International Journal of Technology and Engineering System (IJTES)
Vol 8. No.1 – Jan-March 2016 Pp. 06-11
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) FOR DATA SECURITY IN CLOUD

S. Artheeswari
Research Scholar Dept(CSE)
Annamalai University,
Annamalainagar, Chidambaram.
art.arthe@gmail.com

Dr.RM. Chandrasekaran,
Professor (CSE) /Controller of Examinations
Annamalai University, Annamalainagar,
Chidambaram.
aurmc@hotmail.com

ABSTRACT

Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. There are a number of security issues/concerns associated with cloud computing. There are many security algorithms that are used for security purpose. International Data Encryption Algorithm (IDEA) is a symmetric key encryption technique that uses same key for both encryption and decryption. This key is of length 128-bit which secures 64-bit data. Also, it runs eight and a half rounds for encrypting and decrypting the data. In order to provide more clarity this paper describes how IDEA algorithm works in cloud security.

Keywords: *International Data Encryption Algorithm (IDEA), Key, Symmetric key encryption, Cryptography, Encryption, Decryption.*

1. *INTRODUCTION*

As the use of internet is becoming widely accepted these days, it is a trend of transmitting data over the network. Exchanging data upon internet results in security problem. The data security over internet can be provided by the cryptography. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. IDEA is one of the ciphers which encrypt the text into an unreadable format and makes it secured in order to send it over to internet. The IDEA encryption algorithm provides high level security not based keeping the algorithm a secret, but rather upon ignorance of the secret key.

I. CONCEPT

IDEA operates on 64-bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a round) and an output transformation (the half-round). DEA derives much of its security by interleaving operations from different groups — modular addition and multiplication, and bitwise eXclusive OR (XOR) — which are algebraically "incompatible" in some sense. In more detail, these operators, which all deal with 16-bit quantities, are:

- Bitwise eXclusive OR (⊕).
- Addition modulo 216 (⊞)
-

  Multiplication modulo 2^{16}+1,where the all-zero word (0x0000) in inputs is interpreted as 2^{16} and 2^{16} in output is interpreted as the all- (0x0000) (⊙).
  zero word

After the eight rounds comes a final "half round", for the output.

i. **Structure:**

XOR is used for both subtraction and ad round function. To work with 16 bit words (meaning four inputs instead of two for the 64 bit block size), IDEA uses the Lai-Massey scheme twice in parallel, with the two parallel round functions being interwoven with each other. To ensure sufficient diffusion, two of the sub-blocks are swapped after each round.

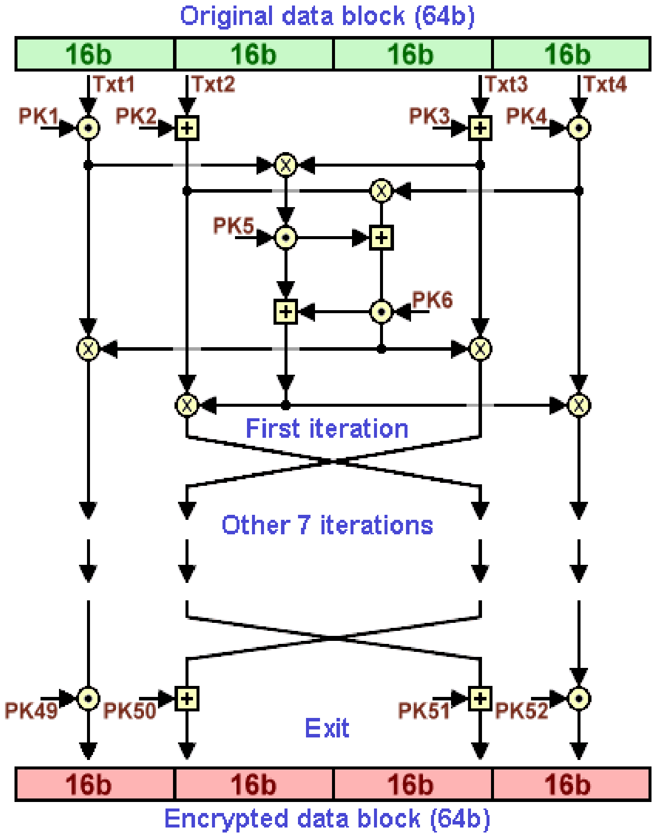


Figure 1 : Structure of IDEA

ii. **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.

Table 1: Encryption of the key sub blocks

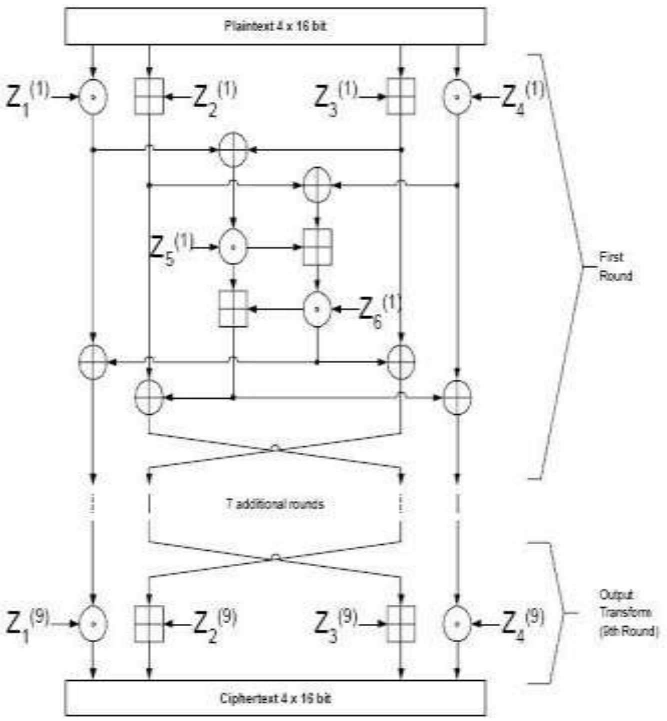
Round 1	$Z_1^{(1)}\ Z_2^{(1)}\ Z_3^{(1)}\ Z_4^{(1)}\ Z_5^{(1)}\ Z_6$
Round 2	$Z_1^{(2)}\ Z_2^{(2)}\ Z_3^{(2)}\ Z_4^{(2)}\ Z_5^{(2)}\ Z_6^{(2)}$
Round 3	$Z_1^{(3)}\ Z_2^{(3)}\ Z_3^{(3)}\ Z_4^{(3)}\ Z_5^{(3)}\ Z_6\ ^{(3)}$
Round 4	$Z_1^{(4)}\ Z_2^{(4)}\ Z_3^{(4)}\ Z_4^{(4)}\ Z_5^{(4)}\ Z_6\ ^{(4)}$
Round 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	$Z_1^{(9)}\ Z_2^{(9)}\ Z_3^{(9)}\ Z_4^{(9)}$

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.

II. *ENCRYPTION:*

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.



- 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 ciphertext blocks.

III. DECRYPTION:

Table 2: Decryption of the key sub blocks

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	$Z_1^{(1)-1} -Z_2^{(1)} -Z_3^{(1)} Z_4^{(1)-1}$

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 Table 2.

IV. APPLICATIONS

Hundreds of IDEA-based security solutions available in many market areas, ranging from Financial Services, and Broadcasting to Government. IDEA is the name of a proven, secure, and universally applicable block encryption algorithm, which permits effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were highest security requirements along with easy hardware and software implementation for fast execution.

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, business TV, VoIP
- Sensitive financial and commercial data
- Email via public networks
- Transmission links via modem, router or ATM link, GSM technology
- Smart cards

V. CONCLUSION

IDEA is a patented and universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties. The fundamental criteria for the development of IDEA were military strength for all security requirements and easy hardware and software implementation. The algorithm is used worldwide in various banking and industry applications. They predestine the algorithm for use in a great number of commercial applications. Our proposed system is to use IDEA to secure the cloud data.

REFERENCES

[1] *How-Shen Chang, "International Data Encryption Algorithm", CS627-1 Fall 2004.*

[2] *William Stallings, "Cryptography And network Security: Principles and Practice second edition", ISBN 0-13869017-0, 1995 by Prentice- Hall, Inc. Simon & Schuster / A Viacom Company Upper Saddle River, New Jersey 07458.*

[3] *Archita Bhatnagar, Monika Pangaria, Vivek Shrivastava "Enhancement Of Security In International Data Encryption Algorithm (Idea) By Increasing Its Key Length" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013`*

[4] *Nick Hoffman, A Simplified Idea Algorithm.*

[5]*Khovratovich, D.; Leurent, G.; Rechberger, C. "Narrow-Bicliques: Cryptanalysis of Full IDEA". Springer-Verlag.*

[6] *Bruce Schneier, "Applied Cryptography",John Wiley & Sons, second ed., 1996.*

[7] *Yi-Jung Chen, Dyi-Rong Duh And Yunghsiang Sam Han, "Improved Modulo (2n + 1) Multiplier for IDEA", Journal Of Information Science And Engineering 23, 907-919 (2007).*

[8] *Dr. Natarajan Meghanathan, "Public Key Encryption RSA Algorithm".*

[9] *Carlos Frederico Cid, "Cryptanalysis of RSA: A Survey".*

[10] *Electronic Frontier Foundation, "DES challenge III broken in record 22 hours," January1999.*

[11] *Ascom, IDEACrypt Coprocessor Data Sheet,*
1999

[12] *H. Bonnenberg, A. Curiger, N. Felber, H. Kaeslin, and X. Lai, "VLSI implementation of a new block cipher," in Proceedings of the IEEE International Conference on Computer Design: VLSI in Computer and Processors, pp. 501-513, 1991.*

[13] *J. Borst, L.R. Knudsen and V. Rijmen, Two Attacks on Reduced IDEA, Advances in Cryptology - EUROCRYPT 1997, Springer- Verlag (1992), pp. 1-13*

[14] *A. Curiger, H. Bonnenberg, R. Zimmerman, N. Felber, H. Kaeslin, and W. Fichtner, "VINCI: VLSI implementation of the new secret-key block cipher IDEA," in Proceedings of the IEEE Custom Integrated Circuits Conference, pp. 15.5.1-15.5.4,*
1993.

[15] *J. Daemen, R. Govaerts, and J. Vandewalle, Weak keys for IDEA, Advances in Cryptology - Crypto '93, Springer-Verlag (1994), pp. 224-231* ***[16]*** *X. Lai, J.L. Massey and S. Murphy, Markov ciphers and differential cryptanalysis, Advances in Cryptology - Eurocrypt '91, Springer-Verlag (1992), pp. 17-38.*

[17] *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," 2000 IEEE Symposium on Field- Programmable Custom Computing Machines, IEEE (2000), pp. 122-131.*

[18] *S. L. C. Salomao, V. C. Alves, and E. M. C. Filho, "HiPCrypto: A high-performance VLSI cryptographic chip," in Proceedings of the Eleventh Annual IEEE ASIC Conference, pp. 7-*
11, 1998.

[19] *S. Wolter, H. Matz, A. Schubert, and R. Laur, "On the VLSI implementation of the international data encryption algorithm IDEA," in Proceedings of the IEEE International Symposium on Circuits and Systems, vol. 1, pp. 397-400, 1995.*

[20] *R. Zimmermann, A. Curiger, H. Bonnenberg,H. Kaeslin, N. Felber, and W. Fichtner, "A*
177Mb/sec VLSI implementation of the

international data encryption algorithm," IEEE Journal of Solid-State Circuits, vol. 29, pp. 303-307, March 1994.