International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

A Review On Different Encryption Techniques: A Comparative Study

Dharitri Talukdar[1], Prof (Dr.) Lakshmi P. Saikia[2]

[1]Ph.D Scholar, Assam down town University, Guwahati, Assam, India

[2] Professor & Head , Dept. of Computer Sc. & Engineering, Assam down town University, Guwahati, Assam, India

lp_saikia@yahoo.co.in contact no. +91-9854040442

ABSTRACT- In today's competitive digital economy, the applications of cyber world require high level of security for expensive data. In recent years, a lot of research has taken place in direction to trim down the security issues by contributing various approaches. Cryptography is such a technique to secure data. Cryptography means secret (crypto) writing (graphy). Cryptography can be categorized into symmetric cryptography and asymmetric cryptography. This paper covers fair comparison between four most commonly used symmetric and asymmetric key algorithms: DES, AES, BLOWFISH, and RSA which are helpful in network security.

KEYWORDS- Cryptography, Encryption, Decryption, DES, AES, BLOWFISH, RSA.

INTRODUCTION -Cryptography is a requisite element of avoiding private data from being purloined. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium for example network like Internet. The main goal of cryptography is to keep the data secure for its intended user only. Encryption is the process of converting normal text to unreadable form; while decryption is the process of converting encrypted text to normal text in the readable form [1]. There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. **:** In symmetric key cryptography, the same key is used by both the parties. In asymmetric key cryptography, there are two keys: private key and public key. Both are required to encrypt and decrypt a message or transmission.

Furthermore, symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively [1].

METHODOLOGY

- ***i)*** Comparing and analyzing the performance of various cryptography algorithms (DES, AES, BLOWFISH, RSA) in terms of throughput, execution time, power consumption and key size.
- ***ii)*** Analyzing the performance of the algorithm when different types of data issued.

COMPARATIVE ANALYSIS - Here these four algorithms are compared with each other on the basis of ten different factors. These factors and their meaning are listed below.

- ***i)*** Developed in: This factor shows that in which year the specific algorithm was developed.
- ***ii)*** Designer by: This factor shows that by whom the specific algorithm was designed.
- ***iii)*** Type of algorithm: It shows that algorithm is symmetric key algorithms or asymmetric key algorithms.
- ***iv)*** Key used: It shows that key used for encryption or decryptions are same or different.
- ***v)*** Key size: This factor shows key length used for algorithm.

vi) Block size: This factor shows key length used for algorithm.

vii) Round: It shows the digit of function used.

viii) Scalability: It shows the ability to work with the growth.

ix) Flexibility: It shows that any type of modification can be possible by the algorithm or not.

x) Power consumption: It displays the power consumption of the algorithm.

ALGORITHM COMPARISON - Here are the tables which represent the comparison between the four algorithms based on ten factors.

Table I. Basics of compared algorithm [2], [3], [4]

Algorithms	**Developed**	**Designer**	**Type of algorithm**	**Key used**
DES	1977	IBM	Symmetric	Same
AES	2000	Rijmen, Daemen	Symmetric	Different
BLOWFISH	1993	Bruce Schneier	Symmetric	Same
RSA	1977	Rivest, Samir and Adleman	Asymmetric	Different

Table II. Work and structure related comparison [2], [4], [5]

Algorithms	**Key size(bit)**	**Block size(bit)**	**Round**	**Scalability**	**Flexibility**	**Power consumption**
DES	64	64	16	Scalable	No	low
AES	128,192or 256	128	18	No	Yes	low
BLOWFISH	32-448	64	16	No	Yes	low
RSA	1024 to 4096	Any byte length	1	No	Yes	high

RELATED WORK

Thambiraja et.al showed that AES consumes highest processing power among DES, 3DES, BLOWFISH. AES is better than RC4 for smaller packets also it is better for live video streaming transmission compared to RC4 and XOR. Time taken by RSA is much higher than that of AES and DES. Memory usage of RSA is high compared to AES, DES. Output byte in RSA is less as compared to AES and DES.RC4 is fast and energy efficient than AES for larger packets. Time for encryption and decryption almost remains constant for RC4 if key size is increased and less time is required to encrypt as compared to AES, DES, and 3DES [6].

Sumedha Kaushik et.al concluded that according to information content test, and randomness test, it was found that the 3DES (ECB) cryptographic Technique is stronger in comparison to other cryptographic Techniques. It can be implemented in C++, Java, and Dot net for encrypting text files [7].

