Implementation of International Data Encryption Algorithm

P.Devi Pradeep[#1], Dr.A.Kamala Kumari[*2]

[#] *Department of ECE , ANITS ,VISAKHAPATNAM, India-531162*

* *Department of instrument Technology, ANDHRAUNIVERSITY, VISAKHAPATNAM, India-530003*

Abstract

Now-a-days there are many security algorithms that are used for security purpose. IDEA is one of them. The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process. The drawback of IDEA is that the large numbers of weak keys were found in IDEA (International Data Encryption Algorithm). Also a new attack on round 6 of IDEA has been detected. This paper describes the design and implementation of secure data encryption algorithm(S-IDEA) protocol, the size of the key has been increased from 128 bits to 256 bits. This increased key size will increase the complexity of the algorithm. To increase the amount of diffusion two MA blocks (multiplicative additive block) are used in a single round of IDEA as compared to one MA block used previously in a single round, with these modifications in the proposed algorithm will increase the cryptographic strength.

Keywords — *cipher, cryptography, encryption, decryption, key*

I. INTRODUCTION

The International Data Encryption Algorithm (IDEA) is a symmetric-key, block cipher. It was published in 1991 by Lai, Massey, and Murphy. IDEA is a modification of the Proposed Encryption Standard (PES) that was published in 1990 by Lai and Massy; PES was designed as a replacement for the Data Encryption Standard (DES). The algorithm was modified and published in 1991 after Biham and Shamir described the technique of differential cryptanalysis. The new algorithm was called the Improved Proposed Encryption Standard (IPES); its name changed to IDEA in 1992. IDEA is a candidate block cipher to the NESSIE Project. NESSIE is a project within the Information Societies Technology (IST) Program of the European Commission. Although IDEA did not replace DES, it was incorporated into Pretty Good Privacy (PGP).

The fundamental keywords are defined below.

- Plain text: This is the original message that is intelligible and is fed into the algorithm as input.
- Encryption algorithm: It performs various operations and transformations on the original message (plain text).
- Secret key: It is shared between the sender and the recipient, and is used as an input to the algorithm.
- Cipher text: It is the algorithm's output. It is scrambled message and unintelligible that depends on the plain text and encryption key.
- Decryption algorithm: The reverse operation is applied on the cipher text to get the plain text (original).

II. CRYPTOGRAPHY

It is a technique used to avoid an unauthorized access of data. It helps to provide accountability fairness and accuracy and also provide confidentiality. Broadly, four different kinds of people contributed their efforts in this technique and are: (i) Military, (ii) The Diplomatic Corps,(iii) Diarists, and (iv) Communications System. Cryptography involves two basic operations and is named as encryption and key management. Information/data can be encrypted using a cryptographic algorithm by various keys. The security of cryptographic system is not only dependent on the encryption algorithm but also depends upon the keys used for the encryption. These keys are always kept secured from the hacker and are known as secret key. Key plays an important role in encryption process, which is a main part of cryptography.

A. Need of Cryptography

As almost all the organizations such as banks, railway, military, telecommunication, etc depends upon wireless approaches and are open to all the computer and the networks (LAN, MAN and WAN). Their transfer of funds, information and data all are carried out online. Secured funding and E-mails are the major requirement of all the above said organizations; therefore, it is highly essential to protect the data from the intruders. Electronic data transfer is used in all the present applications and it includes the security of ATM cards, computer passwords, and electronic commerce. Passwords are not good so far for the task due to their short range; therefore, cryptography has wide future because this technique can be able to with stand against the various attacks. The original information is converted to cipher text using a secured key, this process is called encryption. The encoded data is recovered by the process of decryption. The block diagram of cryptographic model is shown in fig1.

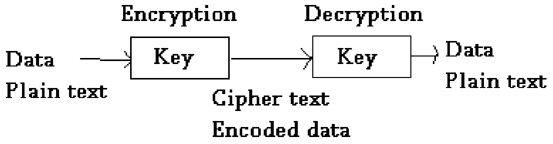


Fig1: Block diagram of Cryptographic Model

B . Secured communication

Secured communication against network is increasing significantly with time. Our communication media should also be secure and confidential. Cryptanalysis is the study used to describe the methods of code-breaking or cracking the code without using the security information, usually used by hackers. For this purpose, the following things can be done by the sender/receiver.

- One can transmit the message secretly, so that it can be saved from hackers.
- The sender ensures that the message arrives to the desired destination.
- The receiver ensures that the received message is in its original form and coming from the authenticate person.

