CUSTOMIZED DATA ENCRYPTION ALGORITHM

Ritu Shukla

Abstract— Data security is one of the most difficult aspects in the web and network applications. Internet and networks applications are mounting very fast, which is increasing the importance and the worth of the exchanged data over the internet or other types of media.
We constantly endeavor to get enhanced algorithms which can work to secure the data wholly. A variety of good algorithms is available and has been used in the cryptography. Mainly stream and block ciphers are accessible and International Data Encryption Algorithm (IDEA) is one of them, which was regarded debatably as one of the best for the purpose of encryption. The attacks like brute force and the combination of weak sub-keys reduce its security.
This paper describes an extension of IDEA algorithm which is immune to the attacks. In this, the number of rounds which are fixed i.e. 8 in the standard algorithm can be varied. That means the user can choose the level of complexity by entering the number of rounds either 4 or 8.

Index Terms—Customized Data Encryption Algorithm (CDEA), Data Encryption Algorithm (DES), Decryption, Encryption, Fiestal Network, International Data Encryption Algorithm (IDEA),.

1 INTRODUCTION

IDEA is an iterated block cipher algorithm based on the Fiestel network. It was designed by Xuejia Lai and James Massey in 1991. Feistel network or Fiestel cipher is a symmetric structure used in the construction of block ciphers. It was named after the German cryptographer Horst Feistel. A Feistel network is an iterated cipher with an internal function called a round function. Iterated block ciphers are constructed by repeatedly applying the round function. The number of rounds varies from algorithm to algorithm. The general setup of each round is almost the same. A key schedule is an algorithm that, given the key, calculates the subkeys for these rounds. A large number of block ciphers use the scheme, including the Data Encryption Standard (DES), IDEA etc [12]. The advantage of Fiestel Cipher is that the operations of encryption and decryption are very similar or even identical. This reduces the size of the code almost by half. The only change required is a reversal of the key schedule and inversion of their values. Hence, the Feistel network model scores over substitution and transposition models as the round function need not be invertible. A block cipher encryption algorithm (E) takes plaintext M of a particular length and key K as an input, and outputs a corresponding cipher text of the same length. The decryption algorithm (E_1) takes the cipher text as an input together with the key, and yields the original block of plaintext of the same length [5]. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.

- *Ritu Shukla is currently pursuing masters degree program in Computer Science & Engineering in Suresh Gyan Vihar University, India, PH-9680335929. E-mail: ritu2159@gmail.com*

2 DESCRIPTION OF THE ALGORITHM

IDEA is a symmetric cryptographic algorithm. It is a block oriented cipher technique i.e the plaintext is first divided into blocks and then processed to convert into an unreadable form i.e the cipher text. It works on 64-bit plain text blocks with the combination of 128-bit key. This combination makes it resistant to brute force attacks [1]. IDEA is based on basic function which is repeated 8 times makes it which complex. It is reversible that means the same steps are implemented for encryption as well as decryption.

The 64-bit block of plain text is fragmented into 4 sub-blocks/portions, each of 16-bits and then these blocks are given as input to the first iteration [6]. The output of the first round is given as input to the next iteration and so on. After the last round i.e. 8th round, its output is given to the final transformation process which produces an output of 64-bit cipher text block. The IDEA completely depends on the three simple operations [4-6]:

1. Bitwise XOR
2. Addition Modulo (2^{16})
3. Multiplication Modulo ($2^{16}+1$)

And, the operations performed in the OUTPUT TRANSFORMATION phase are –

1) Multiplication module $2^{16}+1$.

2) Addition modulo 2^{16}.

These sub-keys are used in the fourteen steps which are repeated 8 times in the form of 8-rounds. Below are the fourteen steps which make a complete round:-

1. Multiply P1 and the first sub-key K1.
2. Add P2 and the second sub-key K2.
3. Add P3 and the third sub-key K3.

4. Multiply P4 and the fourth sub-key K4.
5. Bitwise XOR the results of steps 1 and 3.
6. Bitwise XOR the results of steps 2 and 4.
7. Multiply the result of step 5 and the fifth sub-key K5.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub-key K6.
10. Add the results of steps 7 and 9.
11. Bitwise XOR the results of steps 1 and 9.
12. Bitwise XOR the results of steps 3 and 9.
13. Bitwise XOR the results of steps 2 and 10.
14. Bitwise XOR the results of steps 4 and 10.

