Effective Symmetric Key Block Ciphers Technique for Data Security: RIJNDAEL

Rupinder Kaur, Dr. Madhu Goel

Abstract: In today's scenario, the use of internet are growing increasingly across the world, security becomes a prime concern of issue for the society. With the advent of computers in every field, the need of software tools i.e. Security for protecting files and other information stored on the computer became important. Cryptographic algorithms play a vital role in providing data security which is the art of achieving security by encoding messages to make them non-readable. This research paper presents five Symmetric Key-Block Ciphers Algorithms : AES, RIJNDAEL, DES, 3 DES, RC2 and propose a technique to serve as a guideline for the selection of an appropriate algorithm for a particular input file to encrypt or decrypt. to improve their performance by calculating the execution speed and throughput of Encryption and Decryption method.

Keywords: AES, RIJNDAEL, Cryptography, Data Security, Symmetric Algorithms.

I. INTRODUCTION

Our daily lives are often very dependent on secure communication of information. A thing likes credit card payments at banks, online shopping at book shop, and mobile phone calls to our friends or transferring the information through internet all require a way to keep the information confidential and correct. So, Cryptography provides a way where any entity can communicate securely in adversarial environments. Cryptographic technique are of two types- Symmetric and Asymmetric. Symmetric, if both the sender and the receiver of a information are using the same private key. In contrast to this, cryptographic technique is Asymmetric, if sender and receiver are using different keys, typically a ―Public for encryption and a ―Private for decryption.

Symmetric cryptography technique are very efficient in practically than Asymmetric cryptography technique, most security applications use Symmetric cryptography to ensure the Privacy, the Authenticity and the Integrity of sensitive data. Even most applications of Public-key cryptography are actually working in a hybrid way by transmitting a cipher key with Asymmetric techniques while symmetrically encrypting the payload data under the cipher key. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power. The work here will concentrate on the Symmetric cryptography technique with the aim of providing a brief overview of algorithms of cryptography, a couple of experimental study results to select best algorithm for data security.

II. OVERVIEW OF ALGORITHMS

1 DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) .Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher .

2 Triple DES: 3DES 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. It is a known fact that 3DES is slower than other block cipher methods.

3. RC2: RC2 is 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.

4. AES: AES is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds.

5. RIJNDAEL: It is extension of AES which has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas RIJNDAEL can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits.

III. PROPOSED WORK

Here, we studied some common encryption algorithms like AES, 3DES, DES, RC2, RIJNDAEL. It was shown in [2] that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly. It was concluded in [3] that AES is faster and more efficient than other encryption algorithms. 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).

Increasing the key size by 64-bits of AES leads to increase in energy consumption about 8% without any data transfer. If we reduce the number of rounds leads to power savings. This paper managed as follows: Introduction in section I, Overview of algorithms in section II, Proposed work in section III, Experimental Design in section IV, Results in Section V and last section VI explains the conclusion and future scope of present study.

ISSN: 2278 – 7798

IV. EXPERIMENTAL DESIGN

For our experiment a System with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 is used in which the performance data are collected. In this experiment software encrypts any file size that ranges from KB to MB. Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm.
The performance parameter which is used i.e. throughput. The throughput of encryption as well as decryption schemes is calculated one by one. In the case of Encryption scheme throughput is calculated as the average of total plain text in k bytes/m bytes divided by the average Encryption time/ Execution Time for encryption .Similarly, in the case of Decryption scheme throughput is calculated as the average of total cipher text is divided by the average Decryption time/Execution time for decryption.

V. RESULTS

All the five Encryption Algorithms have been tested with different input file (s) sizes. The figures display the graphs associated with the parameters for both encryption and decryption.
ENCRYPTION PROCESS:

In this section, the comparison between encryption algorithms has been conducted for any data files.

A. AUDIO FILES

We will make a comparison between types of data like Audio file to check which one can perform better. Experimental result for AUDIO data type is shown:

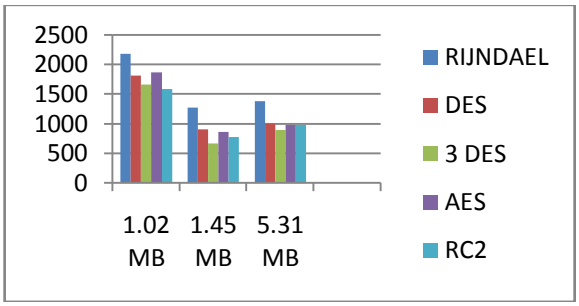

Fig. 1: Throughput of each encryption algorithm (Megabyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

