

The New Cryptography Algorithm with High Throughput

Aashish Kumar Singh

B.TECH(Student), Department of Information Technology
Arya College of Engineering and I.T
42,Old Campus, RIICO Industrial Area, Kukas, Delhi Road,
Jaipur, Rajasthan, India
ashumay0@gmail.com

Er. Chhavi Gupta

Associate Professor, Department of Information Technology
Arya College of Engineering and I.T
42,Old Campus, RIICO Industrial Area, Kukas, Delhi Road,
Jaipur, Rajasthan, India
chhavigupta2009@gmail.com

Abstract – Cryptography is generally an excellent region to look into nowadays. As we realize that security is an essential prerequisite for any business. Also, for that, we need an exceptionally solid and unbreakable calculation that gives high security. For that, we need encryption and unscrambling calculation which is having exceptionally high security with generally excellent throughput. On the off chance that we take a gander at this present reality, there are loads of associations that are having an enormous database with high security. According to security concerns, some encryption and decoding calculations are working behind classified data like DES, 3DES, AES, and Blowfish. In this paper from the start new cryptography (Encryption and Decryption) calculation has been created and new cryptography (Encryption and Decryption) calculation has been thought about by utilizing a few parts like throughput of key age, to produce Encryption content and to produce Decryption content. In the event that any beast power assaults are applied to this calculation, how much security is given by this calculation is incorporated. In this calculation, some number-crunching and intelligent numerical activities are performed.

Keywords – Cryptography, Encryption, Decryption, Security, DES, Blowfish, 3DES, AES.

I. INTRODUCTION

The web is currently a day utilized for correspondence (texting, emailing, long-range interpersonal communication), shopping, blogging, the web takes care of, web banking, and a lot more. As we probably are aware the utilization of the web is expanding naturally in this way, the measure of addresses likewise expanded that is the reason we need IPv6. In 2005 total populace was 6.5 billion in which just 16% of clients use web comparative route in 2010 this populace was 6.9 billion yet 30% of clients use the web, in 2013 populace is 7.1 billion, and over 39% of clients use the internet. In the event that we take a gander at the security of data that are moved from source to goal during surfing, that is likewise expanded. Be that as it may, with the expansion of security, the hacking, splitting are additionally expanded. In the event that we need to make sure about our data, cryptography comes into the image.

The assurance capacity and security of data are imperative to the development of online business and to the development of the web itself. A few clients use correspondence however they needn't bother with security. There are bunches of data that needn't bother with any sort of security. In demonstrate hatred for, there are a few zones that are having a limited quantity of data yet they need exceptionally high security.

Cryptography is the rationale of scientific control of information (ciphertext) with some content (Key). To change over a plain book to a ciphertext encryption calculation is applied on plain content utilizing a key. Also, to change over the ciphertext to plain content decoding calculation is applied to ciphertext utilizing the key. Before encryption and decoding calculation some calculation is required to create a key from the outset. During cryptography, there are three essential procedures Key Generation, Encryption, and Decryption process.

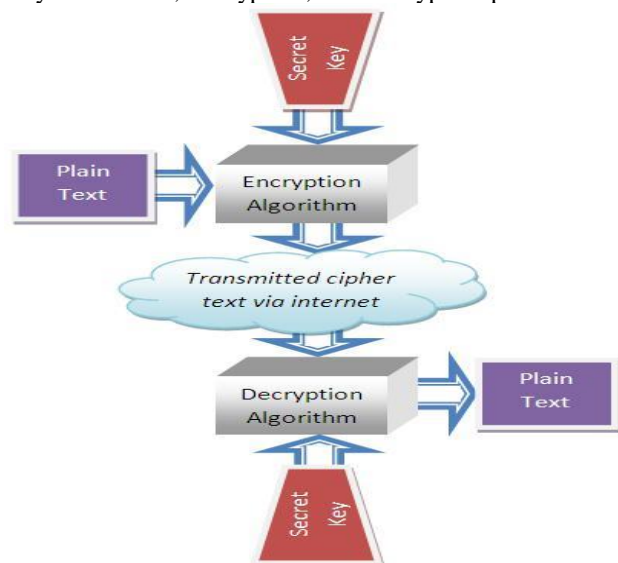


Fig. 1. Encryption and Decryption Process.