Below are the steps which are performed in Output Transformation:-

1. Multiply X1 and the first sub-key.
2. Add X2 and the second sub-key.
3. Add X3 and the third sub-key.
4. Multiply X4 and the fourth sub-key

2.1 Working of Customized Data Encryption Algorithm

The complete working of the algorithm can be easily understood with the help of block diagrams drawn below:

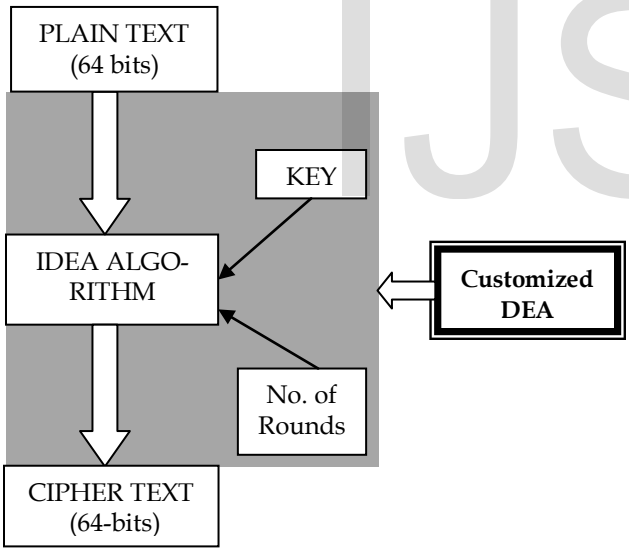

Fig 1. Block Diagram of CDEA

In CDEA, the key and number of rounds are kept secret and the plain text is sent in the encrypted form i.e. the cipher text. Earlier the attacker had to work for finding the key only but now he has two unknown values increases the security and at the same time makes it dynamic.

3 Performances & Security Analysis

The security, performance and the complexity of CDEA is explained using an example:

3.1 Example of CDE Algorithm

The plain text **–"hello"** world this is new in computer Science

The cipher text generated by CDEA:
?>?8½&???>-?{ÙÆ$?SKa-Þ?v?hWÑdm?V?Þ¦u¸1\V?Þ¦u¸1\lAF×.¦?å

Encrypted file will be send to other end via network.

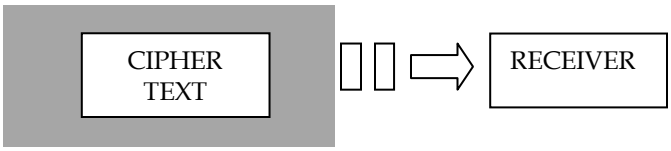

Fig 2. Block diagram of proposed scheme

Table 1
Key matrix for encryption

E_1^1	E_1^2	E_1^3	E_1^4	E_1^5	E_1^6
E_2^1	E_2^2	E_2^3	E_2^4	E_2^5	E_2^6
E_3^1	E_3^2	E_3^3	E_3^4	E_3^5	E_3^6
E_4^1	E_4^2	E_4^3	E_4^4	E_4^5	E_4^6
E_5^1	E_5^2	E_5^3	E_5^4	E_5^5	E_5^6
E_6^1	E_6^2	E_6^3	E_6^4	E_6^5	E_6^6
E_7^1	E_7^2	E_7^3	E_7^4	E_7^5	E_7^6
E_8^1	E_8^2	E_8^3	E_8^4	E_8^5	E_8^6
E_9^1	E_9^2	E_9^3	E_9^4		

Table 2
Key matrix for Decryption

E_9^1	E_9^2	E_9^3	E_9^4	E_8^5	E_8^6
E_8^1	E_8^2	E_8^3	E_8^4	E_7^5	E_7^6
E_7^1	E_7^2	E_7^3	E_7^4	E_6^5	E_6^6
E_6^1	E_6^2	E_6^3	E_6^4	E_5^5	E_5^6
E_5^1	E_5^2	E_5^3	E_5^4	E_4^5	E_4^6
E_4^1	E_4^2	E_4^3	E_4^4	E_3^5	E_3^6
E_3^1	E_3^2	E_3^3	E_3^4	E_2^5	E_2^6
E_2^1	E_2^2	E_2^3	E_2^4	E_1^5	E_1^6
E_1^1	E_1^2	E_1^3	E_1^4		

(Note: Radix or base show round number and power show key number)

On the other end decryption algorithm first decrypt the cipher

text and the text generated from the cipher text received which is desired to be the original text. In decryption, the algorithm will remain same, only the key matrix will be changed.

Cipher Text:

"?>?8½&???>-?{ÙÆ$?SKa-Þ?v?hWÑdm?V?Þ¦u¸1\V?Þ¦u¸1\ lAF×.¦?å"

After decryption form, the original message:-

"hello world this is new in computer Science"

The same algorithm can be applied for number of rounds as 4.

