https://doi.org/10.46335/IJIES.2023.8.3.4 **e-ISSN: 2456-3463**
Vol. 8 , No. 3, 2023, PP. 19- 23

International Journal of Innovations in Engineering and Science, www.ijies.net

Review on Performance Analysis of Lightweight Cryptographic Algorithm-CLEFIA

Atul H. Karode[1], Dr. Shekhar R Suralkar[2]

[1]Ph D Research Scholar,
[1] Department of E&TC, SSBT's College of Engineering and Technology, Bambhori Jalgaon Jalgaon 425001 (India)
[2]Professor
[2] Department of Computer Engg., SSBT's College of Engineering and Technology, Bambhori Jalgaon Jalgaon 425001 (India)

atulkarode@gmail.com

***Received on**:29 March,2023* ***Revised on**: 09 April,2023* ***Published on**:11 April,2023*

Abstract- *CLEFIA algorithm is a 128-bit block cipher with its key length being 128, 192 and 256 bits respectively, which is consistent to AES. CLEFIA is a light weight algorithm concerned with block cipher developed by well-known Sony company. CLEFIA name is given to this algorithm with reference to the French word clef which means "key". The block size used is of 128 bits and the key size may be 128-bit, 192 bit or 256 bits. CLEFIA operates on 128-bit block size with three different key sizes: 128-bit, 192-bit, 256-bits.*
In this Paper the performance analysis of Lightweight Cryptographic Algorithms based on execution time and memory use by algorithm is discussed.

Keywords- Cryptography, CLEFIA, Execution time Light Weight, Memory.

I. INTRODUCTION

The CLEFIA nurture 128-bit block size with three different key sizes: 128-bit, 192-bit, 256-bits. CLEFIA consists of two mains segments: a data processing and a key scheduling segment. CLEFIA hires a generalized Feistel *(Gf)* structure which is a symmetric structure used in the construction of block ciphers, with four data lines, and the width of each data line is 32 bits. Also, there are key whitening parts at the beginning and the end of the cipher key. The term whitening is a technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key. The number of rounds used in the algorithm is related to the key lengths. As per CLEFIA concerned, the 128-bit plain text ,18 rounds were required, similarly for a 192-bit length of plain text the number of rounds is 22. And also, for the 256-bit length of the original message 26 rounds have to be performed.[24]
We executed the cryptographic algorithm CLEFIA in C language with the Microsoft Visual Studio.

II. LITERATURE REVIEW

CLEFIA PERFORMANCE

CLEFIA Execution Time- As the execution time or Speed of the operation is one of the important key parameters used to evaluate the performance of the block ciphers [26]. In paper titled " Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment"[26] the author executed the CLEFIA algorithm for 128 bit, 192 bit, and 256 bit Keys for plaintexts of size 512 Bytes, 1024 Bytes, 2048

https://doi.org/10.46335/IJIES.2023.8.3.4 e-ISSN: 2456-3463
Vol. 8 , No. 3, 2023, PP. 19- 23

International Journal of Innovations in Engineering and Science, www.ijies.net

Bytes, and 3072 Bytes in which they are calculated average values as shown in Figure 1.

From this implementation of execution time, the as the plaintext size increases encryption is increasing rapidly. This happens because of the block cipher consist of two feistal function and two diffusion matrixes. While the decryption follows a similar procedure with only changes made to the order of round keys and whitening keys selection.

From Figure 1, it can be said that for 512-byte plain text with key size 128 bit the execution time is 12.329 msec, similarly for 192 bit the execution time is 16.934 msec and for 256 bit the execution time is 18.562msec.

