

The New Cryptography Algorithm with High Throughput

Dudhatra Nilesh

Department of Computer Science & Engineering
Patel Institute of Engineering & Science,
Rajiv Gandhi Proudhyogiki Vishwavidyalaya,
Bhopal, University of
Technology of Madhya Pradesh, India
nilesh.rkcet@gmail.com

Prof. Malti Nagle

Department of Computer Science & Engineering
Patel Institute of Engineering & Science,
Rajiv Gandhi Proudhyogiki Vishwavidyalaya,
Bhopal, University of
Technology of Madhya Pradesh, India

Abstract— The Cryptography is very good area for research now a days. As we know that security is very primary requirement for the any business. And for that we need very strong and unbreakable algorithm which provides high security. For that we need encryption and decryption algorithm which is having very high security with very good throughput. If we look at the real world, there are lots of organizations that are having very large database with high security. As per security concern, some encryption and decryption algorithms are working behind confidential information like DES, 3DES, AES and Blowfish. In this paper at first new cryptography (Encryption and Decryption) algorithm has been generated and new cryptography (Encryption and Decryption) algorithm has been compared by using some components like throughput of key generation, to generate Encryption text and to generate Decryption text. If any brute force attacks are applied on this algorithm, how much security is provided by this algorithm is included. In this algorithm some arithmetic and logical mathematical operations are performed.

Keywords- Cryptography, Encryption, Decryption, Security, DES, Blowfish, 3DES, AES

I. INTRODUCTION

Internet is now a day's used for communication (instant messaging, mailing, social networking), shopping, blogging, web feeds, internet banking and many more [4]. As we know the use of internet is increasing rustically so, amount of addresses also increased that's why we need IPv6. In 2005 world population was 6.5 billion in which only 16% users use internet similar way in 2010 this population was 6.9 billion but 30% users use internet, in 2013 population is 7.1 billion and more than 39% users use internet[5]. If we look at the security of information which are transferred from source to destination during surfing, that is also increased. But with the increase of security, the hacking, cracking are also increased. If we want to secure our information, cryptography comes into the picture.

The protection ability and security of information is vital to the growth of e-commerce and to the growth of the internet itself. Some users use communication but they do not need security. There is lots of information that do not need any kind

of security. In spite there are some areas that are having very small amount of information but they need very high security.

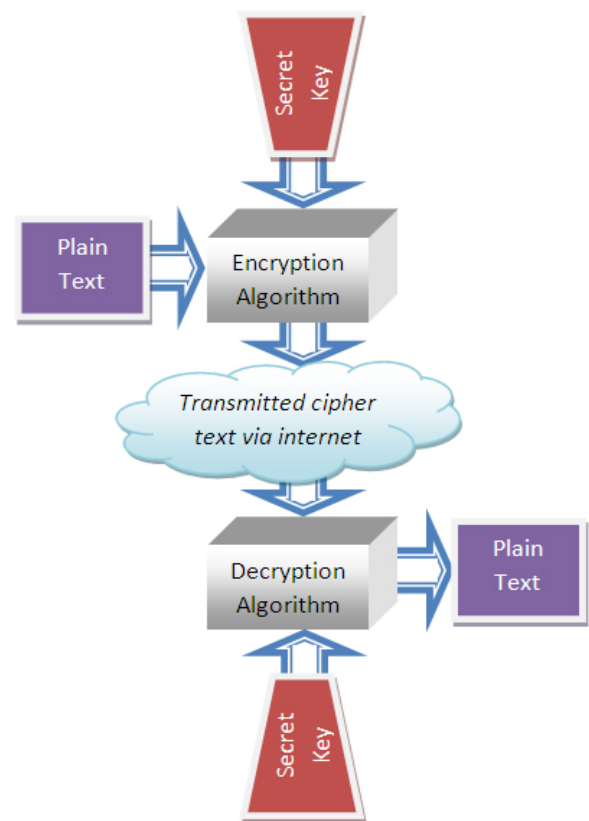


Figure 1. Encryption and Decryption Process

Cryptography is logic of mathematical manipulation of data (cipher text) with some text (Key) [3]. To convert plain text to cipher text encryption algorithm is applied on plain text using key. And to convert cipher text to plain text decryption algorithm is applied on cipher text using key. Before encryption and decryption algorithm some algorithm is required to generate key at first. During cryptography, there are three basic process-Key Generation, Encryption and Decryption process.