B. PDF FILES

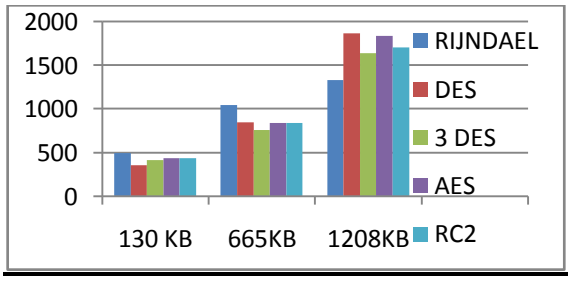

Fig. 2: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDEAL is best for smaller input files like for 130 KB file and 665 Kb file but for larger input files like for 1208 KB DES is best from all other algorithms because its throughput is more so performance is better.

C. IMAGE FILES

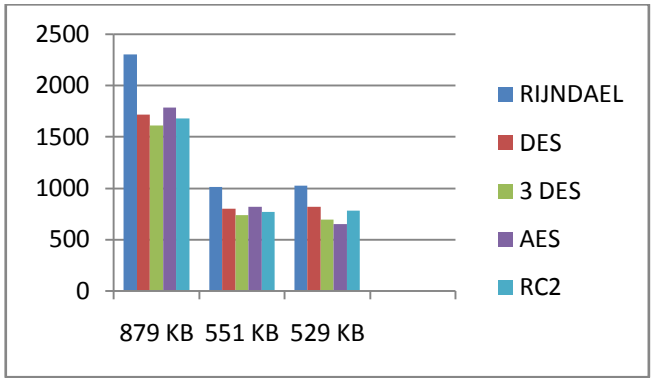

Fig. 3: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

D. PPT FILES

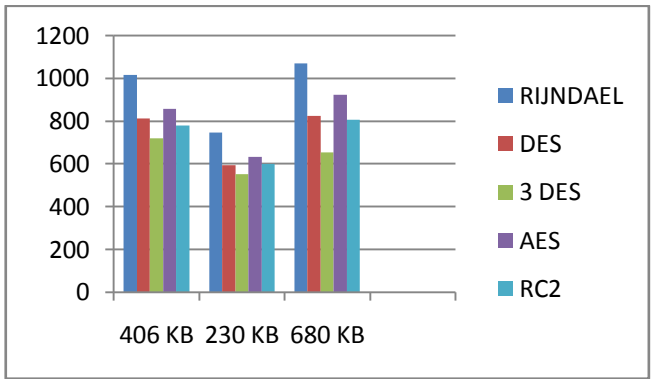

Fig.4: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

E. VIDEO FILES

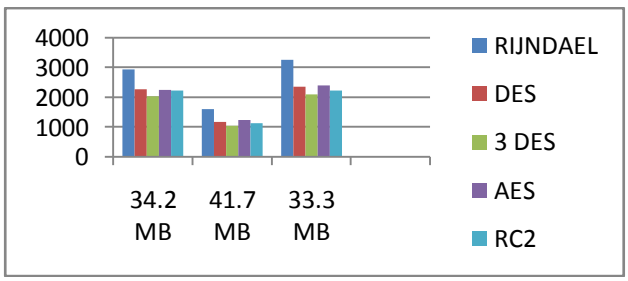

Fig. 5: Throughput of each encryption algorithm (Megabyte/Sec)

ISSN: 2278 – 7798

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

DECRYPTION PROCESS:

A. PDF FILES

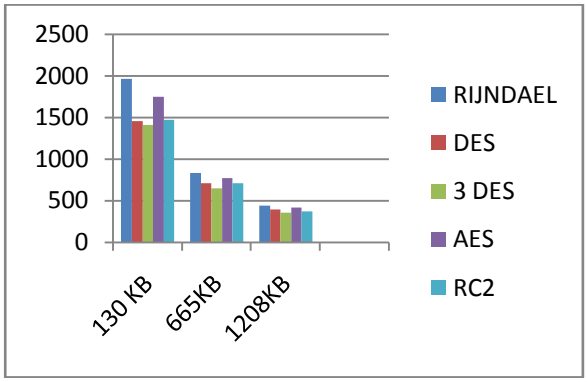

Fig. 6: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

B. AUDIO FILES

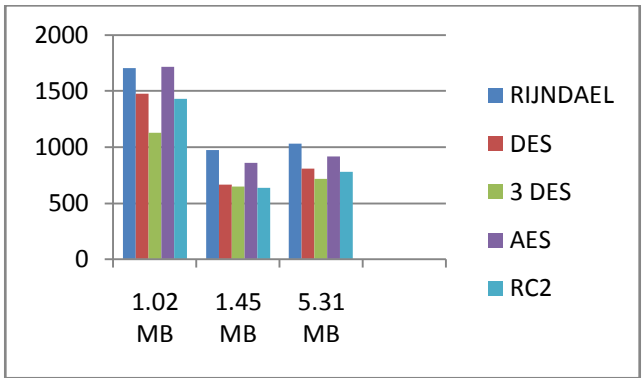

Fig. 7: Throughput of each encryption algorithm (Megabyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

C. IMAGE FILES

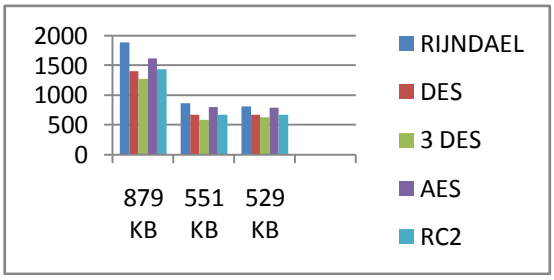

Fig. 8: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

D. PPT FILES

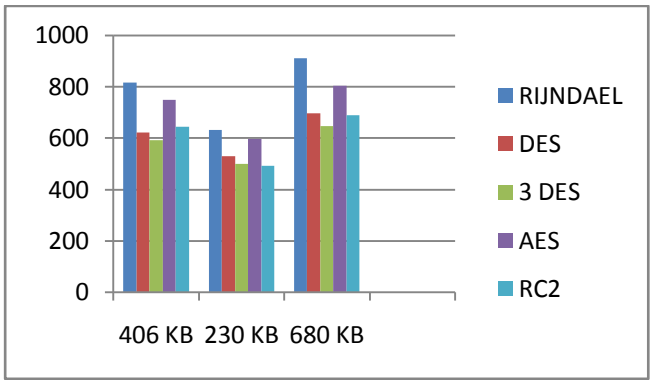

Fig. 9: Throughput of each encryption algorithm (Kilobyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

E. VIDEO FILES

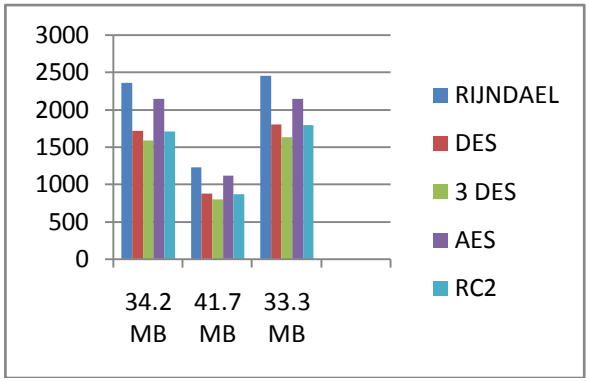

Fig. 10: Throughput of each encryption algorithm (Megabyte/Sec)

Here, RIJNDAEL is best from all other algorithms because its throughput is more so performance is better.

The simulation results for this comparison are shown in number of figures. The result shows the superiority of RIJNDAEL algorithm over the other algorithms in terms of the throughput of encryption and decryption process. Because more the throughput; more the speed of the algorithm & performance is better. Second point can be noticed here that DES has advantage over the other algorithms in terms of throughput for encryption process in some files which are somewhat larger in size like in PDF files.

VI. CONCLUSION AND FUTURE SCOPE

This paper presents the performance evaluation of selected symmetric key-block ciphers algorithms. The selected algorithms are AES, 3DES, RC2, RIJNDAEL, DES. The presented simulation results show the numerous points. It was concluded that RIJNDAEL has better performance than other algorithms in terms of throughput. In future we can perform

ISSN: 2278 – 7798

same experiments for other block ciphers symmetric algorithms for message transmission like on image, audio, video, pdf, ppt, excel as well. For our future work, we will suggest three approaches to reduce the energy consumption of security protocols: Replacement of standard security protocol primitives that consume high energy while maintaining the same security level, modification of standard security protocols appropriately, a totally new design of security protocol where energy efficiency is the main focus and developing a stronger encryption algorithm with high speed and minimum energy consumption.

