ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Augmenting the Protection of Data in International Data Encryption Algorithm (Idea) By Increasing Steps of Operation

Archita Bhatnagar[*1], Vivek Shrivastava[2]
[*1] M.Tech(I.T.) Student,I.T.M. College, India
[2] Asst. Prof. (I.T.), I.T.M. College, India
archita.bhatnagar09@gmail.com

Abstract

As the transmission of data over internet is increasing; the protection issues of data are increasing as well. In order to protect the data and to secure it against intruders, there is a need of such systems which provide security to data. These techniques are known as cryptography or simply cipher. One of the ciphers is International Data Encryption Algorithm (IDEA). This cipher is symmetric in nature i.e. uses only one key both for encryption and decryption. IDEA uses 128-bit key to encrypt the 64-bit data using certain rounds of operation. In this case, eight and half rounds are used. To augment the protection of data in IDEA, some extra steps of operation will be introduces in the system. For increasing the steps of operation, a different cipher, RSA, is merged with IDEA.

Keywords: International Data Encryption Algorithm (IDEA), Cryptography, Cipher, RSA, Rounds of Operation.

Introduction

Transmitting sensitive data over internet has become a drift these days. This technique for exchanging the data on internet is easy but brings some risk factors too. For protection of data from getting insecure, there are techniques available which are known as cryptography or cipher systems. Cryptography converts the data into a form which cannot be easily deciphered by the intruders but by the intended recipient.

Concept

International Data Encryption Algorithm is the cipher which uses 128-bit key over 64-bit data and runs for eight and half rounds.

This cipher is joined with another cipher RSA in order to make this new cipher run for more rounds of operations as both ciphers follow their own rounds of operations.

This new cipher is coined as A-IDEA (Augmented IDEA).

Working

In A-IDEA, the raw data (T) is acted upon by the encryption by IDEA. Then it undergoes encryption by RSA. After the final encryption has been done, it is decrypted by RSA, then by IDEA.

ENCRYPTION:-

IDEA Encryption:

The data to be encrypted by IDEA is denoted as 'T'. Certain rounds of operation are followed in order to encrypt the raw data by IDEA cipher. Here, the no. of rounds followed is eight full rounds and a half round. For each of the eight complete rounds, the 64-bit plaintext block is split into four 16-bit sub-blocks: X_1, X_2, X_3, and X_4. The 128-bit key is split into eight 16-bit blocks, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8, which become eight sub keys. The first six sub keys are used in round one, and the remaining two sub keys are used in round two.

***According to [2],* the rounds of operation are:**

1. Multiply X_1 and the first sub key Z_1.
2. Add X_2 and the second sub key Z_2.
3. Add X_3 and the third sub key Z_3.
4. Multiply X_4 and the fourth sub key Z_4.
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 Z_5.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub key Z_6.
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- result of step 13- result of step 12-result of step 14, which becomes X_1 - X_2 - X_3 - X_4, the input for the next round.

ISSN: 2277-9655
Impact Factor: 1.852

After round 8, a ninth "half round" final transformation occurs:
1. Multiply X_1 and the first sub key.
2. Add X_2 and the second sub key.
3. Add X_3 and the third sub key.
4. Multiply X_4 and the fourth sub key.
The concatenation of the blocks is the output and is denoted as 'T_1'

RSA Encryption:

'T_1' comes as an input in this block. Encryption in RSA consists of the steps of key generation. *According to* [4], the key generation steps are:
Step 1: Choose two distinct prime numbers randomly; say 'p' and 'q'. p and q must be of same bit length.
Step 2: Calculate 'n' with the help of formula n=p*q. This 'n' will serve as modulus for both public and private key.
Step 3: Compute φ (n) = (p-1) (q-1). φ (n) is the Euler's totient function i.e. positive integer less than or equal to 'n' are prime to 'n'.
Step 4: Choose an integer 'e' such that 1<e< φ (n). Also, gcd(e, φ (n))=1. We can say that 'e' and 'φ (n)' are co-primes.
This 'e' will be treated as PUBLIC KEY EXPONENT.
Step 5: Compute multiplicative inverse of e.
d-1 =e(mod φ (n))
This'd' will be treated as PRIVATE KEY EXPONENT.
Hence, summarizing the above steps, we find that,
Public Key=n+e
Private Key=n+d
The data is encrypted by RSA using the public key which is shared and is not secret. This encrypted data becomes 'T_2' and is final encrypted data.

Final encryption is depicted in following flowchart:

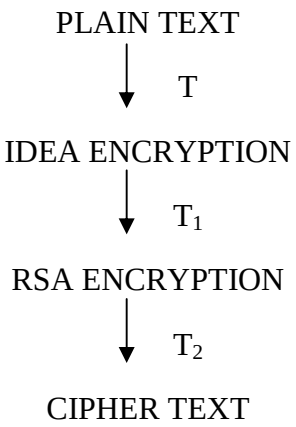

Fig.: Flowchart representing full encryption in A-IDEA

Decryption

RSA Decryption:

The finally encrypted data 'T_2' is the input for decryption process of RSA. In this, the private key which is created in key generation procedure is used to decrypt the data. This private key is secret key and is not shared. The output of this block is 'T_1'

IDEA Decryption:

When the data is decrypted by RSA it becomes the input for IDEA decryption i.e 'T_1'. Here, the steps of operation are same as in encryption process of IDEA, only the key schedule gets changed. This output is 'T' i.e. final decrypted data.

Final decryption is depicted in following flowchart:

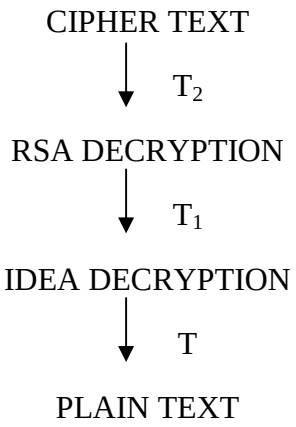

Fig.: Flowchart representing decryption in A-IDEA

Merits and Demerits

Merits:

A-IDEA runs for many rounds as it follows rounds of IDEA as well as those of RSA which leads us to minimization of weak keys. These weak keys may cause breach of security of data. So, after combining IDEA with RSA, no weak keys may violate the data protection.

Demerits:

In A-IDEA, we have implemented two ciphers in order to increase the steps of operation. This has made this cipher a heavy one which may take much cost, efforts and time.

Applications

- Augmented protection of such data which is perceptive in nature can be easily provided.
- In public networks, the data protection can be provided by A-IDEA.
- Smart cards can be protected.

ISSN: 2277-9655
Impact Factor: 1.852

Conclusion & Future Scope

Conclusion:

We have created a new cipher A-IDEA which increases the steps and rounds of operation of the cipher in order to augment the protection of the data. For this, two ciphers, IDEA and RSA, are mingled with each other. As both ciphers will follow their own rounds and steps, it will increase the no. of rounds and steps in the new cipher.

Future Scope:

This new cipher is made up by converging two different ciphers, IDEA and RSA. This congregation of two ciphers lead the new cipher become more bulky as the rounds of operation in each cipher takes its own time, cost and efforts. This may be checked in future that something may be done in order to lessen the efforts to be taken for making the cipher more secured.

References

[1] How-Shen Chang, "International Data Encryption Algorithm", CS-627-1 Fall 2004.
[2] NICK HOFFMAN, A Simplified Idea Algorithm
[3] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, second ed., 1996.
[4] Dr. Natarajan Meghanathan, "Public Key Encryption RSA Algorithm".
[5] 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.
[6] 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).
[7] Carlos Frederico Cid, "Cryptanalysis of RSA: A Survey"