Cryptography – Encryption and Decryption process is shown in Figure 1 as discussed earlier.

II. STUDY OF OTHER ENCRYPTION ALGORITHM

There are lots of encryption algorithms available in cryptography area. In which AES, DES, 3DES and Blowfish algorithms are very much popular. So, in my work, my algorithm is compared with all these algorithms. In these all algorithms different types of operations are performed like bitwise XOR, Substitution, Shifting and many more. Let's see the methods of other encryption algorithm.

AES (Advanced Encryption Standard): also called variant of Rijndael Algorithm, has 128 bits block size with 128(with 10 cycles of repeating), 192(with 12 cycles of repeating) or 256(with 14 cycles of repeating) bits of key size. Brute force attack can unlock the AES algorithm [1]. In this attack algorithm attacker use dictionary of words in English and find out the words which is used as key. [6, 11]

DES (Data Encryption Standard): has 64 bits of block of plain text with 56 bits of key. The main problem is the small size of key. By using attack algorithm on DES, attacker can get plain text [3, 7 and 10].

3DES (Triple Data Encryption Standard): is upgraded version of DES. The steps of 3DES algorithm are similar as in simple DES but encryption level is increased by 3 times. After increasing 3 times encryption level, 3DES is very much slower than other encryption method [8].

Blowfish: the plus point of this algorithm is that it has variable length key (32 bits to 448 bits) with 64 bits of block size. This algorithm is one of the most common algorithms in cryptography area, freely available for all the users and also unpatented. [9]

There are so many issues found during study of all algorithms. Like...

- 1) The more complex structure of algorithm increases the time of execution. So the structure of algorithm should be simple to make algorithm faster.
- 2) The longer the length of key provides higher security as compare to shorter length of key and also increase the speed of execution of algorithm.
- 3) The overall performance of any algorithm depends upon selection of mathematical and/or logical operations applied on plain text, key and cipher text.

In my algorithm, all this issues are considered to improve the performance of encryption algorithm.

III. MY ALGORITHM

In this algorithm, the block size is 128 bits with 128 bits key size. Simple arithmetical and logical operations are used like logical XOR and Shifting. In this algorithm starting and ending 3-4 steps are executed only one time but among these few steps repeat n times. These steps are not fixed that how many times they are executed? So, if attackers know about the algorithm, they cannot assume that how many times steps are

executed. So, security compare to other encryption algorithm is increased. The steps of encryption and decryption algorithms are as following.

1) Steps of Encryption:

- a) Convert 16 characters plain text in binary format (128 bits). Per character 8 bits.
- b) Divide 128 bits plain text into two 64 bits separately.
- c) Arrange both 64 bits in reverse order.
- d) Merge both part and apply XOR operation with 128 bits of key (first convert key in binary form of 128 bits). And perform circular left shift operation on key for second round.
- e) Divide 128 bits of result into 16 parts each of 8bits.
- f) Divide each of the 8bits into two parts each of 4 bits.
- g) Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
- h) Now apply XOR operation on left and right 64 bits and store the result in left 64 bits. And keep the right 64 bits as it is (no change in right 64 bits).
- i) Combine both 64 bits into 128 bits format (Repeat N time from step no 4).
- j) Now divide 128 bits into 16 parts each of 8bits.
- k) Divide each of the 8bits into two parts of 2 bits and 6 bits respectively.
- l) Perform circular left shift operation on all 6 bits.
- m) Combine all parts - and get 128 bit (16 characters) of cipher text.

