International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 8, August 2014 **ISSN 2319 - 4847**

An Enhancement In International Data Encryption Algorithm For Increasing Security

Author Ms Snehal Patil , Prof.Vrunda Bhusari Dept of Computer BSIOTR Pune

ABSTRACT

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 international data encryption algorithm (IDEA) protocol, it operates on 64 bit plaintext and also 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 also use the 12 rounds instead of 8 rounds. With these modifications in the proposed algorithm will increase the cryptographic strength.

Keywords:- DES,IDEA,MA,S-IDEA etc

1. INTRODUCTION

The Data Encryption Standard (DES) algorithm has been a popular secret key encryption algorithm and is used in many commercial and financial applications. introduced in 1976, it has proved resistant to all forms of cryptanalysis. However, its key size is too small by current standards and its entire 56 bit key space can be searched in approximately 22 hours. International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991. It is a minor revision of an earlier cipher, PES (Proposed Encryption Standard); IDEA was originally called IPES (Improved PES). IDEA was used as the symmetric cipher in early versions of the Privacy crypto system.IDEA was to develop a strong encryption algorithm, which would replace the DES procedure developed in the U.S.A. in the seventies. It is also interesting in that it entirely avoids the use of any lookup tables or S-boxes. When the famous PGP email and file encryption product was designed by Phil Zimmermann, the developers were looking for maximum security. IDEA was their first choice for data encryption based on its proven design and its great reputation.

2. LITERATURE SURVEY

2.1International Data Encryption Algorithm

International Data Encryption algorithm (IDEA) is a block cipher algorithm designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991.The original algorithm went through few modifications and finally named as International Data Encryption Algorithm (IDEA). The mentioned algorithm works on 64-bit plain text and cipher text block (at one time). For encryption, the 64- bit plain text is divided into four 16 bits sub-blocks. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits). Each of these blocks goes through 8 ROUNDS and one OUTPUT TRANSFORMATION phase. In each of these eight rounds, some (arithmetic and logical) operations are performed. Throughout the eight ROUNDS, the same sequences of operations are repeated. In the last phase, i.e., the OUTPUT TRANSFORMATION phase, we perform only arithmetic operations. At the beginning of the encryption process, the 64 bit plain text is divided in four equal size blocks and ready for ROUND1 input. The output of ROUND1 is the input of ROUND2. Similarly, the output of ROUND2 is the input of ROUND3, and so on. Finally, the output of ROUND8 is the input for OUTPUT TRANSFORMATION, whose output is the resultant 64 bit cipher text (assumed as C1 (16bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)). As the IDEA is a symmetric key algorithm, it uses the same key for encryption and for decryption. The decryption process is the same as the encryption process except that the sub keys are derived using a different algorithm [6]. The size of the cipher key is 128bits. In the entire encryption process we use total 52 keys (ROUND1 to ROUND8 and OUTPUT TRANSFORMATION phase); generated from a 128 bit cipher key. In each round (ROUND1 to ROUND8) we use six sub keys. Each sub-key consists of 16bits. And the OUTPUT TRANSFORMATION uses 4 sub-keys.

2.2 Secure-International Data Encryption Algorithm

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. In this paper we are describe 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.

2.3 Improved IDEA

Data security is an important issue in today's computer networks. This paper presents the Improved IDEA chip, which implements a new version of the IDEA cryptographic algorithm. Improved IDEA is oriented towards computer network applications demanding high throughput. Its architecture was based on architecture of the HIP Crypto chip, which exploits both the spatial and the temporal parallelism available in the IDEA algorithm. These new versions can encrypt/decrypt at data rates up to 6.5 Gbps. Cryptographic algorithms are an essential part in network security. A well known cryptographic algorithm is the Data Encryption Standard (DES), widely adopted in security products. Another cryptographic algorithm is the International Data Encryption Algorithm, IDEA. IDEA is considered as one of the most important post-DES cryptographic algorithms, due to its high immunity to attacks. This paper describes the Improved IDEA cryptographic algorithm, a modified version of the IDEA algorithm. The main goal of this new concept is to obtain a performance increase over the original HIP Crypto chip. For this, we replaced the multiply units by SMER function. As consequence, we obtain a circuit twice as faster than the original HIP Crypto circuit.