II. STUDY OF OTHER ENCRYPTION ALGORITHM

There are bunches of encryption calculations accessible in the cryptography zone. In which AES, DES, 3DES, and Blowfish calculations are a lot of mainstream. In this way, in my work, my calculation is contrasted and every one of these calculations. In these, all calculations various sorts of activities are performed like bitwise XOR, Substitution, Shifting, and some more. We should see the techniques for other encryption calculations.

AES (Advanced Encryption Standard): additionally called a variation of Rijndael Algorithm, has 128 bits square size with 128(with 10 patterns of rehashing), 192(with 12 patterns of rehashing) or 256(with 14 patterns of rehashing) bits of key size. Animal power assault can open the AES calculation. In this assault, the calculation aggressor uses word reference of words in English and discover the words which are utilized as key.

DES (Data Encryption Standard): has 64 bits of the square of plain content with 56 bits of the key. The fundamental issue is the little size of the key. By utilizing assault calculation on DES, the assailant can get plain content.

3DES (Triple Data Encryption Standard): is an updated form of DES. The means of 3DES calculation are comparative as in basic DES yet encryption level is expanded by multiple times. Subsequent to expanding multiple times encryption level, 3DES is especially more slow than other encryption techniques.

Blowfish: the in addition to the purpose of this calculation is that it has a variable-length key (32 bits to 448 bits) with 64 bits of square size. This calculation is one of the most widely recognized calculations in the cryptography region, unreservedly accessible for all the clients and furthermore unpatented.

There are such a large number of issues discovered during investigation everything being equal. Like...

- 1) The more intricate structure of calculation builds the hour of execution. So the structure of calculation ought to be easy to make calculation quicker.
- 2) The more drawn out the length of the key gives higher security as a contrast with shorter length of the key and furthermore speed up execution of calculation.
- 3) The general execution of any calculation relies on the determination of scientific as well as sensible activities applied on plain content, key, and figure content.

In my calculation, these issues are considered to improve the exhibition of encryption calculation.

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:

- 1.3 Convert 16 characters plain text in binary format (128 bits). Per character 8 bits.
- 1.4 Divide 128 bits plain text into two 64 bits separately.
- 1.5 Arrange both 64 bits in reverse order.
- 1.6 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.
- 1.7 Divide 128 bits of result into 16 parts each of 8bits.
- 1.8 Divide each of the 8bits into two parts each of 4 bits.
- 1.9 Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
- 1.10 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).
- 1.11 Combine both 64 bits into 128 bits format (Repeat N time from step no 4).
- 1.12 Now divide 128 bits into 16 parts each of 8bits.
- 1.13 Divide each of the 8bits into two parts of 2 bits and 6 bits respectively.
- 1.14 Perform circular left shift operation on all 6 bits.
- 1.15 Combine all parts - and get 128 bit (16 characters) of cipher text.

As see the fig 2 Encryption Algorithm

2. Steps of Decryption:

- 2.3 Convert 16 characters cipher text in binary format (128 bits).
- 2.4 Divide 128 bits into 16 parts each of 8bits.
- 2.5 Divide each of the 8 bits in two parts of 2 bits and 6 bits respectively.
- 2.6 Perform circular right shift operation on all 6 bits.
- 2.7 Combine all parts and get 128 bits.
- 2.8 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).
- 2.9 Now divide 128 bits into 16 parts each of 8 bits.
- 2.10 Divide each of 8 bits into two parts each of 4 bits.
- 2.11 Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
- 2.12 Combine both 64bits into 128 bits format
- 2.13 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
- 2.14 (Repeat N time from step no. 6)

- Divided 128 bits plain text into two parts each of 64 bits.

[1] 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.

