ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

An Analytical Analysis of Stream Cipher and Block cipher Algorithms

Harsh Dhiman[1], Md Asif Mushtaque[2], Shahnawaz Hussain[3]

School of Computing Science and Engineering, Galgotias University, U.P., India

Abstract— Cryptography is an art or science to provide security for sharing of information over the internet. Cryptography changes the format of original text into another format that is not easy to understand by unwanted user. There are different types of cryptography techniques are available. Cryptography algorithm is generally described into twp types- Symmetric key encryption and asymmetric key encryption. This paper gives the overview of some symmetric key encryption algorithm. In this paper we also compared these algorithms on their architecture.

Keywords— Stream Cipher, Block Cipher, Cryptography, RC4, RC6, symmetric key, asymmetric key, encryption, decryption.

I. INTRODUCTION

Cryptography is a very important technique to protect data against attacks from unauthorised user. It protects data by changing the format of data into another format. Two main operations are performed in cryptography encryption and decryption. Encryption is a process to convert original message into another format known as cipher text, it uses a secret key and an encryption algorithm to encrypt data while decryption is the reverse process of encryption to obtain original data from cipher text. Decryption also requires a secret key and a decryption algorithm. Main objectives of cryptography are- Confidentiality: it ensures that the only authorized people can access the information, authentication- it confirms the identity of person communicating on the network, Integrity- it means protect data from modification by unauthorised people and non-repudiation- ensure that sender or receiver cannot deny the communication. Cryptography is generally described into two types (a) Symmetric Key and (b) Asymmetric key.

(a) Symmetric key Encryption:

Symmetric key encryption is a type of encryption in which a single key is used by sender and receiver. Same algorithm is used by sender and receiver side. It is also known as secret key or private key cryptography. It is faster than asymmetric key but sometimes symmetric key algorithm is easy to crack by applying different types of attack. AES, DES, TDES, Blowfish, RC4, RC6 are the example of secret key encryption algorithm.

(b) Asymmetric is differing from symmetric key algorithm as it uses two keys to encrypt and decrypt. It is more secure because one key is used to encrypt data and another key is used to decrypt data. It is also known as public key encryption. It is completely based on mathematical function for their process. In public key cryptography receiver has their own public key and sender has own private key. RSA, DSA, ECC are the example of asymmetric key encryption algorithm.

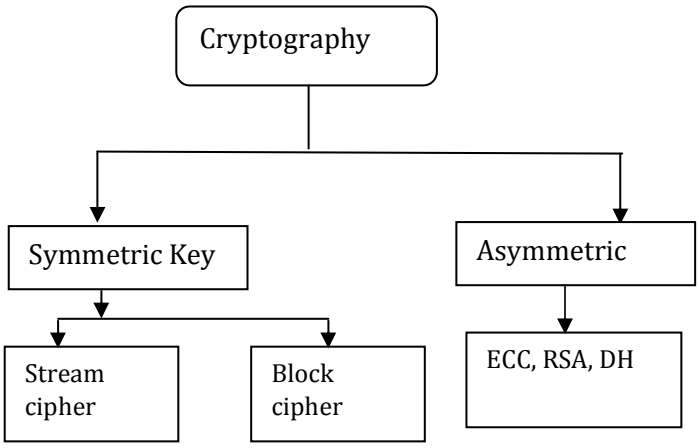

Fig.1. Categories of Cryptography

ISSN: 2321-9653

II. SYMMETRIC KEY ALGORITHM

A. ADVANCE ENCRYPTION STANDARD:

AES is a 128 bit block text encryption algorithm designed by Joan Daemen and Vincent Rijmen in 1998, this algorithm is adopted by the US Government in 2000. AES is a symmetric key encryption algorithm with variable length key of 128, 192 and 256 bits. It is based on substitution-permutation structure, and performs 10, 12 or 14 round. The number of rounds depends on the key [1]. It operates on 4x4 columns and performing some operations on matrix. These operations are:

- Subbyte step
- Shiftrows step
- Mixcolumn step and
- Addround key step

AES performs 10 rounds if the key size is 128 bits, 12 rounds if the key size is 192 bits and 14 rounds if the key size is 256 bits. There are some operations which is performed in each step of AES such as: Key expansion, Initial round, Rounds and Final rounds. The performance of AES is higher than other related algorithm and it is also very secure algorithm [1, 13].