The basic block diagram of secured communication is shown in fig2

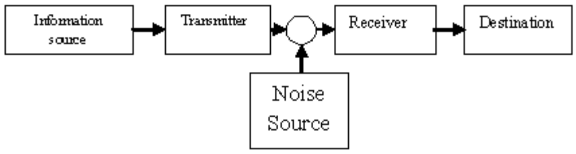


Fig2: Block diagram of Secured Communication

III. IMPLEMENTATION

The functional representation of the encryption process is shown in fig.3 the process consists of eight identical encryption steps followed by an output transformation which is a half round. The structure of the first round is shown in detail in fig3.

The eight rounds are performed using the combination of three algebraic operations:

- Bitwise exclusive OR (⨁).
- Addition modulo 2^16 (⊞).
- denotes multiplication modulo

In each round of the 8 rounds of algorithm, the following sequence of events is performed:

1. Multiply Txt1 by the first sub-key.
2. Add Txtt2 and the second sub-key.
3. Add Txt3 and the third sub-key.
4. MultiplyTxt4 by the fourth sub-key.
5. XOR the results of Steps 1 and 3.
6. XOR the results of Steps 2 and 4.
7. Multiply the results of Step 5 by the fifth sub-key.
8. Add the results of Steps 6 and 7.
9. Multiply the results of Step 8 by the sixth sub-key
10. Add the results of Step 7 and 9.
11. XOR the results of Steps 1 and 9.
12. XOR the results of Steps 3 and 9.
13. XOR the results of Steps 2 and 10.
14. XOR the results of Steps 4 and 10.

The computational process used for decryption of the cipher text is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated.

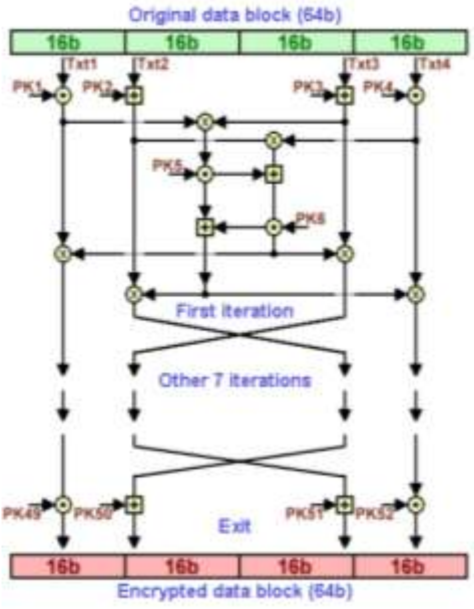


Fig3: Structure of IDEA

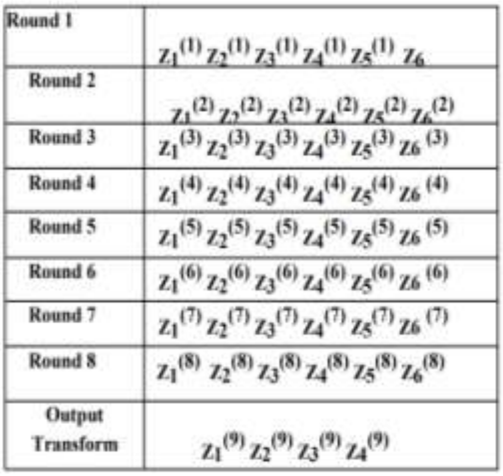
A. Key Generation

The 64-bit plaintext block is partitioned into four 16-bit sub-blocks, since all the algebraic operations used in the encryption process operate on 16-bit numbers. Another process produces for each of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key. Since a further four 16-bit key-sub- blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key. The 52 16-bit key sub-blocks which are generated from the 128-bit key are produced as follows:

- First, the 128-bit key is partitioned into eight 16-bit sub-blocks which are then directly used as the first eight key sub-blocks.
- The 128-bit key is then cyclically shifted to the left by 25 positions, after which the resulting 128-bit block is again partitioned into eight 16-bit sub-blocks to be directly used as the next eight key sub-blocks.
- The cyclic shift procedure described above is repeated until all of the required 52 16-bit key sub-blocks have been generated.

