



Symmetric Key Algorithms: A Comparative Analysis

Rajasekaravarman.S¹, Joshna.S²

M. Sc Student, Dept. of CT, Sri Krishna Arts and Science College, Coimbatore, India¹

Assistant Professor, Dept. of CT., Sri Krishna Arts and Science College, Coimbatore, India²

ABSTRACT: With the advancement of technology internet and various communication techniques that pass through it has grown in prominence each day. However along with this advancement has also grown the threat of hackers and malicious groups. There has been several passive and active attacks making the role of data security pretty important. Most of the time the data passed via internet might contain confidential or personal information which many people would want to be protected against attacks. Various data encryption algorithms has been developed to make sure that the data transmitted via internet is secure from any sort of hacking or attacks. Several cryptographic algorithms also have been developed for encryption and with each one having some advantages and disadvantages. This paper presents a detailed study of symmetric encryption/decryption algorithms and its advantages and disadvantages.

KEYWORDS: Symmentric key algorithm; Encryption; Decryption; Attacks

I. INTRODUCTION

Data exchanging via internet has become an inevitable factor in our day to day life. Even though private networks exist generally people prefer data access and transfer via internet which has become the fastest and the easiest means of data communication. A variety of confidential data/information is exchanged through internet which includes ATM passwords, bank dealings, medical records and information, personal details etc. Confidential and sensitive information should always be protected from hackers. For protection various encryption algorithms are currently used one way or other and it has emerged as the most common method of data protection. Cryptography algorithms play an important role in data protection. To put in simple terms Cryptography is the art of changing plain text to cipher text or encrypted text. The art of breaking ciphers, called cryptanalysis, and the art devising them which is cryptography is collectively known as cryptology. Cryptography has two stages to it. One is encryption where the plain text is converted to cipher text. The second stage is at the receiver end where the cipher text is decrypted back to the original text. Mainly we can classify cryptography into three encryption models 1) Symmetric key encryption models 2) Asymmetric key encryption models 3) Hash functions (Mathematical) models In this paper we are concentrating on symmetric key encryption models and tries to compare the performance of the most popular encryption algorithms.

II. RELATED WORK

The presentation is about the comparison in performance of four most useful algorithms: DES, 3DES, AES and BLOWFISH. Performance of different algorithms is different according to data loads. In the case of changing key size – it can be seen that higher key size leads to clear increase in time needed for encryption. Paper [2] provides a comparison between some symmetric and asymmetric techniques. The factors are achieving an effectiveness, flexibility and security, which is a face of researchers. As a result, the better solution to the symmetric key encryption and the asymmetric key encryption is provided. From [3] evaluation of encryption algorithms like AES, DES, 3DES, RC2, Blowfish, and RC6 are done. That paper tested each of these algorithms and conducted a comparison of these algorithms. The results showed that Blowfish was the best encryption algorithm. Comparison between the different symmetric and asymmetric encryption/decryption algorithms are explained in [4] [5] [6] and [7]. Hardware performance of symmetric algorithms are discussed in [9]. This allows us to choose the best available one on the basis of their performance parameter. As technology has grown it can be all the more important as various functions in our day to day life as reprogrammable devices are highly necessary places where for hardware implementations of



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

encryption algorithms as they provide cryptographic algorithm agility, physical security, and potentially much higher performance. This hardware design is applied to the new secret and variable size key block cipher called Blowfish designed to meet the requirements of the previous known standard and to increase security and to improve performance.

III. SYMMETRIC KEY ALGORITHMS

As part of our performance analysis we have selected the below symmetric algorithms. DES (Data Encryption Standard): DES is a block cipher encryption algorithm. This is the first encryption standard that was published by NIST. It is a symmetric algorithm which means it is operated by the same key for encryption and decryption. It uses one 64-bit key [1] [4] and [13]. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation, 8bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is in the reverse order of encryption. The output is a 64-bit block of cipher text. Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher key. 3DES It is an enhancement of DES. As a part of incrementing the security it developed 3 keys for encryption/decryption. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. It uses 64 bit block size with 192 bits of key size [1] [4]. The encryption method is similar to the one used in the original DES but applied 3 times to increase the encryption level and the average safe time. But it takes more time for encryption/decryption.

AES: Advanced Encryption Standard (AES) also known as the Rijndael algorithm. It is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible [1] [13] and [14]. It can be implemented on various platforms especially in small devices. AES has been tested for many security applications.

BLOWFISH: It is one of the most common public domain encryption algorithms provided by Bruce Schneider - one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security [1] [4] and [13]. Blowfish is 64-bit block cipher used to replace DES algorithm. Ranging from 32 bits to 448 bits, variable length key is used. Variants of 14 round or less are available in Blowfish. Blowfish is unpatented and license-free and is available free for all uses.