B. RC4:

RC4 was developed by Ron Rivest of RSA in 1987. It supports key size of 40-2048bitsand performs total 256 rounds. It is very important and commonly used in protocols such as TLS and WEP. RC4 is observed that it is not very secure algorithm because of using non-random key. It generates pseudorandom key stream which is combining with the plaintext for encryption using Exclusive-or operation. RC4 was never officially released by Ron Rivest. The main weakness of RC4 is a weak key mixing state, these keys can easily detect by some attacks. In RC4 the permutation operation is performed by key using the key scheduling algorithm and then the stream of bits is obtained by using pseudo random generation algorithm [4, 12].

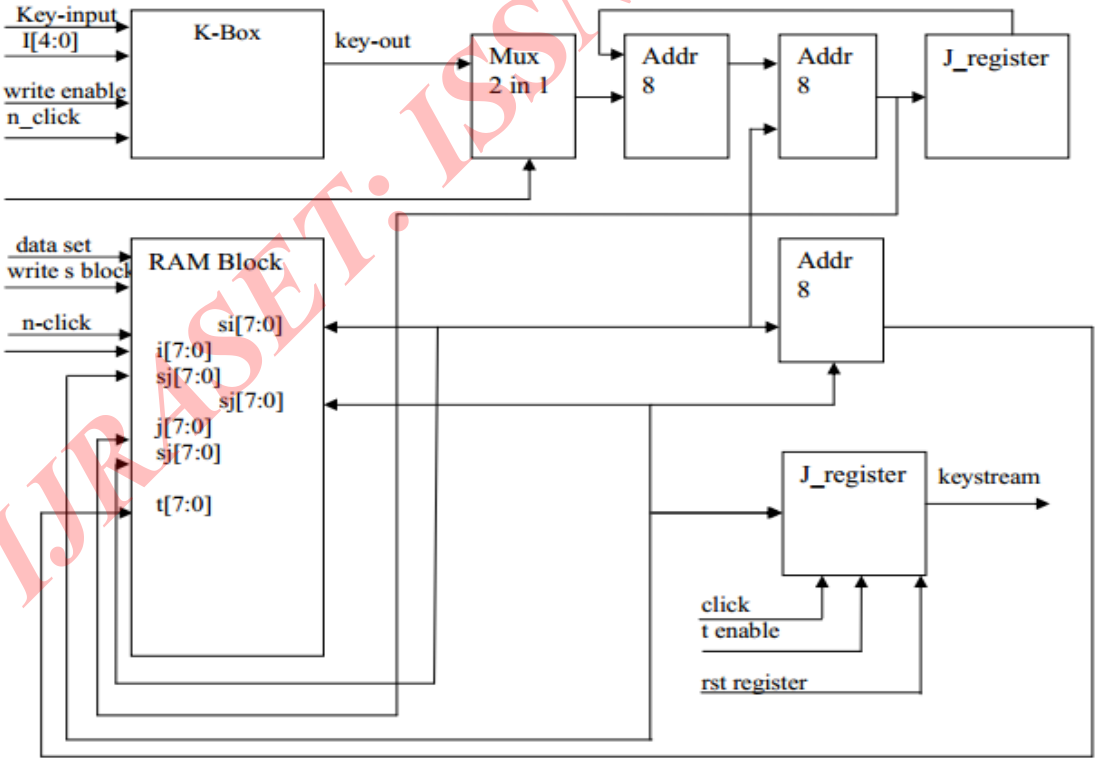

Fig.2. Transformation of RC4

C. RC6: It is symmetric key block cipher algorithm, RC6 is derived from RC5. It is based on Feistel network and supports 128 bits block size, 128, 192 and 256bits key size and processes total 20 rounds [5]. It provides better security than RC5 and it is differed from its

Predecessor because it uses four registers rather than two and performs some extra operation. RC6 looks alike two parallel execution of RC5. Generally the performance of RC6 and memory used by RC6 are equal. RC6 protects data against differential attacks.

The main advantages of RC6 are it can be extended in future up to 2048 but the length must be in multiple of 32. Up to 17 rounds RC6 can be cracked by some attacks otherwise it is observed as a secure encryption technique [4].