As see the fig 2 Encryption Algorithm

2) Steps of Decryption:

- a) Convert 16 characters cipher text in binary format (128 bits).
- b) Divide 128 bits into 16 parts each of 8bits.
- c) Divide each of the 8 bits in two parts of 2 bits and 6 bits respectively.
- d) Perform circular right shift operation on all 6 bits.
- e) Combine all parts and get 128 bits.
- f) Now apply XOR operation on left and right 64 bits and store result in left 64 bits. And keep the right 64 bits as it is (no change in right 64 bits).
- g) Now divide 128 bits into 16 parts each of 8 bits.
- h) Divide each of 8 bits into two parts each of 4 bits.
- i) Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
- j) Combine both 64bits into 128 bits format
- k) Merge both part and apply XOR operation with 128 bits of key (key convert at first in binary form). And perform circular rightshift operation on key for second round

(Repeat N time from step no. 6)

- l) Divided 128 bits plain text into two parts each of 64 bits.
- m) Arrange reverse order of both 64 bits and combine both 64 bit parts, plain text in form of 16 characters and 128 bits is generated.

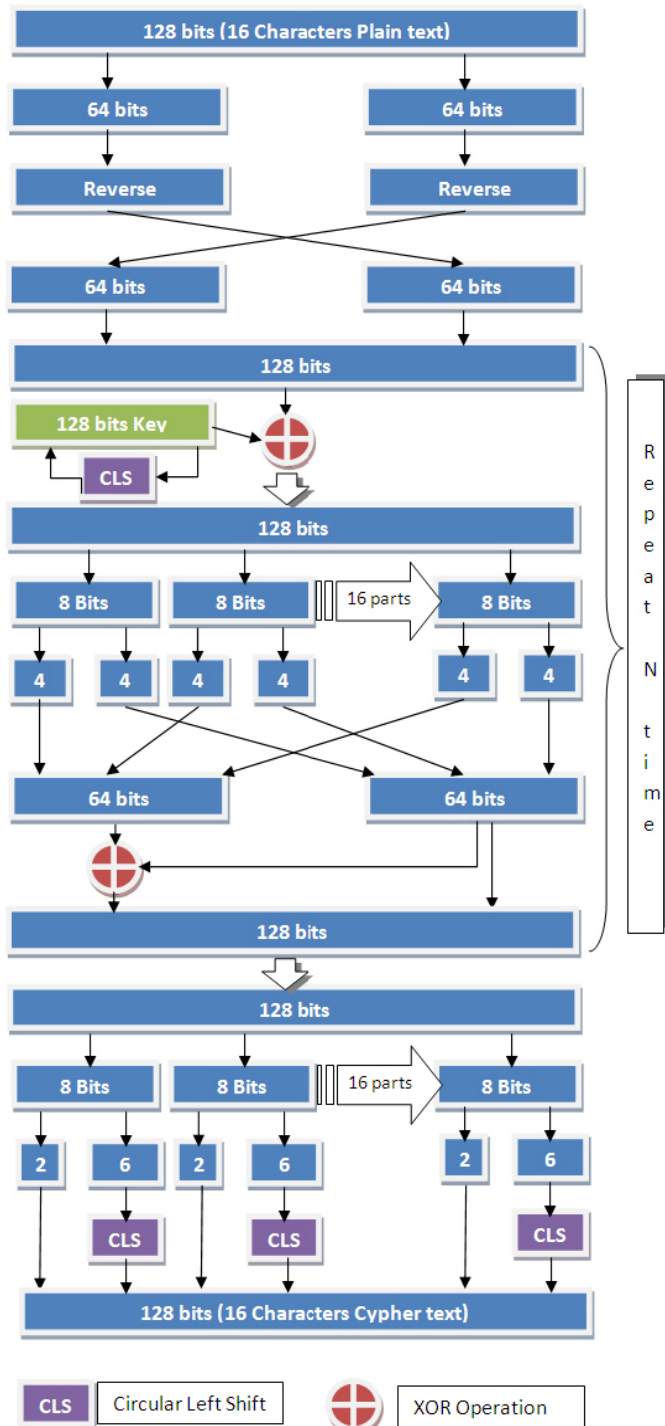


Figure 2. Encryption Algorithm

IV. RESULT OF THE ALGORITHM

For the implementation of above algorithm in Microsoft Visual Studio 2008, C#.NET got following screen as fig 3 Snap Shot of implantation Algorithm

The Output of the Implementation algorithm is as following

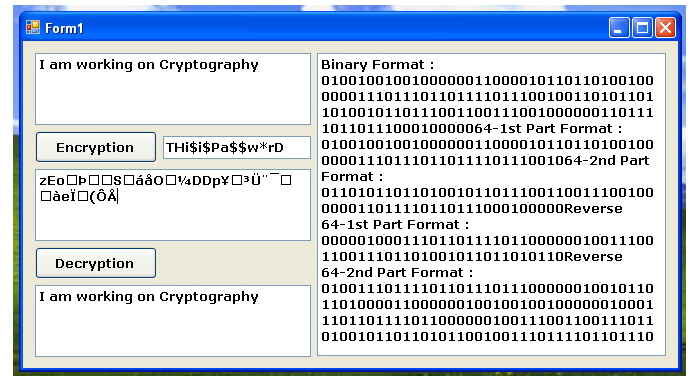


Figure 3. A Snap Shot of Implantation Algorithm

Encryption Process

Plain Text is "I am working on Cryptography"

Key Text is "THi\$Pa\$w*rD

Binary format of Plain text :

```

01001001001000000110000101101101001000000111011101
10111101110010011010110110100101101110011001110010