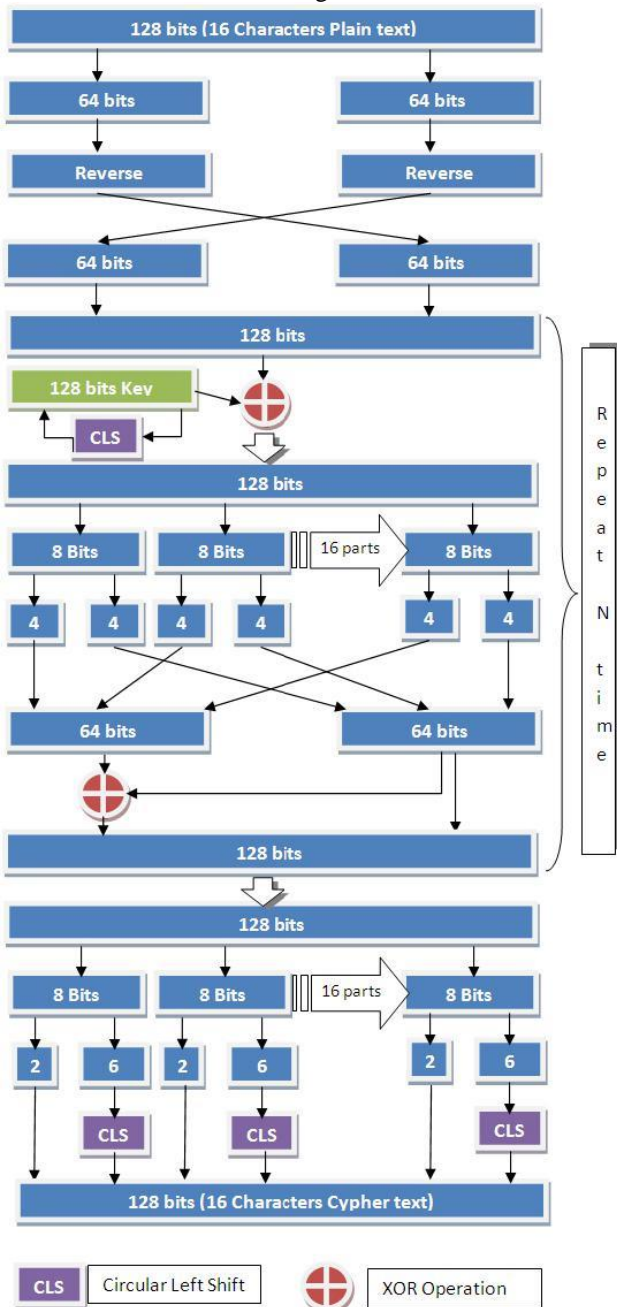


Fig.2. Encryption Algorithm.

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

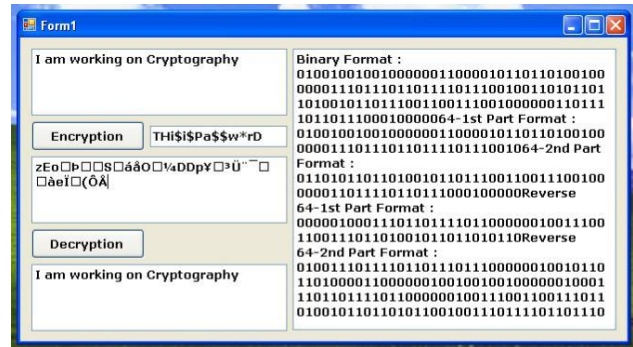


Fig.3. A Snap Shot of Implantation Algorithm.

Encryption Process

Plain Text is "I am working on Cryptography"

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

Binary format of Plain text :

```
0100100100100000011000010110110100100000011101
1101
1011110111001001101011011010010110111001100111
0010
```

```
0000011011110110111000100000
```

Binary format of Cipher text:

```
011100001010010110000101011001111011100101010
00
```

```
101011110011000000110001110000001100101110011
1110
000101001010001101010011000101
```

(This is cipher text:
zEo™PœSááO...¼DDp¥,³Û~ˆæĬ...(ÔÅ) Decryption
Process

Cipher Text is
"zEo™PœSááO...¼DDp¥,³Û~ˆæĬ...(ÔÅ"

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

Binary format of Cipher text:

```
011100001010010110000101011001111011100101010
0010
101111001100000011000111000000110010111001111
1000
```

```
0101001010001101010011000101
```

Binary format of Plain text :

```
0100100100100000011000010110110100100000011101
1101
```

1011110111001001101011011010010110111001100111
0010
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.

