ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

ENHANCEMENT OF SECURITY IN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) BY INCREASING ITS KEY LENGTH

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

M.Tech Student, Information Technology, Institute of Technology and Management, Bhilwara, India [1]
M.Tech Student, Information Technology, Institute of Technology and Management, Bhilwara, India [2]
Assistant Professor, Information Technology, Institute of Technology and Management, Bhilwara, India [3]

Abstract: Security of the data has become most important in today's world. In order to provide security to the data over internet, there is a technique known as Cryptography. One of the encryption techniques, which secure the data over internet, is International Data Encryption Algorithm (IDEA). IDEA uses same key both for encryption and decryption. This key is of length 128-bit which secures 64-bit data. Also, it runs for certain rounds for encrypting and decrypting the data, here, runs for eight and a half rounds. In order to provide more security to the data, a new system is proposed here which has a longer key length.

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

I. INTRODUCTION

Exchanging data upon internet has become widely accepted in recent years. This advancement in technology makes it easy for the data trade but arises a major issue i.e. security of the data. The data security over internet can be provided by the *cryptography*, which is defined as the conversion of readable data into non readable form for transmission purpose and back to readable form when gets transmitted to intended recipient successfully.
Here, IDEA is one of the crypto systems which converts readable data into non readable form for transmission purpose and back to readable form when gets transmitted to intended recipient.

II. CONCEPT

International Data Encryption Algorithm is a crypto system which uses 128-bit key length of symmetric nature in order to convert a data of 64-bit length into non readable format before transmission and back to readable form after successful transmission. In order to enhance the security of IDEA, another cipher, RSA, will be combined with IDEA which will add the length of key i.e. 128-bit+512-bit key length. It is abbreviated as ES-IDEA (Enhanced Security-IDEA)

III. WORKING

There are four processes involved in the ES-IDEA; Encryption by IDEA, Encryption by RSA, Decryption by RSA and Decryption by IDEA.

Encryption by IDEA:
For encryption process of IDEA the raw data (T) acts as input. This data undergoes the encryption by IDEA and gets converted into cipher text (T_1). The key which is used in this process is of 128-bit. The following flowchart describes the encryption process of IDEA.

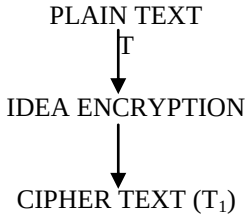

Fig.: Flowchart representing encryption by IDEA

According to [1], the IDEA processes of encryption are as follows:
The 64-bit plaintext block is split into four 16-bit sub-blocks: X_1, X_2, X_3, X_4.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

The 128-bit key is split into eight 16-bit blocks, which become eight subkeys $Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8$. The first six subkeys are used in round one, and the remaining two subkeys are used in round two.
Steps are:
STEP1. Multiply X_1 and the first subkey Z_1.
STEP2. Add X_2 and the second subkey Z_2.
STEP3. Add X_3 and the third subkey Z_3.
STEP4. Multiply X_4 and the fourth subkey Z_4.
STEP5. Bitwise XOR the results of steps 1 and 3.
STEP6. Bitwise XOR the results of steps 2 and 4.
STEP7. Multiply the result of step 5 and the fifth subkey Z_5.
STEP8. Add the results of steps 6 and 7.
STEP9. Multiply the result of step 8 and the sixth subkey Z_6.
STEP10. Add the results of steps 7 and 9.
STEP11. Bitwise XOR the results of steps 1 and 9.
STEP12. Bitwise XOR the results of steps 3 and 9.
STEP13. Bitwise XOR the results of steps 2 and 10.
STEP14. Bitwise XOR the results of steps 4 and 10.

Encryption by RSA:
For encryption process of RSA, the cipher text of IDEA (T_1) acts as input. This data undergoes the encryption by RSA and gets converted into cipher text (T_2). The key which is used in this process is of 512-bit. The following flowchart describes the encryption process of RSA.

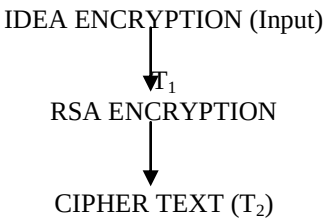

Fig.: Flowchart representing encryption by RSA

According to [7], key generation for RSA:-
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
Decryption by RSA:
For decryption process of RSA, the cipher text of RSA (T_2) acts as input. This data undergoes the decryption by RSA and gets converted into plain text (T_1). The key which is used in this process is of 512-bit. The following flowchart describes the decryption process of RSA.

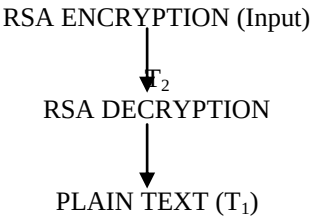

Fig.: Flowchart representing decryption by RSA

Decryption by IDEA:
For decryption process of IDEA the plain text of RSA (T_1) acts as input. This data undergoes the decryption by IDEA and gets converted into plain text (T). The key which is used in this process is of 128-bit. The following flowchart describes the decryption process of IDEA.

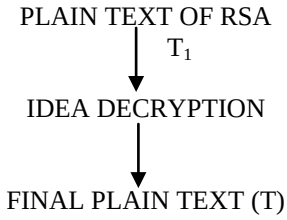

Fig.: Flowchart representing decryption by IDEA

IV. MERITS AND DEMERITS

Merits:
We have proposed such a crypto system which eliminates the weak key concept as we have introduced another bit of key length into this system. So, this provides enhancement in the security of IDEA.
Demerits:
There involves a bulky implementation of ES-IDEA as we are combining two ciphers. This requires extra efforts and time.

V. APPLICATIONS

- ES-IDEA can provide security to the receptive data.
- It can be used for the purposes of e-mails on public networks

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

- Smart card users can use this cipher.
- GSM technology finds great use of ES-IDEA.

VI. CONCLUSION

We have successfully enhanced the security of the data by combining two ciphers, IDEA and RSA. IDEA uses 128-bit key for encryption and decryption and this key is the same for both processes. RSA uses 512-bit key which is asymmetric in nature i.e. encryption process uses one key and decryption uses another key. This combination of ciphers leads us to increase in length of key which makes it 128-bit+512-bit key for ES-IDEA and enhance the security of data.

Future Scope:

In ES-IDEA we have combined two ciphers, i.e. IDEA cipher and RSA cipher. This has increased the key length up to 128-bit+512-bit. This increase in key length enhanced the security of the data. But the combination of ciphers has made it a bulky project which takes longer time and much effort. In future, such a system can be developed which may take less time and efforts.

REFERENCES

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