IV. COMPARISON OF ALGORITHMS

A comparison of the various algorithms is given below.

	DES	3DES	AES	BLOWNFISH
Designers	IBM	IBM	JOAN DAEMEN & VINCENT RIJMEN	BRUCE SCHNEIER
First Published	1977	1998	1998	1993
Derived from	Lucifer	DES	Square	
Key size	56 bits	112 bits or 168 bits	128 bits, 192 bits, 256 bits	32-448 bit in steps of 8 bits. 128 bits by default
Block size	64 bits	64 bits	128 bits	64 bits
Rounds	16	48	10, 12 or 14 depending on key	16
Attacks	Brute force attack, differential cryptanalysis,	Chosen plain text attacks or known plain text attacks.	Brute force attack, Biclique attack, Related-key attacks	Second order differential attack

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

	linear cryptanalysis			
Cipher type	Block cipher	Block cipher	Block cipher	Block cipher
Security	In secure	Secure than DES	Secure	Secure
Keys	Single	Single key divided into three	Single	Public
Speed	Fast	Slow than DES	Fast	Fast
Power	High than AES	Higher than DES	Higher than Blow fish	Very low
Throughput	Lower than AES	Lower than DES	Lower than Blow fish	Very High
Encryption	High	Moderate	High	High

V. RESULTS

COMPARISON OF ALGORITHMS ON THE BASIS OF SPEED.

Size of input (MB)	DES	3DES	AES	Blowfish
2	1	3	2	1
5	2	6	4	2
10	3	9	6	3
50	10	30	12	8
100	18	55	25	15

Table 2 – Shows the time taken for encryption for each algorithm in seconds.

Size of input (MB)	DES	3DES	AES	Blowfish
2	1	2	1	1
5	1	3	2	2
10	2	6	4	3
50	8	24	8	7
100	15	45	20	12

Table 3 – Time taken for Decryption for each algorithm in seconds.

VI. CONCLUSION AND FUTURE WORK

From the studies which we have performed considering security, throughput, speed, encryption/decryption, power consumption and other factors, it is shown that blowfish algorithm having good performance than other symmetric algorithm like DES and 3DES, AES having better performance. The memory requirement of symmetric algorithms is lesser than asymmetric encryption algorithms and symmetric key algorithms runs faster than asymmetric key algorithms. Further, symmetric key encryption provides more security than asymmetric key encryption. AES even though its widely used today, it uses more processing power when compared with other algorithms.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

REFERENCES

- [1] Milind Mathur and Ayush Kesarwani "Comparison Between DES , 3DES ,RC2 , RC6 , BLOWFISH And AES", Proceedings of National Conference on New Horizons, university of Oklahoma, , ISBN 978-93-82338-79-6,2013.
- [2] Ritu Tripathi and Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC), Volume 1, Issue 6. ISSN 2348 – 4853, June 2014.
- [3] Mr. Gurjeevan Singh, Mr. Ashwani Singla, and Mr. K.S. Sandha, "Cryptography Algorithm Comparison for Security Enhancement In Wireless Intrusion Detection System", International Journal of Multidisciplinary Research Vol.1 Issue 4, ISSN 2231- 5780, August 2011.
- [4] 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.
- [5] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah and Obaid Ur Rehman, "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012, ISSN (Online): 1694-0814.
- [6] Ranjeet Masram, Vivek Shahare, Jibi Abraham and 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.
- [7] Swapna B Sasi, Dila Dixon and Jesmy Wilson, "A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security", IOSR Journal of Engineering (IOSRJEN), Vol. 04, Issue 03 ||V3|| PP 01-04,(March. 2014).
- [8] Anjali Patil and Rajeshwari Goudar "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, VOLUME 2, ISSUE 8, AUGUST 2013, 2006.
- [9] Deepak Kumar Dakate and Pawan Dubey, "Performance Comparison of Symmetric Data Encryption Techniques" , International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.
- [10] E. Surya and C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Vol 2(4), 475-477.
- [11] Monika Agrawal and Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSSE), Vol. 4
- [12] Abdel-Karim Al Tamimi "Performance Analysis of Data Encryption Algorithms" .
- [13] 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, ISSN 2250-2459, Volume 1, Issue 2, December 2011.
- [14] Joan Daemen , Vincent Rijmen "ADVANCED ENCRYPTION STANDARD (AES)", FIPS PUB November 26, 2001.
- [15] SparkIM project DLL for blowfish - <http://www.codeproject.com/Tips/235342/Blow-fish-Encryption-Implementation-in-Net>.

BIOGRAPHY

Rajasekaravarman.S is a MSc Student in Computer Technology, Sri Krishna Arts and Science College, Coimbatore, TamilNadu, India.

Ms.Joshna.S is working as Assistant Professor at Department of CT, Sri Krishna Arts and Science College, Coimbatore, TamilNadu, India.