Table 1 Memory usage of CLEFIA for different key size

Block length	Key length	Number of rounds	FRAM	RAM
128	128	18	3.8KB	1.6KB
128	192	22	3.8KB	1.6KB
128	256	26	3.8KB	1.6KB

For 1024-byte plain text with key size 128bit the execution time is 24.782 msec, similarly for 192 bit the execution time is 33.521msec and for 256 bit the execution time is 36.89 msec

Figure 1 CLEFIA encryption execution time.[26]

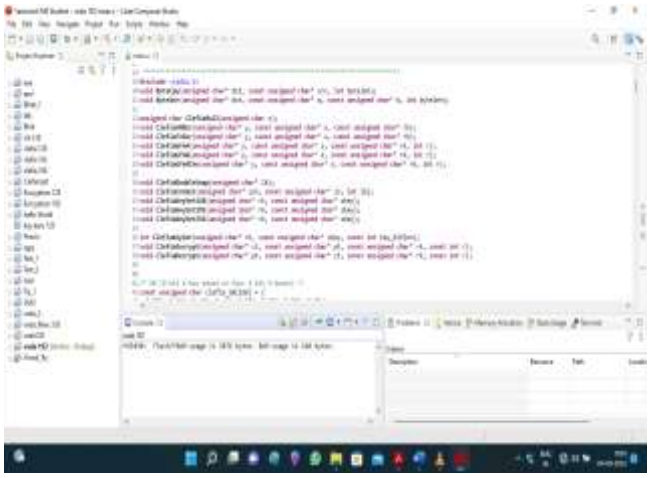
Also, for 2048-byte plain text with key size 128 bit the execution time is 49.105 msec, similarly for 192 bit the execution time is 67.76 msec and for 256 bit the execution time is 73.727msec.

Finally for 3072 byte plain text with key size 128bit the execution time is 73.86 msec , similarly for 192 bit the execution time is 100.89 msec and for 256 bit the execution time is 110.635msec.

III- RESULTS

A. Memory usage of CLEFIA

For various memory usage of CLEFIA the hardware kit is used is a development kit with the MSP430FR5994 ultra low power microcontroller. It is microcontroller with 16MHz clock frequency has 256 kB ultra-low power consumption FRAM (Ferroelectric Random-Access Memory) permanent memory. MSP430FR5994 family consist of eZ-FET next generation on board emulation facility with Energy Trace Technology. The execution performance of the encryption and decryption code can be tested and analyzed. Code Composer Studio (CCS) [25], which can be used in devices synthesized by company named Texas Instruments TI, has been used as an ecological development [26].The Operating system used is Windows 10, v.10.0, x86_64 / win32 Java version: 11.0.11 is use with configuration Intel(R) Core(TM) i3-8145U CPU running at frequency of 2.10GHz, with RAM4GB of 64 bit processor. On this platform the extracted parameters related to memory usage are as follows:



Photograph 1 showing Memory usage of CLEFIA

B. Calculation of Execution Time

Now in this section we are going to focus on execution time of CLEFIA with Microsoft Visual studio with following platform

System configuration

System model- Laptop
System type- x64 based PC
RAM - 4GB
OS- MS Window 10 pro
The Version used 10.0.18363 with build 18363

https://doi.org/10.46335/IJIES.2023.8.3.4 **e-ISSN: 2456-3463**
Vol. 8 , No. 3, 2023, PP. 19- 23

International Journal of Innovations in Engineering and Science, www.ijies.net

Processor- Intel (R) Core™ i3-8145 CPU with frequency 2.10 GHz

As Shown in Figure 1, the execution time for 512-byte plain text with key size 128 bit the execution time is 12.329 msec, similarly for 192 bit the execution time is 16.934 msec and for 256 bit the execution time is 18.562 msec. [26].

The CPU clock speed is 84 MHz and SRAM are of 96 KB [26].

Now process time is calculate as follows. The time taken by a process, so here we are using clock function time.h. Hence, we called the clock function at the starting and end of the code for which we have to measure time, subtract the values, and then divide by CLOCKS_PER_SEC (the number of clock ticks per second) to get approximate time taken by processor The code for the program is as follows.

```
#include <time.h>
clock_t begin = clock();
/* here, do your time-consuming job */
clock_t end = clock();
double time_spent = (double)(end - begin) / CLOCKS_PER_SEC;
printf ("%f\n", time_spent);
```

The Result obtained from execution on Laptop having configuration- x64 based PC having RAM - 4GB, OS- MS Window 10 pro, Processor- Intel (R) Core™ i3-8145 CPU at 2.10 GHz with Microsoft Visual Studio is as shown in following Figures 1,2,3 for different key size.