It can processed by applying 16 bits long block of original text which is equivalent to 2 characters and 32 bits long key (4 character).[5]

3.2 Comparison between the execution time

1) IDEA

2) CDEA

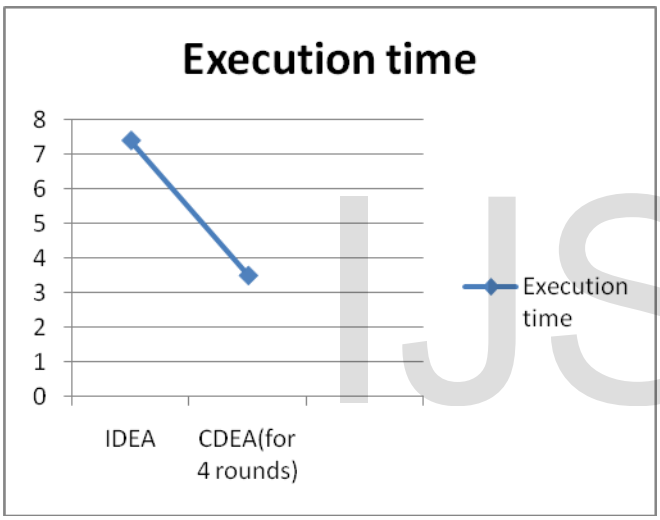

Fig.3 Graph representing execution time

Table 3 Comparison between Execution time of IDEA & CDEA

No. of Rounds	Total time for the process (in milli-seconds)	
	IDEA (in millisec)	Customized IDEA (in millisec)
4		3.5
8	7.3	7.4
16		13.9

4. Conclusion And Future Scope

In private key cryptography, single key is used for encryption as well as decryption. No other key can decrypt the message. IDEA is a symmetric; block-oriented algorithm .The security of IDEA is based on its key generation process and the intelligent combination of mathematical operations in the fourteen steps.

This new method/ algorithm can serve in the following ways:

1) CDEA can reduce as well as decrease the execution time of the process because the user has the authority to choose the number of rounds, depending on the utility of the data to be transferred.
2) The attacker has to lay his hands not only for the keys but also for the number of rounds which increases the complexity and hence make it more secure.

Future Scope

- Finding more efficient cryptanalysis technique for security.
- Finding technique to add more rounds in CDEA.
- Finding technique to decrease the execution time without decreasing the number of rounds.
- Finding different combination of sub-keys.

Acknowledgment

I would like to take this opportunity to express my profound gratitude and deep regard to Mr.Dinesh Goyal, for his exemplary guidance, valuable feedback and constant encouragement.His valuable suggestions were of immense help throughout this work. His perceptive criticism kept me working to make it in a much better way. Working under him was an extremely knowledgeable experience for me.

I would also like to give my sincere gratitude to my parents.The product of this research paper would not be possiblewithout them.

References

[1] William Stallings, "Cryptography and Network Security", ISBN 81-317-0366-5, Pearson Education, Second Edition, pgs. 29-31,42-94, 121-144,253-297.

[2] R.Rivest, A.Shamir and L.Adleman,"A Method for Obtaining Digi tal signatures and Public-key Cryptosystems", Communications of the ACM, 21 (2), February 1978, pgs 120-126.

[3] Atul Kahate, "Cryptography and Network security", ISBN-10:0-07-064823-9, TATA McGraw-Hill Publishing Company Limited, India, Second Edition, pgs 38-62, 152-165, 205-240.

[4] Anoop MS (2007) Public key cryptography – Applications Algo rithms and Mathematical Explanations. India: TataElxsi. http://www.dkrypy.com/home/pkcs. (23/03/2010)

[5] Research Paper- A simplified IDEA Algorithm by Nick Hoffman.

[6] Sandipan Basu- IDEA-a typical illustration, JGRCS, ISSN-2229-

37IX, Volume 2, 7, July, 2011.
[7] Pontjho M. Mokhonoana, Martin S. Olivier- "APPLICATION OF MESSAGE DIGESTS FOR THE VERIFICATION OF LOGICAL FO RENSIC DATA".
[8] Kamaldeep Sharma, Ashish Kumar – "Study and Performance Analysis of IDEA", Vol.2, Issue 5, My 2012, ISSN: 2277 128X.
[9] Chang H.S.,"International Data Encryption Algorithm" CS-627-1 fall, 2004.
[10] X.Lai and James L. Massey, "A proposal for A New Block En cryption Standard" Advances in Crptology EUROCRYPTO'90, Springer-Verlag Berlin 1991.
[11] Philip Hawkes, "Differential-Linear Weak Key Classes of IDEA", Springer-Verlag, 1998.
[12] Meier, W., On the Security of the IDEA block cipher, Advances in Cryptology.
[13] Phan, R. 2002. Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. Cryptologia. 26 (4): 283 - 306.
[14] Schaefer, E. 1996. A Simplified Data Encryption Standard Algorithm. Cryptologia. 20 (1): 77- 84.
[15] Schneier, B. 1996. Applied Cryptography, Second Edition. Wiley.