B. Encryption

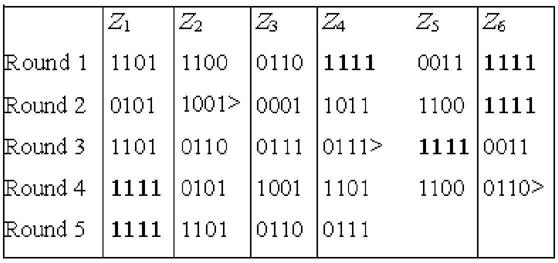
Encryption is the process of converting plain text into cipher text. The process consists of eight identical encryption steps (known as encryption rounds) followed by an output transformation. The structure of the first round is shown in detail in fig4



Round 1	$Z_1^{(1)} Z_2^{(1)} Z_3^{(1)} Z_4^{(1)} Z_5^{(1)} Z_6$
Round 2	$Z_1^{(2)} Z_2^{(2)} Z_3^{(2)} Z_4^{(2)} Z_5^{(2)} Z_6^{(2)}$
Round 3	$Z_1^{(3)} Z_2^{(3)} Z_3^{(3)} Z_4^{(3)} Z_5^{(3)} Z_6^{(3)}$
Round 4	$Z_1^{(4)} Z_2^{(4)} Z_3^{(4)} Z_4^{(4)} Z_5^{(4)} Z_6^{(4)}$
Round 5	$Z_1^{(5)} Z_2^{(5)} Z_3^{(5)} Z_4^{(5)} Z_5^{(5)} Z_6^{(5)}$
Round 6	$Z_1^{(6)} Z_2^{(6)} Z_3^{(6)} Z_4^{(6)} Z_5^{(6)} Z_6^{(6)}$
Round 7	$Z_1^{(7)} Z_2^{(7)} Z_3^{(7)} Z_4^{(7)} Z_5^{(7)} Z_6^{(7)}$
Round 8	$Z_1^{(8)} Z_2^{(8)} Z_3^{(8)} Z_4^{(8)} Z_5^{(8)} Z_6^{(8)}$
Output Transform	$Z_1^{(9)} Z_2^{(9)} Z_3^{(9)} Z_4^{(9)}$

Fig4: Encryption in IDEA

The first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 2^16, and with the other two plaintext blocks using multiplication modulo 2^16 + 1. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round. The process is repeated in each of the subsequent 7 encryption rounds. The four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 2^16 and multiplication modulo 2^16 + 1 to form the resulting four 16- bit cipher text blocks.The simplified IDEA encrypts a 16-bit block of plaintext to a 16-bit block of cipher text. It uses a 32-bit key. The simplified algorithm consists of four identical rounds and a "half round" final transformation. The simplified algorithm mixes three algebraic operations on nibbles (4-bitblocks): bitwise XOR, addition modulo 24(=16), and multiplication modulo 24+1(=17). There are 16 possible nibbles: 0000... 1111, which represent 0... 15, for addition modulo 16. The 16 nibbles are thought of as 0001... 1111, 0000, which represent 1... 15, 16, for multiplication modulo17. Notice that 0000, which is 16, is congruent to -1 modulo 17. 0000 is it own inverse under multiplication modulo 17.



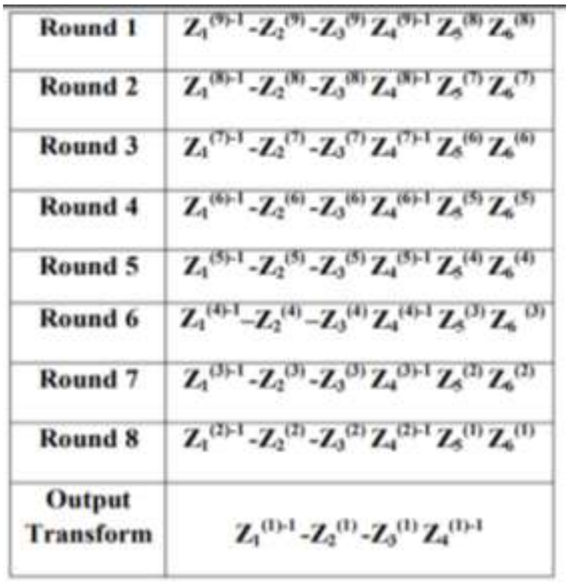
	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6
Round 1	1101	1100	0110	**1111**	0011	**1111**
Round 2	0101	1001>	0001	1011	1100	**1111**
Round 3	1101	0110	0111	0111>	**1111**	0011
Round 4	**1111**	0101	1001	1101	1100	0110>
Round 5	**1111**	1101	0110	0111		

Fig5: Encryption Key Scheduling

The 32-bit key, say 11011100011011110011111101011001 is split into eight nibbles 11011100 0110 1111 0011 1111 0101 1001. The first six nibbles are used as the sub keys for round1.The remaining two nibbles are the first two sub keys for round2, then the bits are shifted cyclically 6places to the left and the new 32-bitstring is split into eight nibbles that become then eight sub keys. The first four of these nibbles are used to complete the sub keys needed for round2, the remaining four sub keys are used in round3.The shifting and splitting process is repeated until all 28 sub keys are generated. Six sub keys are used in each of the 4 rounds. The final 4 sub keys are used in the fifth "half round" final transformation. As an example, we will encrypt the plaintext message 1001110010101100 using the key 110111000110111100111111. The cipher text message is 1011101101001011.