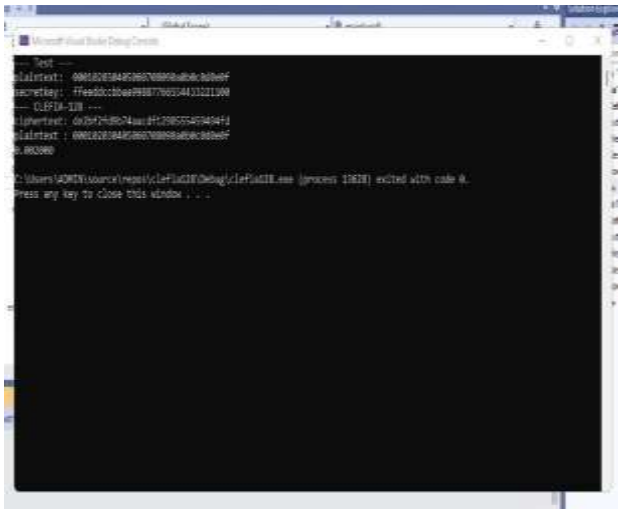


Figure 2 Exection Time for CLEFIA 128 bit key size with plain Text 512 byte

From the Figure 2 the calculated time for 128 bit key size is 2 microsec.

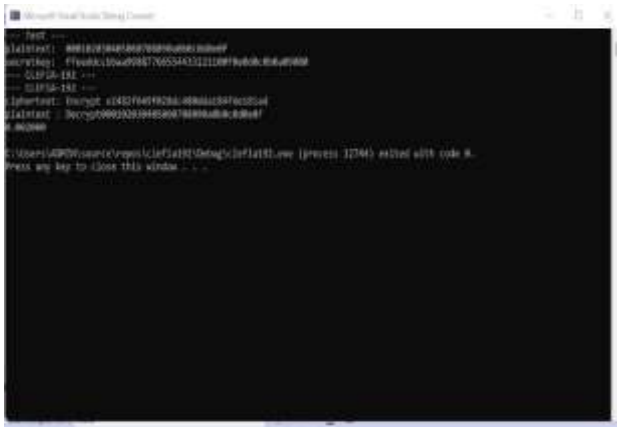


Figure 3 Exection Time for CLEFIA 192 bit key size with plain Text 512 byte

Similarly for 192 and 256 bit key size is 2 msec which is shown in Figure 3.

As mentioned in paper "Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment " [26], the time required for 128 bit key size having plain text size 512 byte is 12.329 mili second having CPU speed (Clock /cycle) 84 MHz, hence for laptop having CPU Speed of 2.10 GHz, The exection time is approximately is of 2 mili second.

From the Figure 4 it is seen that **t**otal Exection Time for CLEFIA (128, 192 256 bit key size) with plain Text 512 byte is 6 milisec.

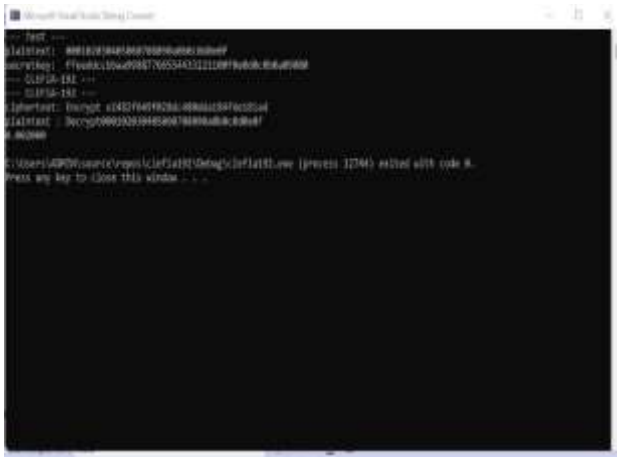


Figure 4: Total Exection Time for CLEFIA (128, 192 256 bit key size) with plain Text 512 byte

IV- CONCLUSION

After studying the Memory usage and execution time of CLEFIA algorithm, it is concluded that the as the plaintext size increases encryption is increasing rapidly. This happens because of the block cipher employs two feistal function and two diffusion

matrixes. In the decryption process same two feistal function and two diffusion matrixes are used in similar fashion with only changes made to the order of round keys and whitening keys selection.