2.4 Weak Keys for IDEA

Large classes of weak keys have been found for the block cipher algorithm IDEA, previously known as IPES. IDEA has a 128- bit key and encrypts blocks of 64 bits. For a class of 223 keys IDEA exhibits a linear factor. For a certain class of 235 keys the cipher has a global characteristic with probability 1. For another class of 251 keys only two encryptions and solving a set of 16 nonlinear Boolean equations with 12 variables is sufficient to test if the used key belongs to this class. If it does, its particular value can be calculated efficiently. It is shown that the problem of weak keys can be eliminated by slightly modifying the key schedule of IDEA. IDEA is an iterated cipher consisting of 8 similar rounds and a single output transformation. The building blocks of the round function are multiplication modulo $2^{16}+1$, addition modulo 2^{16} and bitwise XOR. IDEA has a 128-bit key and encrypts/decrypts data in blocks of 64 bits.

IDEA

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 substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. 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.

EXISTANCE SYSTEM

There are several modern key-based cryptographic techniques. The two common key based encryption techniques are symmetric and asymmetric key cryptography In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric schemes, one key is used for encryption and another is used for decryption . The increased confidence in the integrity of systems that use encryption is based on the notion that Cipher text should be very difficult to decipher without knowledge of the key .

PROBLEM STATEMENT

This paper describe the design and implementation of international data encryption algorithm (IDEA) protocol, it operates on 64 bit plaintext and also 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 also use the 12 rounds instead of 8 rounds. With these modifications in the proposed algorithm will increase the cryptographic strength. And also reduce the weak keys problem in Daemon's report.

PROPOSED SYSTEM

The proposed encryption algorithm consists of a three level cipher attempt to keep your personal data secure. The first level is achieved through the words compression flowchart in the second level is realized by transforming the compressed words.

This algorithm increase the cryptographic strength.

This algorithm reduce the weak keys problem in Daemon's report.

- The accuracy of the predicted model should be good as compared to other existing algorithm.
- This enhanced algorithm is increasing the security.

SCOPE

The proposed algorithms increased the cryptographic strength and eliminate the shortcoming of the existing International data Encryption algorithm (IDEA).The future scope of S-IDEA algorithm is that it can also be implemented in hardware using VLSI technology.

Mathematical Model

The improved IDEA encrypts a 64-bit block of plaintext to a 64-bit block of cipher text. It uses a 256-bit key. The improved algorithm consists of twelve identical rounds and a "half round" for final transformation.

The improved algorithm mixes three algebraic operations on 12 blocks (16-bit blocks):

1. Bitwise XOR,
2. Addition modulo 2^{32}(=4294967296), and
3. Multiplication modulo $2^{32} + 1$(=4294967297).

The 256-bit key, is split into 16 bit blocks. The first twelve blocks are used as the subkeys for round 1. The remaining four blocks are the first two subkeys for round 2. Then the bits are shifted cyclically 50 places to the left, and the new 256-bit string is split into sixteen blocks that become the next 16 subkeys. The first 12 of these blocks are used to complete the subkeys needed for round 2, and the remaining four subkeys are used in round 3. The shifting and splitting process is repeated until all 148 subkeys (12*12+4) are generated.

Steps:

1. K is 256 bit key.
2. The round keys for round r=1,...,12
3. K cyclically rotated to the left 50·r times.
4. Split the string obtained into eight substrings and call them Z(r)1, ..., Z(r)12.

The keys Z(r) 13 to Z(r) 16 are mask the output in transformation round

3 DESIGN PROCESS

3.1 Description of IDEA

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 substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. 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.

Characteristics of IDEA

To date, no method of cracking IDEA faster than exhaustive key search brute force has been discovered. Comparison of the algorithms

- DES 56-bit key in 1 second
- NSA Skipjack 80-bit key in 194 days
- IDEA 128-bit key in 149745258842898 years
- Software implementation speeds are comparable with those for DES.
- Hardware implementations are just slightly faster.
- Keep the IDEA key safely, you lose it, you DESTORIED your data

Figure 1 gives simply overview of an IDEA algorithm. As we mentioned before, in the IDEA algorithm, we take input text of size 64 bits at a time and divide it in evenly; i.e.64bit plain text is divided into 4 sub-blocks, each of 16bits in size. Now, let us look, what are the basic operations needed in the entire process.

Operations needed in the first 8 rounds

1. Multiplication modulo $2^{16}+1$.
2. Addition modulo 2^{16}.
3. Bitwise XOR.

And, operations needed in the OUTPUT TRANSFORMATION phase

1. Multiplication module $2^{16}+1$.
2. Addition modulo 2^{16}.

All the above mentioned operations are performed on 16 bit sub-blocks.