0000011011110110111000100000

```

Binary format of Cipher text:

```
01110000101001011000001010100111101110010101000
1010111110011000000110001110000001100101110011110
000101001010001101010011000101
```

(This is cipher text: zEo™PœSáåO...¼DDp¥,³Ü~æě...(ÔÅ)

Decryption Process

Cipher Text is "zEo™PœSáåO...¼DDp¥,³Ü~æē...(ÔÅ"

Key Text is "THi\$!\$Pa\$\$w*rD

Binary format of Cipher text:

```
01110000101001011000001010110011110111001010100010
10111110011000000110001110000001100101110011111000
0101001010001101010011000101
```

Binary format of Plain text :

```
01001001001000000110000101101101001000000111011101
10111101110010011010110110100101101110011001110010
0000011011110110111000100000
```

(This is plain text: I am working on Cryptography)

V. THROUGHPUT OF THE ALGORITHM

During execution of all the cryptography algorithms, throughput is divided in three main processes.

1. Key generation Process
2. Encryption Process
3. Decryption Process

This experiment is performed on system having P4 (Core 2 Duo) processor with 1GB of RAM. Table 1 is throughput of 100KB, 1MB and 10MB. Fig 4 is chart of throughput with 100KB. Fig 5 is chart of throughput with 1MB. Fig 6 is chart of throughput with 10MB.

TABLE I. THROUGHPUT OF ALGORITHM

Process of Algorithm	Compared with Other Algorithms				
	<i>AES</i>	<i>DES</i>	<i>Triple DES</i>	<i>Blowfish</i>	<i>My Algo.</i>
Throughput 100KB					
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.34	0.35	0.36	0.32	0.33
Decryption	0.34	0.35	0.36	0.32	0.33
Throughput 1MB					
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.41	0.45	0.65	0.39	0.4
Decryption	0.42	0.45	0.65	0.39	0.4
Throughput 10MB					
Key Generation	0.25	0.25	0.25	0.25	0.2
Encryption	1.2	1.5	3.25	1.1	1.1
Decryption	1.2	1.5	3.25	1.1	1.1