REFERENCES

[1] *Avinash Kak "Some Basic Vocabulary of Computer and Network Security and a Brief Review of Classical Encryption Techniques Lecture Notes on Computer and Network Security, Purdue University 18 April, 2018.*

[2] *Sattar B.Sadkhan, Akbal O. Salman "A Survey on Lightweight-Cryptography Status and Future Challenges", International Conference on Advances in Sustainable Engineering and Applications (ICASEA), Wasit University, Kut, Iraq. IEEE Conference proceeding, ISSN 978-1-5386-3540-7/18/31.00$©2018 IEEE, 2018. pp.105-108. June 2018.*

[3] *Thomas Eisenbarth Sandeep Kumar Christof Paar and Axel Poschmann "A Survey of Lightweight-Cryptography Implementations" IEEE proceeding on IEEE Design & Test of Computers, Co published by the IEEE CS and the IEEE CASS, ISSN 0740-7475/07/$25.00 G 2007 IEEE, pp 1-12,4 October 2017.*

[4] *Yulong Zou, Jia Zhu, XianbinWang and Lajos Hanzo, "A Survey on Wireless Security Technical Challenges, Recent Advances, and Future Trends" Proceedings of the IEEE Volume 104, No. 9, Digital Object Identifier: 10.1109/JPROC.2016.2558521, pp 1727-1765 September 2016.*

[5] *Gaurav Bansod, Nishchal Raval and Narayan Pisharoty "Implementation of a New Lightweight Encryption Design for Embedded Security" IEEE Transactions on Information Forensics And Security, Vol. 10, No. 1, ISSN 1556-6013 © 2014 IEEE, DOI10.1109/TIFS.2014.2365734 pp,142-151 January 2015.*

[6] *Pradeep Semwal, Mahesh Kumar Sharma "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing" ISSN 978-15090-6403-8/17/$31.00 © 2017 IEEE pp.1-7, 2017.*

[7] *Sarika Y. Bonde ,Dr. U. S. Bhadade, "Analysis of Encryption Algorithms (RSA, SRNN and 2 key pair) for Information Security" ISSN 978-1-5386-4008-1/17/$31.00 ©2017 IEEE. pp. 1-7 2017.*

[8] *Ahmer Khan Jadoon , Licheng Wang , Tong Li , and Muhammad Azam Zia ,"Review Article Lightweight Cryptographic Techniques for Automotive Cybersecurity ", Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 1640167, pp 1-15, 26 June 2018.*

[9] *Shehnaz T. Patel,Nita H. Mistry,"A Survey: Lightweight Cryptography in WSN" IEEE International Conference on Communication Networks (ICCN) 2015, IEEE Proceeding ISSN 978-I-S090-00S 1-7I 1S/$3 1.00©2015 IEEE, DOl 1O.l 109/ICCN.20IS.3. pp 11-15,2015.*

[10] *Oscar Delgado-Mohatar , Amparo Fúster-Sabater, Jose M. Sierra ,"A light-weight authentication scheme for wireless sensor networks" , Journal of Elsevier B.V, ISSN 1570-8705/$. doi:10.1016/j.adhoc.2010.08.020, pp 727-735, 8 September2010.*

[11] *Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi Taeshik Shon , Hafiz Farooq Ahmad "A lightweight message authentication scheme for Smart Grid communications in power sector" , Journal of Elsevier B.V Computers and Electrical Engineering ,0045-7906/©2016 Elsevier Ltd .pp 1-11,07 March 2016.*

