International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 3, March 2015 **ISSN 2319 - 4847**

CRITICAL ANALYSIS OF CRYPTOGRAPHIC ALGORITHM FOR DATA SECURITY

Dhanashri R. Kadu [1], Dr.G.P.Dhok[2]

[1]ME (EXTC) Scholar, Department of EXTC,
Sipna College of Engg. & Tech., Amravati-444605, India

[2]Head Department of Instrumentation,
Sipna College of Engg. & Tech., Amravati-444605, India

ABSTRACT

Information security is the process of protecting information. The main issue of Reading or tapping data is secrecy and confidentiality. Confidentiality has always played an important role in diplomatic and military matters. Often Information must be stored or transferred from one place to another without being exposed to an opponent or enemy. The main aim of presenting this paper is to encrypt a Data using Rijndael Algorithm. The first aspect that has to be considered in our paper is Data security and the need for Data security. Key management is also related to Confidentiality. This deals with generating, distributing and storing key . To write this paper I have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, I am presenting my proposed work. This paper is dividing in Seven sections. In section-I, I am presenting just basic introduction about Information Security using cryptography, in section-II, I am presenting description of Rijndael algorithm, in section-III, I am presenting anatomy and the design of rijndael algorithm, and in section IV I am Presenting terminologies key and block size, in section V I am presenting strength of rijndael algorithm, in section VI I am presenting the performance comparison between rijndael and DES algorithms and in VI section I am presenting conclusion and references where I have completed my review report.

Keywords:-Decryption, Encryption, Key, Cipher Text,.

1.INTRODUCTION

Encryption: It is the process by which we can encode the data to prevent the access to unauthorized users from accessing or changing the data.Prevents unwanted access to documents and e-mail messages. Strongest levels of encryption are very difficult to break. Recent changes in cryptography export laws should expand access to software. If you're not paranoid, maybe you should be. If you use a PC, unscrupulous types can intercept e-mail you send, and coworkers could be reading your documents. Encryption--the process of encoding data so that it requires a special key to be read--can protect your data from prying eyes. Once the domain of spies, encryption is fast becoming an advisable precaution for businesses and home users: It's your best tool for protecting your trade secrets and privacy. So as to provide better security my paper suggest the rijndael algorithm for data security. On October 2000 and having reviewed further public analysis of the finalists, NIST decided to propose Rijndael as the Advanced Encryption Standard (AES). Rijndael, designed by Joan Daemen (Proton World International Inc.) and Vincent Rijmen (Katholieke Univeriteit Leuven) of Belgium, is a blockcipher with asimple and elegant structure [2]

2.OVERVIEW OF RIJNDAEL ALGORITHM

The Rijndael Algorithm (pronounced “Reign Dahl,” “Rain Doll” or “Rhine Dahl”) is the new Advanced Encryption Standard (AES) recommended by the US National Institute of Standards and Technology (NIST) for protecting sensitive, unclassified government information. NIST has been using other encryption algorithms, such as DES (Data Encryption Standard), Triple DES and Skipjack for encrypting important government information. However, it felt in 1997 the need for a new stronger encryption algorithm to circumvent any potential threats to these algorithms from advanced hackers. Consequently, on 2 January 1997, NIST announced the initiation of the AES development effort. NIST made a formal call for algorithms on 12 September 1997. The key requirements to be fulfilled by the submitted algorithms were that they be royalty-free publicly-disclosed algorithms based on symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits with key sizes of 128-bits, 192-bits and 256-bits. As a result of this call, 15 candidate algorithms from members of the cryptographic community around the globe entered the first round of scrutiny.

3.ANATOMY OF RIJNDAEL

Since Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array.
With an iterated block cipher, the different transformations operate in sequence on intermediate cipher results (states). The design of Rijndael is based on easily understandable mathematical concepts including finite field mathematics and linear algebra for matrix manipulation.

4.KEY AND BLOCK SIZE

A prime feature of Rijndael is its ability to operate on varying sizes of keys and data blocks. It provides extra flexibility in that both the key size and the block size may be 128, 192, or 256 bits. Since Rijndael specifies three key sizes, this means that there are approximately 3.4 x 1038 possible 128-bit keys, 6.2 x 1057 possible 192-bit keys and 1.1 x 1077 possible 256-bit keys
The Sub key and the Key Schedule The sub keys are derived from the cipher key using the Rijndael key schedule. The cipher key is expanded to create an expanded key and the sub key is created by deriving a 'round key' by round key. The required round key length is equal to the data block length multiplied by the number of rounds plus 1. Therefore, the round keys are taken from the expanded key.
To maintain a secure system, the expanded key is always derived from the cipher key. This method ensures that the expanded key is never directly specified, which would open Rijndael up to several cryptanalytic attacks against its key generation methods. Recall that the security of this system depends entirely on the secrecy of the key, as the design of the algorithm itself is public and contains no secrecy.
Whole Byte operations There are several mathematical preliminaries that define the addition and multiplication operations within a finite field and with matrices. When performing finite mathematics, the bytes are treated as polynomials rather than numbers, which can allow different and occasionally allows for more simple implementations