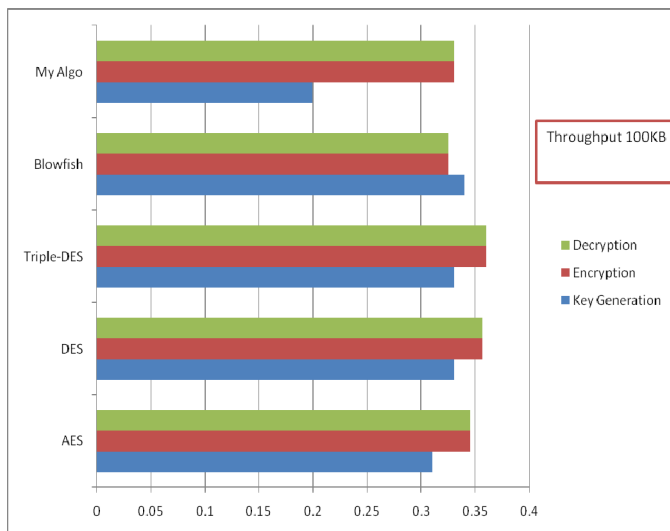


Figure 4. Algorithm throughput of 100KB

Now from Table 1 and Fig 4, 5 and 6 – observed that new algorithm give fast output as compare to other algorithms.

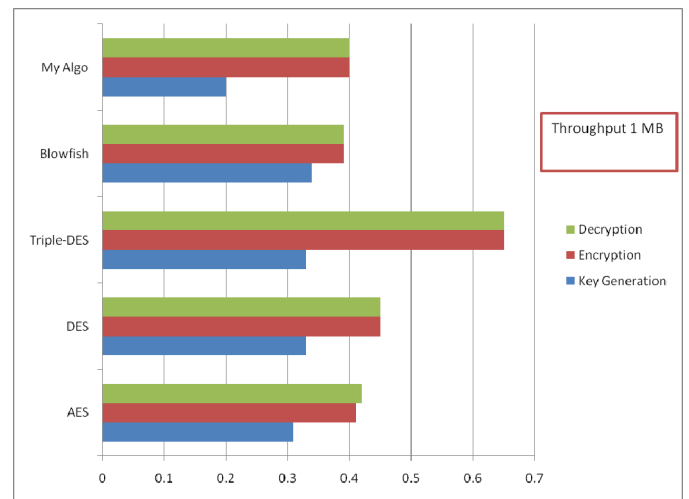


Figure 5. Algorithm throughput of 1MB

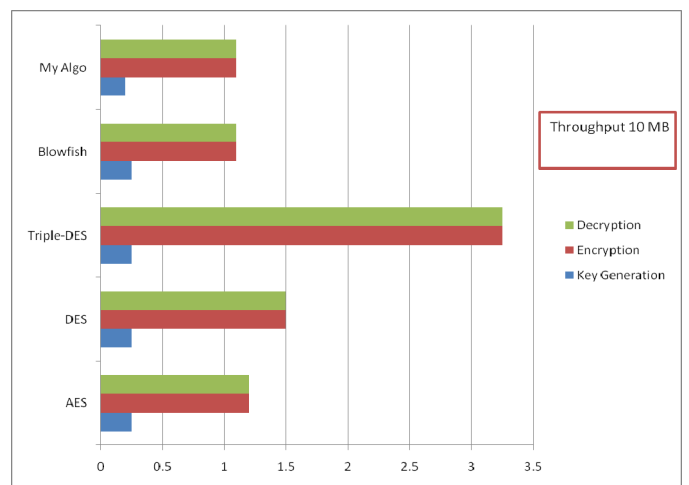


Figure 6. Algorithm throughput of 10MB

VI. SECURITY OF ALGORITHM IN FRONT OF BRUTE FORCE ATTACKS

Encryption algorithm is used to provide security; during attack the attacker cannot get the plain/original text from cipher text that is main aim. So, let's check it for Brute Force Attack algorithm how this algorithm can secure the information.