Thakur et.al showed that AES can be implemented more comfortably in high and low level language as compared to DES. Blowfish has better performance when packet size is changing as compared to AES, DES, 3DES, RC2, and RC6 [8].

Sanchez-Avila C. et al. studied that in October 2000, after three years of competition between 15 candidate algorithms, the National Standards and Technology (NIST) chose the Rijndael algorithm to be adopted as Advanced Encryption Standard (AES) by the U.S. Department of Commerce, replacing to Data Encryption Algorithm (DES), which has been the standard since 1977. The

authors analyse the structure and design of new AES, following three criteria: a) resistance against all known attacks; b) speed and code compactness on a wide range of platforms; and c) design simplicity; as well as its similarities and dissimilarities with other symmetric ciphers. On the other side, the principal advantages of new AES with respect to DES and T-DES, as well as its limitations, are investigated. Thus, for example, the fact that the new cipher and its inverse use different components, which practically eliminates the possibility for weak and semi-weak keys, as existing for DES, and the non-linearity of the key expansion, which practically eliminates the possibility of equivalent keys, are two of the principal advantages of new cipher. Finally, the implementation aspects of Rijndael cipher and its inverse are treated. Thus, although Rijndael is well suited to be implemented efficiently on a wide range of processors and in dedicated hardware [9].

Othman O. Khalifa et.al [10] discussed basic concepts, characteristics, and goals of various cryptography. In today's information age, communication plays an important role which is contributed to growth of technologies therefore privacy is needed to assure the security that is sent over communication media.

Meyer C.H. et al. proposed that Cryptography is the only known practical method for protecting information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. Administrative and physical security procedures often can provide adequate protection for offline data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection. The authors gives an overview of cryptographic methods using symmetric and asymmetric algorithms and demonstrates why future cryptographic applications should use a hybrid approach, i.e., combination of symmetric and asymmetric (public key) methods [12].

Punita Meelu et.al presented the fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security since AES provides better security and has less implementation complexity and has emerged as one of the strongest and most efficient algorithms in existence today. It also includes several computational issues, optimization of cipher as well as the analysis of AES security aspects against different kinds of attacks including the countermeasures against these attacks and also highlighted some of the important security issues of AES algorithm [11].

CONCLUSION -This paper presents the performance evaluation of selected cryptographic symmetric and asymmetric algorithms for various file sizes. It can be concluded that DES is only scalable and is not flexible among compared algorithms. From the second table we can see that key size of RSA is biggest. As the key size is biggest it is harder to break the security. Power consumption of RSA is higher than other compared algorithms.

REFERENCES:

[1] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed "Review on Comparative Study of Various Cryptography Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015 ISSN: 2277 128X.

[2] Priyanka Raval, Jeegar Trivedi "Comparative Analysis of Eight Different Cryptographic Algorithms with Fourteen Factors" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014 ISSN: 2277 128X.

[3] Preeti and Bandana Sharma "Review Paper on Security in Diffie-Hellman Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014 ISSN: 2277 128X .

[4] Harshraj N. Shinde, Aniruddha S. Raut, Shubham R. Vidhale, Rohit V. Sawant, Vijay A. Kotkar "A Review of Various Encryption Techniques" International Journal Of Engineering And Computer Science, ISSN:2319-7242, Volume 3 Issue 9 September, 2014 Page No. 8092-8096

[5] Lalit Singh and Dr. R.K. Bharti "Comparative Performance Analysis of Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013 ISSN: 2277 128X

[6] E. Thambiraja, G. Ramesh and Dr. R. Umarani "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: 2277128X.

[7] Sumedha Kaushik and Ankur Singhal "Performance Evaluation Using Cryptographic Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012 ISSN: 2277 128X.

[8] Jawahar Thakur and Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011, ISSN 2250-2459.

[9] Sanchez-Avila C., Sanchez-Reillol R. "The Rijndael block cipher (AES proposal): a comparison with DES" IEEE 35th International Carnahan Conference on Security Technology, pp. 229 – 234, 2001.

[10] Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S. Shebani "Communication Cryptography" 2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.

[11] Punita Mellu and Sitender Mali "AES: Asymmetric key cryptographic System" International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[12] Meyer C.H. "Cryptography-a state of the art review" Conference on VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks, pp. 4/150 - 4/154, 1989