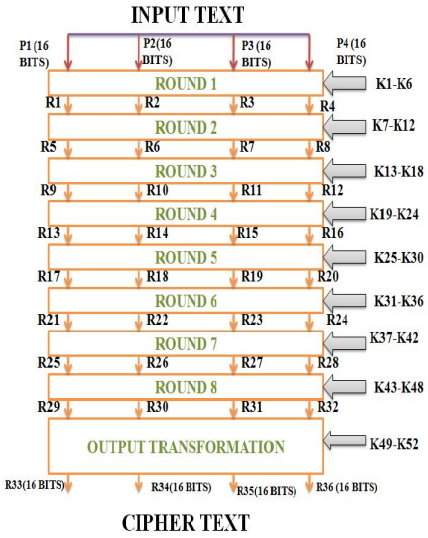

Figure 1 Overview of an IDEA algorithm

3.1.1 Single Round Encryption

The functional representation of the encryption process is shown in Figure 2 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.

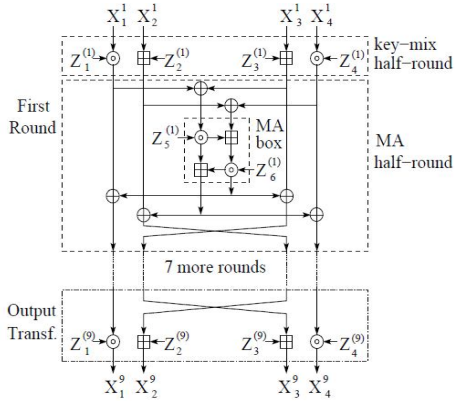

Figure 2 Single Round Encryption

In the first encryption round, 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 $2^{16} + 1$. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8^{th} 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.

3.1.2 Modes of operations

For a description of IDEA, we follow Schneier, who breaks the encryption algorithm into fourteen steps. For each of the eight complete rounds, the 64-bit plaintext block is split into four 16-bit sub-blocks: X1, X2, X3, X4. The 64-bit input block is the concatenation of the sub blocks: X1 k X2 k X3 k X4, where k denotes concatenation. Each complete round requires six sub keys. The 128-bit key is split into eight 16-bit blocks, which become eight subkeys. The first six subkeys are used in round one and the remaining two subkeys are used in round two. We will discuss the generation of the remaining keys in the next section. Each round uses each of the three algebraic operations: bitwise XOR, addition modulo 2^{16}, and multiplication modulo $2^{16} + 1$. Here are the fourteen steps of a complete round (multiply means multiplication modulo $2^{16} + 1$, and add means addition modulo 2^{16}):

1. Multiply X1 and the first subkey Z1.
2. Add X2 and the second subkey Z2.
3. Add X3 and the third subkey Z3.
4. Multiply X4 and the fourth subkey Z4.
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 subkey Z5.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth subkey Z6.
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.

For every round except the final transformation, a swap occurs, and the input to the next round is: result of step 11 k result of step 13 k result of step 12 k result of step 14, which becomes X1 k X2 k X3 k X4, the input for the next round.
After round 8, a ninth "half round" final transformation occurs:

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

The concatenation of the blocks is the output.

4.SYSTEM ARCHITECTURE

The improved IDEA encrypts a 64-bit block of plaintext to a 64-bit block of cipher text. It uses a 256-bit key. The improved algorithm consists of twelve identical rounds and a "half round" for final transformation. The improved algorithm mixes three algebraic operations on 12 blocks (16-bit blocks):

1. Bitwise XOR,
2. Addition modulo 2^{32}(=4294967296), and
3. Multiplication modulo $2^{32} + 1$(=4294967297).

The 256-bit key, is split into 16 bit blocks. The first twelve blocks are used as the subkeys for round 1. The remaining four blocks are the first two subkeys for round 2. Then the bits are shifted cyclically 50 places to the left, and the new 256-bit string is split into sixteen blocks that become the next 16 subkeys. The first 12 of these blocks are used to complete the subkeys needed for round 2, and the remaining four subkeys are used in round 3. The shifting and splitting process is repeated until all 148 subkeys (12*12+4) are generated.

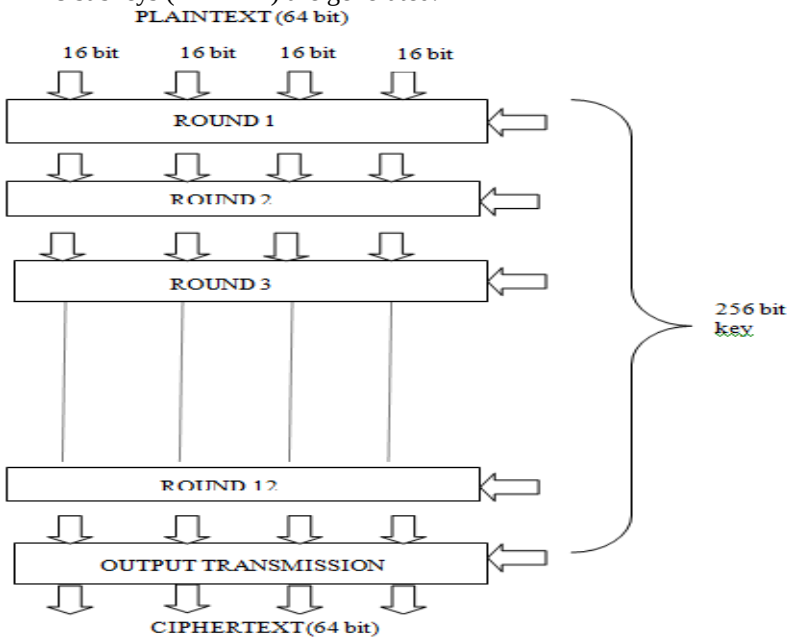

Figure 3 Overview of an Enhanced IDEA Algorithm

Single Round Encryption

In single round encryption Enhanced IDEA uses 12 keys and uses two MA (Multiplicative/additive). And do Three operations on it Bitwise XOR, Addition modulo 2^{32}(=4294967296), and Multiplication modulo $2^{32} + 1$.

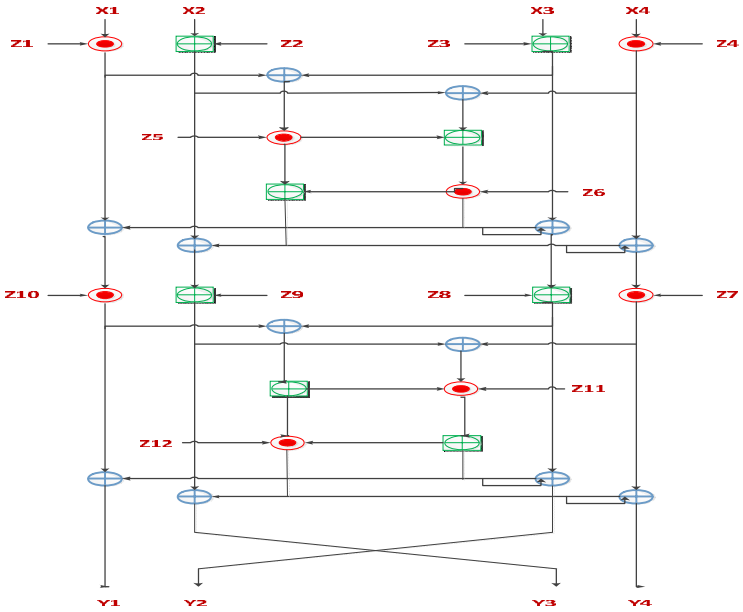

Figure 4 Single Round Encryption

5. SOFTWARE REQUIREMENTS

Operating System : Windows Operating System
Application Libraries: Java and J2EE
Language : J2EE and Java
Front End : Application console

6. HARDWARE REQUIREMENTS

Processor : Pentium IV. (& onwards).
Memory (RAM) :256 MB RAM.
Hard disk : 40GB

7. RESULTS

Results are presented to show the security of the data which is transferred on the network by using An Enhanced International Data Encryption Algorithm. The performance of algorithm is tested by giving several types of input.

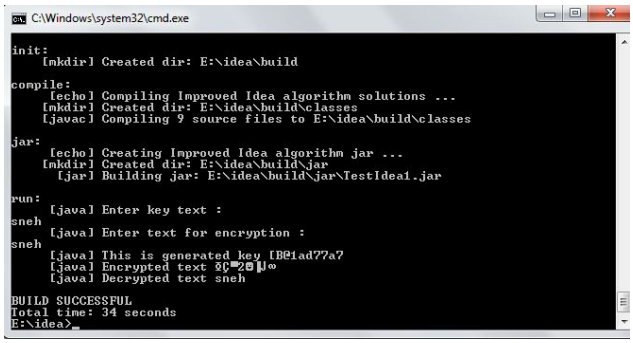

Fig 5 Given input is String (characters).

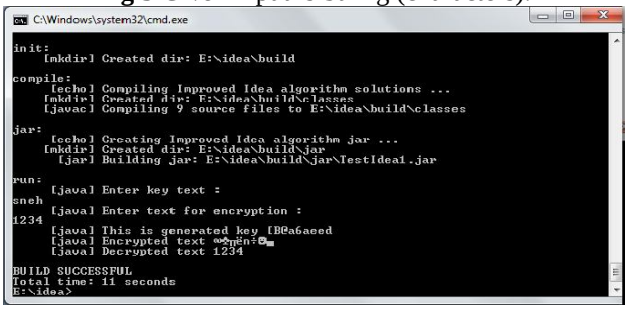

Fig 6 Result when given input is numbers.

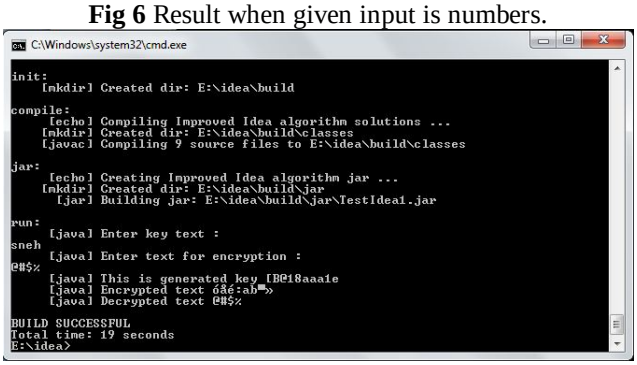

Fig 7 Result when given input is special symbols.

8. FUTURE ENHANCEMENT

The proposed algorithms increased the cryptographic strength and eliminate the shortcoming of the existing International data Encryption algorithm (IDEA).The future scope of Enhanced IDEA algorithm is that it can also be implemented in hardware using VLSI technology.

9. CONCLUSION

An Enhanced IDEA (International Data Encryption Algorithm) is a universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. The Enhanced IDEA (International Data Encryption Algorithm) is a strong block-cipher. Though there are many operations involved in the entire algorithm, only three different of operations are involved and also increased rounds in algorithm increases the security of an algorithm. The Enhanced IDEA (International Data Encryption Algorithm) eliminates the weak keys problem of an IDEA (International Data Encryption Algorithm) by key scheduling of an IDEA (International Data Encryption Algorithm).With a key of 256 bits in length, Enhanced IDEA is far more secure than the widely known DES and original IDEA. The proposed algorithms increased the cryptographic strength and eliminate the shortcoming of the existing International data Encryption algorithm (IDEA).The future scope of S-IDEA algorithm is that it can also be implemented in hardware using VLSI technology.

REFERENCES

[1] Sandipan Basu, INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION in Journal of Global Research in Computer Science
[2] Chang H.S., "International Data Encryption Algorithm" CS-627-1 Fall, 2004.
[3] Lai, Xuejia, and Massey, James L., A Proposal for a New Block Encryption Standard, Advances in Cryptology - EUROCRYPT '90, Lecture Notes in Computer Science, Springer-Verlag, 1991: 389-404.
[4] Harivans Pratap Singh1, Shweta Verma2, Shailendra Mishra, Secure-International Data Encryption Algorithm in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013
[5] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 389-404, 1990
[6] J. Daemen, R. Govaerts, and J. Vandewalle, Weak keys for IDEA, Advances in Cryptology - Crypto '93, Springer-Verlag (1994), pp. 224-231
[7] Thaduri, M., Yoo, S.M. and Gaede, R., "An efficient implementation of IDEA encryption algorithm using VHDL", ©2004 Elsevier.
[8] R. Modugu, N. Park and M. Choi, A Fast Low-Power Modulo 2n+1 Multiplier Design, 2009 IEEE International Instrumentation and Measurement Technology Conference, pp.951-956, May 2009.
[9] Rahul Ranjan and I. Poonguzhali, "VLSI Implementation of IDEA Encryption Algorithm", Mobile and Pervasive Computing(CoMPC –2008).
[10] Dr. Salah Elagooz, Dr. Hamdy,Dr. KhaledShehata and Eng.M. Helmy, "Design and implementation of Highand Low Modulo (216+1) multiplier used in IDEA Algorithm on FPGA", 20th National Radio Science Conference CAIRO, Egypt , March 18-20 , 2003.
[11] Zimmermann,A.Curiger,H.Bonnenberg,H.Kaeslin,N.Felber and W.Fichtner, A 177 Mb/s VLSI implementation of the international data encryption algorithm, IEEE J.Solid-State Circuits, 1994, 29, (3), pp. 303-307