In algorithm, the key length is 16 characters. So attackers have total 64 possible characters. So, 1/64 octet is there. If attackers have super computer, they can attempt 10^{12} attacks per second. Total possible keys are 7.9×10^{28} (64^{16}). So, total 2.5×10^9 years need and it's not possible for universe.

Following fig 7: Mathematically Calculation for the Brute Force Attack

$$\text{Brute Force Attacks need times} = \frac{7.9 \times 10^{28}}{10^{12}} \text{Seconds}$$

$$\text{Brute Force Attacks need times} = \frac{7.9 \times 10^{28}}{10^{12} \times 60 \times 60 \times 24 \times 365} \text{Years}$$

$$\text{Brute Force Attacks need times} = 2.5 \times 10^9 \text{Years}$$

Figure 7. Time Needed for Brute Force Attacks

VII. CONCLUSIONS

The results showed that my algorithm has better performance than other commonly used encryption algorithm. As per my observation there is no weak point so far. This algorithm provides very high throughput and provides very high security. Due to simple calculation of arithmetic and logic operations execution speed is very fast and due to 128 bits key size security is very high. Main property of encryption algorithm is security and high throughput, and this algorithm has both properties.

For the future work I want to improve this algorithm by increasing more number of arithmetic and logical operation with more and more throughput.

REFERENCES

- [1] Christian Mainka, Juraj Somorovsky, Jorg Schwenk "Penetration Testing Tool for Web Services Security", Honolulu HI, Page 163-170, published in Services (SERVICES) Eighth World Congress on IEEE, 24-June-2012 ISBN: 978-1-4673-3053-4
- [2] Quinn Martin, Alan D. George "Scrubbing Optimization via Availability Prediction (SOAP) for Reconfigurable Space Computing" UKACC International Conference on Control 2012, Cardiff, UK, 3-5 September 2012
- [3] Shah Kruti R, Bhavika Gambhava "New Approach of Data Encryption Standard Algorithm" International Journal of Soft Computing and Engineering(IJSCE) ISSN:2231-2307, Vol-2, Issue-1, March 2012
- [4] Nadeem, A. ; Javed, M.Y. "A Performance Comparison of Data Encryption Algorithms" Information and Communication Technologies, 2005. ICICT 2005. First International Conference Publication Year: 2005 , Page(s): 84 - 89
- [5] "Welcome to ITU TELECOM WORLD 2011 | ITU TELECOM WORLD 2011". Itu.int. 27 October 2011. Retrieved 9 July 2012.
- [6] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.
- [7] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology 4 (1): 3–72. doi:10.1007/BF00630563.
- [8] "The Cryptography Guide: Triple DES". Cryptography World. Retrieved 2010-07-11.
- [9] Vincent Rijmen (1997). "Cryptanalysis and Design of Iterated Block Ciphers" (PostScript). Ph.D thesis.
- [10] Lin Zi ; Shi Wenxiao ; Wang Li "A study and analysis on a high intensity public data encryption algorithm" Intelligent Control and Automation, 2000. Proceedings of the 3rd World Congress on Pub Year: 2000 , Page(s): 2492 - 2494 vol.4
- [11] Perez, O. ; Berviller, Y. ; Tanougast, C. ; Weber, S. "Comparison of various strategies of implementation of the algorithm of encryption AES on FPGA" Industrial Electronics, 2006 IEEE International Symposium on Volume: 4 Publication Year: 2006 , Page(s): 3276 - 3280 IEEE Conference Publications
- [12] Hamalainen, P. ; Hannikainen, M. ; Hamalainen, T. ; Saarinen, J. "Configurable hardware implementation of triple-DES encryption algorithm for wireless local area network" Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on Publication Year: 2001 , Page(s): 1221 - 1224 vol.2