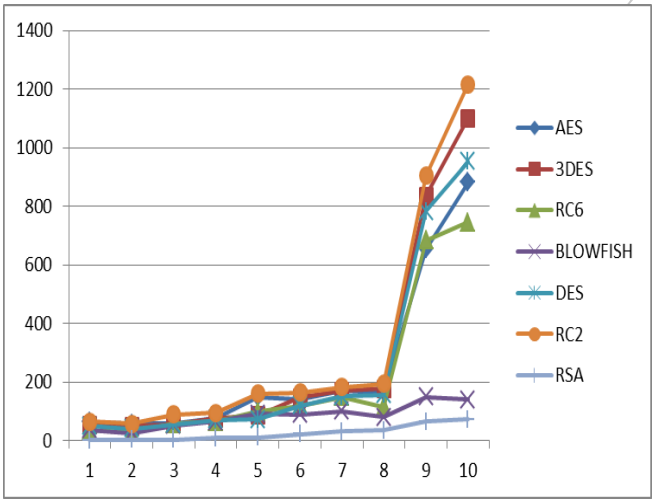

Fig 3: Decryption time of different cryptography algorithm

By analyzing the Table 3.8 we conclude that the encryption time taken by BLOWFISH is very small as compare to DES and relatively small as compared to RSA. Similarly, we conclude that the encryption time taken by DES is smaller than 2DES and relatively small as compared to RSA. After analyzing the different cryptography techniques we come to conclusion that RSA has taken the large encryption time as compare to other variants of cryptography.

By analyzing the graph, we conclude that the decryption time taken by BLOWFISH is very small as compare to DES and relatively small as compared to RSA. Similarly, we conclude that the decryption time taken by DES is smaller than 2DES and relatively small as compared to RSA. After analyzing the different cryptography techniques we come to conclusion that RSA has taken the large decryption time as compare to other variants of cryptography. The decryption time taken by AES, DES, 2DES, RC6, RC2, BLOWFISH, and RSA algorithms.

V. CONCLUSION

After the analysis of encryption time and decryption time of different algorithms of cryptography. We conclude that time taken for encryption on various size of text file by algorithms i.e AES, DES, 2DES, RC6, RC2, BLOWFISH, and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by other algorithm. BLOWFISH algorithm consumes least time for encryption. AES and DES algorithm show very minor difference in time taken for encryption.

Similarly, By analyzing of figure, which shows that time taken for decryption on various size of text file by algorithms i.e AES, DES, 2DES, RC6, RC2, BLOWFISH, and RSA, it is noticed that RSA algorithm takes much longer encryption time compare to encryption time taken by other algorithm. BLOWFISH algorithm consumes least time for encryption. AES and DES algorithm show very minor difference in time taken for encryption.

The analysis shows that time taken for decryption on various size of text file by algorithms i.e AES, DES, 2DES, RC6, RC2, BLOWFISH, and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by other algorithm. BLOWFISH algorithm consumes least time for decryption. AES and DES algorithm show very minor difference in time taken for encryption.

Similarly, By analyzing figure which shows that time taken for decryption on various size of text file by algorithms i.e AES, DES, 2DES, RC6, RC2, BLOWFISH, and RSA, it is noticed that RSA algorithm takes much longer decryption time compare to decryption time taken by other algorithm. BLOWFISH algorithm consumes least time for decryption. AES and DES algorithm show very minor difference in time taken for decryption.

VI. FUTURE WORK

The present work deals with plain text being represented by numerical and characters of English alphabet. This also includes encryption and decryption of images of different format, medical images and text files of different size. The work can be improved so that it can support the characters of not only English but also of other languages as well. The work can also be improved to support not only text but also other forms of message transmission like audio and video.

ACKNOWLEDGEMENT

There are many people that I would to thank for their support, encouragement and friendship throughout my studies and in particular during the making of this thesis. Firstly, I would like to thanks God. My humble respect to my parents and to my guide.