[12] *Rajani Devi.T, "Importance of Cryptography in Network Security", IEEE Proceeding ISSN 978-0-7695-4958-3/13 $26.00 © 2013 IEEE, IEEE Computer Society, DOI 10.1109/CSNT.2013.102,pp 462-467, 2013.*

[13] *Masanobu Katagi and Shiho Moriai, "Lightweight Cryptography for the Internet of Things", White paper by Sony Corporation, pp 1-4.*

[14] *Lara-Ni, Carlos Andres, Morales-Sandoval, Miguel and Dıaz-Perez "An evaluation of AES and PRESENT ciphers for lightweight cryptography on smart phones", IEEE Proceeding ISSN 978-1-5090-0079-1/16/$31.00 ©2016 IEEE, pp 87-93, 2016.*

[15] *Charalampos Manifavas , George Hatzivasilis , Konstantinos Fysarakis , and Konstantinos Rantos "Lightweight Cryptography for Embedded Systems - A Comparative Analysis" White paper by Dept. of Applied Informatics & Multimedia, Technological Educational Institute of Crete, Heraklion, Crete, Greece, pp 1-10.*

[16] *Axel York Poschmann Bochum, "LIGHTWEIGHT CRYPTOGRAPHY -Cryptographic Engineering for a Pervasive World " Thesis ,Faculty of Electrical Engineering and Information Technology RuhrUniversity Bochum, Germany. pp 1-5, February 2009.*

[17] *Kerry A. McKay ,LarryBassham, Meltem Sonmez Turan , Nicky Mouha "Report on Lightweight Cryptography" NISTIR 8114,National Institute of Standards and Technology U.S. Department of Commerce, Internal Report 8114 pp-1-14 March 2017.*

[18] *Tetsu Iwata "The 128-bit Block cipher CLEFIA Design Rationale" Report on development of CLEFIA by Sony Corporation, Konan, Minato-ku, Tokyo 108-0075 Japan June 1, 2007.*

[19] *Madhumita Panda "Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016 IEEE Proceeding ISSN 978-1-5090-4620-1/16/$31.00 ©2016 IEEE, pp 278-284, 2016.*

[20] *Chaitra B, Kiran Kumar V. G, Shatharama Rai "A Survey on Various Lightweight Cryptographic Algorithms on FPGA" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 1, Ver. II (Jan.-Feb. 2017), PP 54-59*

[21] *Jaber Hossein Zadeh,Abbas Ghaemi Bafghi "Evaluation of Lightweight Block Ciphers in Hardware Implementation: A Comprehensive Survey"2016 1st International Conference on New Research Achievements in Electrical and Computer Engineering.*

[22] *Levent Ertaul, Sachin Kattepura Rajegowda "Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment" International Conference on Security and Management SAM'17, ISBN: 1-60132-467-7, CSREA Press ©, Pp 25-31.*

[23] *Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata "The 128-bit Block cipher CLEFIA"(Extended Abstract), Sony Corporation, Konan, Minato-ku, Tokyo 108-0075 Japan June 1, 2007.*

[24] *Tetsu Iwata of Nagoya University, The 128-bit Block cipher CLEFIA Algorithm Speciation, Revision 1.0June 1, 2007.*

[25] *Bora Aslan Fusun Yavuzer Aslan and M. Tolga Sakallı "Energy Consumption Analysis of Lightweight Crypto graphic Algorithms That Can Be Used in the Security of Internet of Things Applications" Research Article Hindawi Security and Communication Networks, Volume 2020, Article ID 8837671, 15 pages*

[26] *Levent Ertaul, Sachin Kattepura Rajegowda California State University East Bay, Hayward, CA, USA." Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment". International Conference on Security and Management. ISBN: 1-60132-467-7. CSREA PRESS. Pp 25-31*

[27] *Vishal A. Thakor, Mohammad Abdur Razzaque (Member, IEEE), Muhammad R. A. Khandaker (Senior Member, IEEE) "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities"*

[28] *IEEE Access, date of publication January 19, 2021, date of current version February 22, 2021.Volume 9 2021, pp 28177-28193.*