III. COMPARISON

Factors	**AES**	**RC4**	**RC6**
Created By	Joan Daemen and Vincent Rijmen	Ron Rivest in 1994	Yiqun Lisa Yin in 1998
Block size	128	2064 bits (1,684 effective)	128 bits
Key Length	128, 192 or 256 bits	40– 2048 bits	128, 192 or 256 bits
Rounds	10, 12, 14	256	20
Algorithm Structure	Feistel N/w	Feistel N/w	Feistel N/w
Effective Ness	Effective in both S/W and H/W	Effective in both S/W and H/W	Slow
Attacks	Side channel attacks	Fluhrer Mantin and Shamir attack	Brute force Attack

Table1. Comparison of Encryption Algorithm

IV. Conclusion

This paper gives the complete comparison between various symmetric key encryption algorithms. From the above comparison and a survey, we found that AES is best among these algorithms. RC4 is not more secure because of its simplicity, but RC4 is efficient in both hardware as well as software. RC6 is observed as a secure algorithm, but its performance is not so high and it is not more efficient in hardware. AES is secure because several attacks tried to crack AES but not even a single attack can crack this algorithm. Because of its security level the US Government adopted AES. AES is also efficient in both hardware as well as software. From this analysis we analyse that stream cipher encryption algorithm is faster than block cipher but there is a challenge to increase its security level.

V. ACKNOWLEDMENT

I would like to thank all those people who helped me in my thesis work including this paper and those peoples who guided me with their hard work.

References

[1] MD Asif Mushtaque, Harsh Dhiman, Shahnawaz Hussain and Shivangi Maheshwari, "*Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity*", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[2] Shraddha Soni, Himani Agrawal and Dr. (Mrs.) Monisha Sharma, "*Analysis and Comparison between AES and DES Cryptographic Algorithm*", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.J

[3] E. Surya and C. Diviya, "*A Survey on Symmetric Key Encryption Algorithms*", International Journal of Computer Science & Communication Networks, Vol. 2(4), 475-477.

[4] Limor Elbaz & Hagai Bar-El, "*Strength Assessment of Encryption Algorithms*", October 2000, website: http://www.discretix.com/PDF/Strength%20Assessment%20of%20Encryption%20Algorithms.pdf

[5] Kirti Aggarwal, Jaspal Kaur Saini, Harsh K. Verma, "*Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers*", International Journal of Computer Applications (0975 – 8887), April 2013, Volume 68– No.25, pp. 10-16.

[6] Tingyuan Nie, Yansheng Li and Chuanwang Song, "*International Conference on Computing, Control and Industrial Engineering*", IEEE, 2010.

[7] 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, July 2012.

[8] Michal Halas, Ivan Bestak, Milos Orgon, and Adrian Kovac, "*Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks*", IEEE, 2012.

[9] 1Shashi Mehrotra Seth, 2Rajan Mishra, "*Comparative Analysis of Encryption Algorithms for Data Communication*", IJCST Vol. 2, Iss ue 2, June 2011.

[10] Anjali Patil, Rajeshwari Goudar, "A *Comparative Survey of Symmetric Encryption Techniques for Wireless Devices*", International Journal of Scientific & Technology Research Vol. 2, Issue 8, 2013.

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

[12] Nidhi Singhal, J.P.S.Raina, "*Comparative Analysis of AES and RC4 Algorithms for Better Utilization*", International Journal of Computer Trends and Technology- July to Aug Issue 2011.

[13] A. K. Mandal, C. Parakash and M. A. Tiwari, "*Performance Evaluation of Cryptographic Algorithms: DES and AES*", 2012 IEEE Student's Conference on Electrical, Electronics and Computer Science.

[14] E. Thambiraja, G. Ramesh and Dr. R. Umarani "A *Survey on Various Most Common Encryption Techniques*", IJARCSSE, Volume 2, Issue 7, July 2012.

[15] 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.

[16] Comparison of ciphers, "*Summary of Algorithms*", Website: http://www.javamex.com/tutorials/cryptography/ciphers.shtml.

[17] RSA Laboratories, "*RC6 Block Cipher*", 2012, Historical: RSA Algorithm: Recent Results on OAEP Security: RSA Laboratories submissions.