REFERENCES

1. R. Rivest, A. Shamir, and L. Adleman , "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" ,Communications of the ACM Vol. 21, No. 2, pp.120 - 126,1978.
2. Dan Boneh,"Twenty Years of Attacks on the RSA Cryptosystem", Notices of the AMS, Vol. 46, No. 2, Feb. 1999, pp. 203-213.
3. A.Fiat. Batch RSA. ,"Advances in Cryptology", Crypto ″89,Vol. 435, 1989, pp.175–185.
4. T. Collins, D. Hopkins, S. Langford, and M. Sabin, "Public Key Cryptographic Apparatus and Method", US Patent#5,848,159. Jan. 1997.
5. T. Takagi, "Fast RSA-Type Cryptosystem Modulo pkq",Crypto ″98, 1462 of LNCS. 1998, pp. 318–326
6. M. Wiener, "Cryptanalysis of Short RSA Secret Exponents", IEEE Transactions on Information Theory, Vol.36, No. 3, 1990, pp. 553–558.
7. Cesar Alison Monteiro Paixao, "An efficient variant of the RSA cryptosystem", preprints (2003).
8. Garg D,Verma S, "Improvement over Public Key cryptographic Algorithm", Advance Computing Conference,2009, IACC 2009, IEEE International Conference, March 2009, pp. 734-739
9. David Pointcheval, "New public key cryptosystem based on the dependent RSA problem", Eurocrypt″99 LNCS Springer-Verlag, 1999, Vol. 1592, pp.239-254.
10. J-J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem" ,Eletronic Letters, Vol. 18, 1982, pp. 905–907.
11. A.A. Mamun, M. M. Islam, S.M. M. Romman, A.H.S.U Ahmad, "Performance Evaluation of Several Efficient RSA Variants", IJCSNS VOL.8 No.7, July 2008, pp. 7-11.
12. H.Cohen, "A Course in Computational Algebraic Number Theory", Graduate Texts in Mathematics, Vol. 138, p. 137.
13. S. D. Galbraith, C. Heneghan, and J. F. McKee, "Tunable balancing of RSA", Proceedings Information Security and Privacy, 2005, Vol. 3574, pp. 280–292.
14. H.-M. Sun and Mu-En. Wu, "Design of Rebalanced RSACRT for Fast Encryption," Information Security Conference 2005. pp. 16-27.
15. M. J. Hinek, "Another look at small RSA exponents," Topics in Cryptology, CT-RSA 2006, 2006, Vol. 3860, pp. 82–98.
16. Camille Vuillaume. Efficiency Comparison of Several RSA Variants Master Thesis, Fachbereich Informatik derTUDarmstadt, 2003
17. Coppersmith, D., 1997. Small solutions to polynomial equations and low exponent RSA vulnerabilities. Journal of Cryptology 10, 233–260.
18. Coppersmith,D.,Franklin, M.,Patarin, J., Reiter, M., 1996. Low-exponent RSA with related message. In: Proceedings of Eurocrypt'96, LNCS, vol. 1070, pp. 1–9.
19. Durfee,G.,Nguyen,P.Q. "Cryptanalysis of the RSA schemes with short secret exponent form Asiacrypt'99".In: Proceedings of Asiacrypt'00, LNCS, vol. 1976, pp. 14–29.
20. Boneh, D., Durfee, G., 2000. " Cryptanalysis of RSA with private key d less than N0.292." IEEE Transactions Information Theory 46 (4),1339–1349.
21. D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N 0.292," IEEE Trans. on Information, Vol. 46(4), pp. 1339-1349, 2000.
22. D. Boneh, G. Durfee and Y. Frankel, "An Attacks on RSA Given a Small Fraction of the Private Key Bits," Advanced in Cryptology—ASIACRYPT '98, LNCS 1514, Springer-Verlag, pp.25-34, 1998.
23. G. Durfee, P. Q. Nguyen, "Cryptanalysis of the RSA Schemes with Short Secret Exponent form Asiacrypt '99," Advances in Cryptology-Asiacrypt'00, LNCS 1976, Springer-Verlag, pp.1-11,2000.
24. A.Niven, H. S. Zuckerman, "An Introduction to the Theory of Number," John Wiley and Sons Inc,1991.
25. M. J. Wiener, "Cryptanalysis of RSA with short secret exponents," IEEE Transactions on information Theory, IT-36, pp.553-558, 1990.
26. Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha , "Performance Evaluation of Symmetric Cryptography Algorithms ", in IJECT Vol. 2, Issue 3, Sept. 2011 ,ISSN : 2230-9543
27. W. Stallings. Cryptography and Network Security, Prentice Hall, 1995.
28. Zirra Peter Buba & Gregory Maksha Wajiga "Cryptographic Algorithms for Secure Data Communication International "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.