ACKNOWLEDGMENT

I would like to articulate my profound gratitude and indebtedness to my guide and to my college (KITM), for their generous help in various ways for the completion of this paper.

REFERENCES

[1] Coppersmith, D. *"The Data Encryption Standard (DES) and Its Strength against Attacks."* IBM Journal of Research and Development, May 1994, pp. 243-250.

[2] Ruangchaijatupon, P. Krishnamurthy, *''Encryption and Power Consumption in Wireless LANs-N,''* The Third IEEE Workshop on Wireless LANs -September 27-28, 2001-Newton, Massachusetts.

[3] S.Hirani, *''Energy Consumption of Encryption Schemes in Wireless Devices Thesis,''* university of Pittsburgh, April 9, 2003.

[4]. R.Chandramouli, "*Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC),''* Vol. 9 Issue 2, May 2006.

[5] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader, Mohie Mohamed Hadhoud, "*Performance Evaluation of Symmetric Encryption Algorithms",* International Journal of Computer Science and Network Security, Dec 2008. .

[6] W.Stallings, *''Cryptography and Network Security 4th Ed,''* Prentice Hall, 2005, pp. 58-309.

[7] J. Daemen, and V. Rijmen, "Rijndael*: The advanced encryption standard,"* Dr. Dobb's Journal, pp. 137-139, Mar. 2001.

[8] S. Z. S. Idrus, and S. A. Aljunid, *"Performance anal-ysis of encryption algorithms text length size on web browsers,"* IJCSNS International Journal of Com-puter Science and Network Security, vol. 8, no.1, pp.20-25, Jan. 2008.

[9] K. McKay, Trade-offs between Energy and Security in Wireless Networks Thesis, Worcester Polytechnic Institute, Apr. 2005.

[10] K. Naik, "*Software implementation strategies for power-conscious systems*," Mobile Networks and Ap-plications, vol. 6, pp. 291-305, 2001.

[11] A. A. Tamimi, Performance Analysis of Data Encryption Algorithms, Retrieved Oct. 1, 2008.(http://www.cs.wustl.edu/_jain/cse567-06/ftp/encryption perf/index.html)

[12] Results of Comparing Tens of Encryption Algorithms Using Different Settings- Crypto++ Benchmark, Re-trieved Oct. 1, 2008. (http://www.eskimo.com/ wei-dai/benchmarks.html)

[13] A. Nadeem and M. Y. Javed, *"A performance comparison of data encryption algorithms*," Information and Communication Technologies, ICICT 2005, pp.84-89, 2005.

[14] Ramesh G, Umarani. R, " UR5*:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation"*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 Page 16-22. 2010.

[15] Ramesh G, Umarani. R," *Data Security In Local Area Network Based On Fast Encryption Algorithm",* International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.

[16] S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin. "*The Security of the RC6 Block Cipher. Version 1.0 ".* August 20, 1998.

[17]Ramesh, G. Umarani, R. ,UMARAM: A novel fast encryption algorithm for data security in local area network http://ieeexplore.ieee.org /xpl/ freeabs_all.jsp? arnumber=5670740

[18] W.S.Elkilani, "H.m.Abdul-Kader, "*Performance of Encryption Techniques for Real Time Video Streaming,* BIMA Conference, Jan 2009, PP 1846- 1850.

[19] Jose J. Amador, Robert W.Green, *"Symmetric-Key Block Ciphers for Image and Text Cryptography",* International Journal of Imaging

[20] ANSI3.106, "American National Standard for Information Systems—Data Encryption Algorithm—Modes of Operation," American National Standards Institute, 1983.

[21] AES Proposal: Rijndael, John Daemen and Vincent Rijmen, September 3, 1999.

[22]*Data Encryption Standard(DES*).Available:http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[23] Microsoft Unveils Next Version of Visual Studio and .NET Framework". Microsoft.http://www.microsoft.com/presspass/press/200 8/sep08/09 29vs10pr.mspx. Retrieved 17-06-2011.

[24] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.

[25] Dr. Madhu Goel,Rupinder Kaur,"A Review of Some Popular Encryption Techniques", International Journal of Software and Web Sciences,pp. 41-45,May 2014.

[26] Dr. Madhu Goel,Rupinder Kaur,"Survey Study-Symmetric Key Encryption Algorithms",International Journal of Advanced And Innovative Research,Vol.3,Issue 5,pp. 131-135,May 2014

ISSN: 2278 – 7798