- Key generation Process
- Encryption Process
- 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				
	AES	DES	Triple DES	Blowfish	My Algo
<i>Throughput 100KB</i>					
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.34	0.33	0.36	0.32	0.33
Decryption	0.34	0.33	0.36	0.32	0.33
<i>Throughput 1MB</i>					
Key Generation	0.31	0.33	0.33	0.34	0.2
Encryption	0.41	0.43	0.65	0.39	0.4
Decryption	0.42	0.43	0.65	0.39	0.4
<i>Throughput 10MB</i>					
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

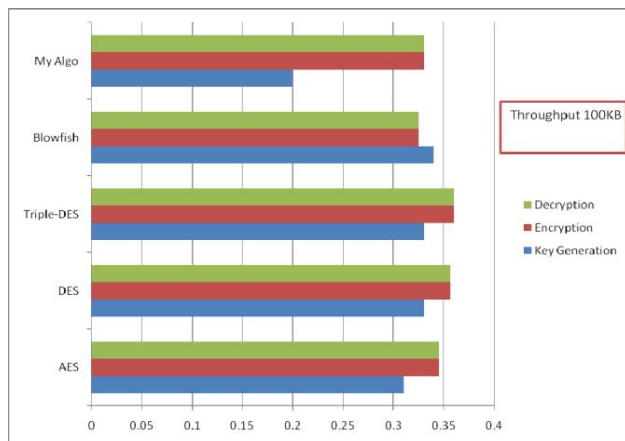


Fig.4. Algorithm throughput of 100KB.

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

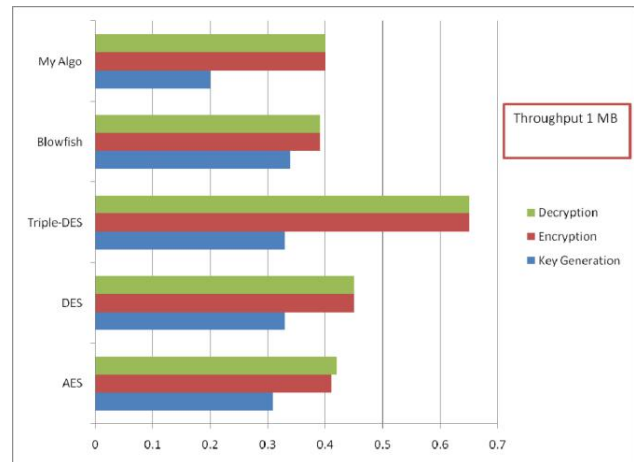


Fig. 5. Algorithm throughput of 1MB.

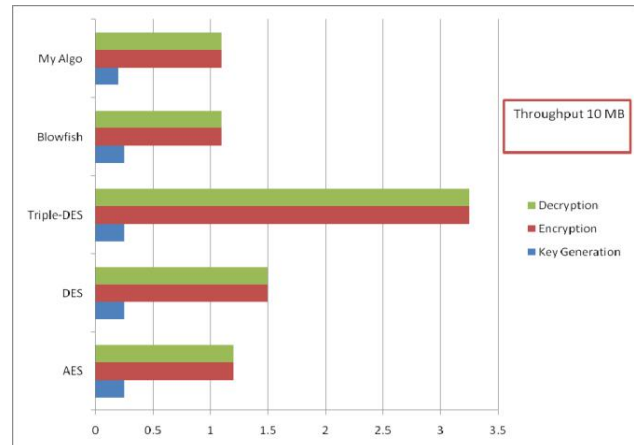


Fig. 6. Algorithm throughput of 10MB

VI. SECURITY OF ALGORITHM IN FRONT OF BRUTE FORCE ATTACKS

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

IN The Algorithm, The Key Length IS 16 Characters. SO Attackers Have Total of 64 Possible Characters. SO, 1/64 Octet is There. IF Attackers Have A SuperComputer, They Can Attempt 1012 Attacks PER Second. The Total Possible Keys are 7.9×10^{28} (64 16). SO, TOTAL OF 2.5×10^9 Years Need and IT'S Not Possible for The Universe.

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

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

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

Fig7. Time Needed for Brute Force Attacks.

Above Fig 7: Mathematically Calculation for the Brute Force Attack

VII. CONCLUSION

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
- [6]. "Welcome to ITU TELECOM WORLD 2011 | ITU TELECOM WORLD 2011". Itu.int. 27 October 2011. Retrieved 9 July 2012.
- [7]. "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.
- [8]. Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology 4 (1): 3-72. doi:10.1007/BF00630563.
- [9]. "The Cryptography Guide: Triple DES". Cryptography World. Retrieved 2010-07-11.
- [10]. Vincent Rijmen (1997). "Cryptanalysis and Design of Iterated Block Ciphers" (PostScript). Ph.D thesis.
- [11]. 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
- [12]. 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
- [13]. 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