C. Decryption

Converting the cipher text into plain text is known as decryption. It is a complete reverse process of encryption. The computational process used for decryption of the cipher text is essentially the same as that used for encryption of the plaintext. The only difference compared with encryption is that during decryption, different 16-bit key sub-blocks are generated. More precisely, each of the 52 16-bit key sub- blocks used for decryption is the inverse of the key sub-block used during encryption in respect of the applied algebraic group operation. Additionally, the key sub-blocks must be used in the reverse order during decryption in order to reverse the encryption process as shown in fig6.



Round 1	$Z_1^{(9)-1}$ $-Z_2^{(9)}$ $-Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
Round 2	$Z_1^{(8)-1}$ $-Z_2^{(8)}$ $-Z_3^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
Round 3	$Z_1^{(7)-1}$ $-Z_2^{(7)}$ $-Z_3^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
Round 4	$Z_1^{(6)-1}$ $-Z_2^{(6)}$ $-Z_3^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
Round 5	$Z_1^{(5)-1}$ $-Z_2^{(5)}$ $-Z_3^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
Round 6	$Z_1^{(4)-1}$ $-Z_2^{(4)}$ $-Z_3^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
Round 7	$Z_1^{(3)-1}$ $-Z_2^{(3)}$ $-Z_3^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
Round 8	$Z_1^{(2)-1}$ $-Z_2^{(2)}$ $-Z_3^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Output Transform	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

Fig6: Decryption in IDEA

IV. Applications of IDEA

- Today, there are hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government
- The IDEA algorithm can easily be embedded in any encryption software. Data encryption can be used to protect data transmission and storage. Typical fields are:
  - Audio and video data for cable TV, pay TV, video conferencing, distance learning
  - Sensitive financial and commercial data
  - Email via public networks
  - Smart cards

V. Conclusion and Future Scope

IDEA is a well-known cipher that has been analyzed by many researchers for the past decade, and, yet, no attack against five or more of its 8.5 rounds has been found. Due to its strength against cryptanalytic attacks and due to its inclusion in several popular cryptographic packages, IDEA is widely used. [4] The Simplified IDEA algorithm is not intended to be compared for efficiency or security with simplified versions of DES or AES. The Simplified IDEA algorithm is intended to help students understand the IDEA algorithm by providing a version of IDEA that permits examples to be worked by hand and to provide a comparison of the method of IDEA with the methods of DES and AES. As electronic communications grow in importance, there is also an increasing need for data protection. When PGP (Pretty Good Privacy) was designed, the developers were looking for maximum security. IDEA was their first choice for data encryption. The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation. In the future, the DS-IDEA is going to be enhanced by including more security operations that can strengthen the confidentiality, integrity and availability of data that are encrypted using this algorithm. We also plan to apply this modified version of IDEA to other web-based systems in e-business, e-commerce, and e-learning environments with slightly different methods of implementation.

References

[1] M. P. Leong, O. Y. H. Cheung, K. H. Tsoi and P. H. W. Leong, "A bit-serial implementation of the international data encryption algorithm IDEA," Proceedings 2000 IEEE Symposium on Field-Programmable Custom Computing Machines (Cat. No.PR00871), Napa Valley, CA, USA, 2000, pp. 122-131.

[2] International Data Encryption Algorithnm CS-627-Fall 2004 by How-Shen Chang

[3] FPGA Implementation of International Data Encryption Algorithm-.IJESRT by MS.A.D.Chaudhari,Prof.S.D.Josh University of Pune, India

[4] https://www.nku.edu/~christensen/simplified%20IDEA%20algorithm.pdf

[5] Introducing an Encryption Algorithm based on IDEA Osama Almasri , Hajar Mat Jani. https://pdfs.semanticscholar.org/16e1/14914494b68518743740776fd735fb673aee.pdf

[6] https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm