ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

CONVERTING INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) INTO ASYMMETRIC KEY CIPHER

Archita Bhatnagar[1], Monika Pangaria[2], Vivek Shrivastava[3]

Student, Dept. of Information Technology, I.T.M. College, Bhilwara, Rajasthan, India [1]

Student, Dept. of Information Technology, I.T.M. College, Bhilwara, Rajasthan, India [2]

Asst. Prof., Dept. of Information Technology, I.T.M. College, Bhilwara, Rajasthan, India [3]

Abstract: International Data Encryption Algorithm (IDEA) is a symmetric key encryption technique and uses 128-bit key over 64-bit plain text with eight and a half round. To enhance the technology in IDEA, a new approach is introduced in which we will establish two different keys for encryption and decryption respectively which was single key in IDEA. This will introduce more security in IDEA by making it an asymmetric key encryption algorithm.

Keywords: International Data Encryption Algorithm (IDEA), Asymmetric key encryption.

I. INTRODUCTION

As the use of internet is becoming widely accepted these days, it is a trend of transmitting data over the network. But, people have discovered ways to breach the security of the data which has to be sent over network. Providentially, there came into existence a method to make our data secured against the hacking and it is known as cryptography.

Cryptography is a method which is used to secure the data by converting it into such a format which can only be read by the recipient and not by the intruders.

In the cryptography, 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.

II. CONCEPT

International Data Encryption Algorithm converts a 64-bit plain text into 64-bit cipher text using a single key of 128-bits both for encryption and decryption. For imparting more security to IDEA cipher, we will implement another cipher with IDEA i.e. RSA cipher. RSA cipher is an asymmetric key cipher which uses two different keys for encryption and decryption. This is named as E-IDEA.

III. WORKING

Encryption:

A plain text (T) acts as an input for the encryption process in E-IDEA. The first process of encryption of EIDEA is the IDEA Encryption block. So, this plain text (T) goes to IDEA encryption block. Here, the key used is ‘x’. The text from this block gets converted into cipher text, T_1. This T_1 is cipher text of IDEA encryption block and acts as input i.e. plain text for RSA encryption block. Since, RSA is an asymmetric key cipher, it uses two different keys. Hence, the key applied is ‘x+y’ where ‘x’ is the key from above block and ‘y’ is Public key in RSA block. Here in this block, T_1 gets encrypted into final cipher text i.e. T_2.

The whole encryption part of E-IDEA is described in the following flowchart.

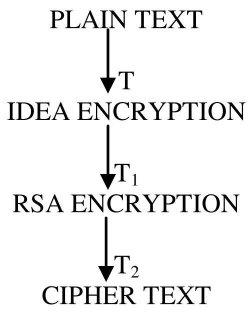

Fig. 1 Flowchart representing encryption in E-IDEA

In encryption phase, the plain text is to be encrypted and converted into cipher text using two ciphers, IDEA and RSA. Encryption by both ciphers is discussed in following phases. In order to achieve the advancements in the cipher, RSA is introduced in the IDEA cipher. This brings up two different phases of encryption:

PHASE I: We apply IDEA cipher and generate key and text. Let the key be 'x' and text be 'x/2'. This phase lasts for 8 rounds (R1, R2, R3, R4, R5, R6, R7 and R8) and a last formation round (half round). Each full round uses different set of sub keys viz. R1, R2, R3 , R4, R5, R6, R7 and R8 uses 6 sub keys (Z1, Z2, Z3, Z4, Z5 and Z6) since these are full rounds. And the half round uses only four sub keys Z1, Z2, Z3 and Z4. This phase is same for all the IDEA ciphers. The plain text 'T' in this phase is converted into cipher text 'T1'.

PHASE II: In this phase, we introduce the RSA cipher in IDEA cipher. The RSA algorithm involves the presence of another whole cipher which increases the steps of operation in addition to those of IDEA. As RSA is an asymmetric key cipher, it introduces the concept of two different keys, one for encryption (public key) and the other one for decryption (private key). This phase treats T1 as an input (plain text) and encrypts it into 'T2'. T2 is the final encrypted text.

T= Plain text

T1= Cipher text after IDEA cipher and Plain text for RSA cipher.

T2= Final cipher text.

$$T \xrightarrow{IDEA} T1$$

$$T1 \xrightarrow{RSA} T2$$

Decryption:

The cipher text (T_2) of the encryption block of E-IDEA acts as an input (plain text) for the decryption process in E-IDEA. Since, encryption with RSA is done at the end; decryption with RSA will take place before that of IDEA. So, the input goes to RSA decryption block. Here, the key used is 'x+z' where 'x' is the key from IDEA encryption block and 'z' is Private Key in RSA block. The text from this block gets converted into plain text, T_1. This T_1 is plain text of RSA decryption block and acts as input i.e. cipher text for IDEA decryption block. In IDEA block, the key applied is 'x' which is same to that of IDEA encryption block since it is symmetric key cipher. Here in this block, T_1 gets decrypted into final plain text i.e. T. The whole decryption part of E-IDEA is described in the following flowchart.

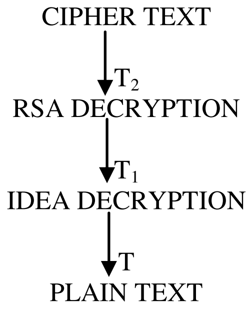

Fig. 2 Flowchart representing decryption in E-IDEA

IV. RELATED ISSUES

According to [4], the IDEA is designed into a stronger algorithm against differential cryptanalytic attacks after being revised.

According to [7], RSA is the most popular security products and cipher protocols which are being used today. It is one of the bases for secure communication in the Internet.

V. MERITS AND DEMERITS

Merits:

This new cipher does not have the concept of weak keys and since there are no classes of weak keys, security issues cannot be caused. Also, easy detection and recovery of the keys is not possible.

Demerits:

Since, two ciphers are involved in E-IDEA; this makes it a long procedure.

Therefore, much time and efforts is needed to fully implement this new cipher.

VI. APPLICATIONS

-Sensitive financial and commercial data security
- E-mail via public networks
- Smart cards
- Transmission links via MODEM, Router or ATM link
- GSM technology

VII. FUTURE SCOPE & CONCLUSION

Future Scope:

E-IDEA has united IDEA cipher with RSA cipher for making the keys strong hence undetectable and unrecoverable. But it makes it a heavy operation to be taken out as the whole operation gets divided into two. One operation is that which involves the IDEA cipher and another operation involves the RSA cipher. This division of operations makes it a lengthy procedure to be carried out which takes much of time and efforts. So, such an algorithm can be created which uses less time and fewer efforts.

Conclusion:

Since, IDEA had weak key classes which hindered in the faultless security of the data; there was a need of such a cipher which does not have weak keys. E-IDEA made it possible to fade away the weak keys from the cipher hence increased the data security. It uses RSA algorithm in addition to the IDEA cipher making an enhancement in it. Now the keys cannot be detected easily. So, data recovery is not possible. The addition of RSA cipher has included the concept of two different keys each for encryption and decryption which was only one key in IDEA.

REFERENCES

[1] Bruce Schneier, *"Applied Cryptography",* John Wiley & Sons, second ed., 1996.
[2] How-Shen Chang, "International Data Encryption Algorithm", CS-627-1 Fall 2004.
[3] NICK HOFFMAN, A Simplified Idea Algorithm
[4] William Stallings, "CRYPTOGRAPHY ANDNETWORK SECURITY: Principles and Practice SECOND EDITION", ISBN 0-13-869017-0, 1995 by Prentice-Hall, Inc. Simon & Schuster / A Viacom Company Upper Saddle River, New Jersey 07458.
[5] Yi-Jung Chen, Dyi-Rong Duh And Yunghsiang Sam Han, "Improved Modulo (2^n + 1) Multiplier for IDEA", Journal Of Information Science And Engineering 23, 907-919 (2007).
[6] Dr. Natarajan Meghanathan, "Public Key Encryption RSA Algorithm".
[7] Carlos Frederico Cid, "Cryptanalysis of RSA: A Survey".