5.POWER OF RIJNDAEL

Daemen and Rijmen have specified Rijndael's advantages based on implementation aspects, simplicity of design, variable block length and extensions. Rijndael's implementation is very flexible since it can be used with varying key sizes and block sizes. It is also possible to change the sequence of some steps in Rijndael without affecting the cipher. The cipher is has a simple and elegant structure. It does not hide its structure by using complex components. Instead, it benefits from the advantages gained by the use of simple components in a well defined structure. Rijndael's security is based on the interaction of the cipher's individual components.
Rijndael is described as having a 'rich algebraic structure' which allows the cipher's security to be easily assessed in a limited time frame. This is an advantage over more complex designs that require extensive thinking, searching and 'bit tracing'. Rijndael is consistently a very good performer in both hardware and software across a wide range of computing environments. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments. There is additional security in that Rijndael's operations are among the easiest to defend against power and timing attacks
Rijndael's advantages based on implementation aspects, simplicity of design, variable block length and extensions Rijndael's implementation is very flexible since it can be used with varying key sizes and block sizes.

TABLE IV. COMPARING DES AND AES

	DES	AES
Key Length	56 bits	128, 192, or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher
Block Size	64 bits	128, 192, or 256 bits
Developed	1977	2000
Cryptanalysis resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and Square attacks
Security	Proven inadequate	Considered secure
Possible Keys	2^{56}	2^{128}, 2^{192}, or 2^{256}

Possible ASCII printable character keys*	95^7	95^{16}, 95^{24}, or 95^{32}
Time required to check all possible keys at 50 billion keys per second**	For a 56-bit key: 400 days	For a 128-bit key: 5×10^{21} years

6.RIJNDAEL AND DES COLLATION

DES keys are only 56 bits long, which means there are approximately 7.2 x 1016 possible DES keys. Therefore, there are on the order of 1021 times more AES 128-bit keys than DES 56-bit keys [5] Since Rijndael specifies three key sizes, this means that there are approximately 3.4 x 1038 possible 128-bit keys, 6.2 x 1057 possible 192-bit keys and 1.1 x 1077 possible 256-bit keys DES with 64-bit key, and data length of, also, 64 bits. DES in CBC configuration, in order to compute 128 bits of data with a 64-bit key Rijndael algorithm in its simplest form: 128-bit key, 128-bit data length.

7.CONCLUSION

In this paper the structure and the format of rijndael have been analyzed with its advantages, and proposed the comparison between AES and DES with some entities such as key length, cipher type ,block size etc. If any user emphasis on security or he wants better security for his secure data then rijndael algorithm should be taken into consideration. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption.

REFERENCES

[1] National Institute of Standards and Technology, Data Encryption Standard, FIPS 46-2, 1993.
[2] J. Daemen and V. Rijmen, AES Proposal: Rijndael, version 2, 1999. Available from URL: http://www. Esat.kuleuven.ac.be/vijmen/rijndael
[3] B. Schneier and D. Whiting, A Performance Comparison of the Five AES Finalist, 15 March 2000.
[4] J. Daemen and V. Rijmen, The Design of Rijndael, published by Springer-Verlag, 2002.
[5] AES webpage at US National Institute of Standards and Technology website:http://csrc.nist.gov/encryption/aes/
[6] The Rijndael's Algorithm URL: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
[7] N. Koblitz, A Course in Number Theory and Cryptography, Springer- Verlag New York Inc., 1987.
[8] M. Matsui, Linear Cryptanalysis method for DES cipher, Advances in Cryptology, Proc. Eurocrypt' 93, LNCS 765, Springer-Verlag, 1994,pp. 386- 397.
[9] S. Murphy and M. Robshaw, New observations on Rijndael, version of August 7, 2000. Available from URL: http://isg.rhbnc. ac.uk/inrobshaw.
[10] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.
[11] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT
[12] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security, Volume (1) : Issue (1).
[13] Advanced Cryptanalytic algorithm for data security published in international journal ijaiem volume(2) issue (3)2013
[14] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010

AUTHORS

Miss.Dhanashri R. Kadu Received Bachelor's Degree inElectronicAnd Telecommunication from Sant Gadge Baba Amravati University in S-2012 & Pursuing Master Degree In EXTC from Sipna College of Engineering. Amravati-444605.

Prof. DR. G.P.Dhok Head Of The Instrumentation Deapartment ,Sipna College of engineering Amravati -444605.