Design and implementation of Two Layer Encryption System in Cryptography

[1]Rejoy Chakraborty, [1]Arpan Bairagi, [2]Prof. Samir Kumar Bandyopadhyay

Department of Computer Science
Ramakrishna Mission Vivekananda Centenary College, Rahara, India
[2]GLA University, UP, India

***Abstract*: Network security has become a crucial part of the modern communication system. The security of data is crucial. In cryptography, we encrypt the data into an unreadable form. Though there are several strong encryption algorithms at present times, still we are searching for more secure encryption algorithm as 'Secure' is just a relative word. In this paper, a secure encryption algorithm has been proposed to ensure confidentiality of the information by hiding the key from attacker.**

***Keywords*: Cryptography, Encryption, Decryption, Security, Secret Key**

Introduction:

In the arena of digital technology, everyone is trying to secure his/her data in the virtual world as data's are so much valuable. So there are mainly two techniques to hide or secure a data i.e. Cryptography and Steganography. Cryptography is a technique defined in data security to ensure there that there is no unauthorized access to any unknown person (attacker) to get the original data [1]. In Steganography the messages are hidden within a media in such a way so that none can understand the very existence of the message i.e. it cannot be perceived by human [2]. In Cryptography data is encrypted in such a way that the data will be in unreadable form but the point to be noted. It is possible to suspect that in encrypted text there may be something hidden within it. Steganography hides the data from the attacker.

Cryptography has mainly two types: Symmetric Key Cryptography (also known as Private Key Cryptography) and Asymmetric Key Cryptography (also known as Public Key Cryptography). Nowadays, there is another type of cryptography i.e. "Quantum Cryptography". Researchers have been doing work in the field.

Symmetric Key Cryptography uses same key for encryption and decryption and that's why the key must be kept private. In Asymmetric Key Cryptography uses two different key where the encryption key is Public Key but the decryption key is Private Key. Examples of Symmetric Key Cryptography are DES, AES etc. & examples of Asymmetric Key Cryptography are RSA, Diffie Hellman etc.

Many cryptography algorithms are available but still researches are going on to make data more secret. The major problem of hiding the key from third party poses a threat to cyber security and thus requires further research. In this paper, a bit of more security is proposed to the key for encryption the plain text data.

Proposed Methodology:

Initially the normal encryption is applied. That means, encrypting a plain text using encryption algorithm which have 1 (or 2) key(s). As mentioned above, to secure the key, we shall encrypt the key also with another algorithm which will produce another key(s). Then the first key will be hidden and will be shared as an encrypted text whereas the second key will be the key of the whole process which must to be secret.

As, we encrypted the key after encrypting the plain text, we named this mechanism as "Two Layer Encryption System" as it performs two times encryption.

Proposed Method:

In below, we are mentioning the proposed encryption algorithm.

Input: Plain Text M, Encryption Algorithms Algo1 and Algo2, Key1 and Key2

Output: Cipher Text CM and Cipher Key CK

Step 1: Take the input of M.

Step 2: Encrypt M by Algo1 using Key1 which will produce CM.

Step 3: Encrypt Key1 by Algo2 using Key2 which will produce CK.

Step 4: Share CM and CK as the secret message and kept Key2 private (secure) as the key of the whole method.

Step 5: Stop Execution

Now, we are mentioning the proposed decryption algorithm.

Input: Cipher Text CM, Cipher Key CK and Key2

Output: Plain Text M and Key1

Step 1: Take the input of CM and CK.

Step 2: Decrypt CK by Algo2 using Key2 which will produce Key1.

Step 3: Decrypt CM by Algo1 using Key1 which will produce M.

Step 4: Stop Execution

Implementation:

For a demonstration, we have chosen "RSA algorithm" [3] for encryption of the plain text. And for encrypting the Private Key of RSA we are using the simplest "Ceaser Cipher" [4]. In below, we are giving Python Code including Results

I> ***Python Code:-***

```
from decimal import Decimal

def gcd(a,b):
    if b==0:
        return a
    else:
        return gcd(b,a%b)
p = int(input('Enter the value of p = '))
q = int(input('Enter the value of q = '))
no = int(input('Enter the value of text (Data to be encrypt) = '))
n = p*q
t = (p-1)*(q-1)
for e in range(2,t):
    if gcd(e,t)== 1:
        break
for i in range(1,10):
    x = 1 + i*t
    if x % e == 0:
        d = int(x/e)
        break
ct = Decimal(0)
ct =(pow(no,e))%n   #Encryption
```

```
print('n = '+str(n))

print('t = ' + str(e))

print('Private key (d) = ' + str(e))

print('Public key (e) = ' + str(d))

print('Cipher Text = ' + str(ct))

r = int(input('Enter the rotation value of Ceaser Cipher: '))

d = d+r #Encryption of the Private Key of RSA

print("Encrypted Private Key of RSA =  " + str(d))

print("New Private key of the whole process = " + str(r))

d = d-r

dt = Decimal(0)

dt = (pow(ct,d))%n   #Decryption

print('Decrypted Text = ' + str(dt))
```

II> ***<u>Results (Outputs):-</u>***

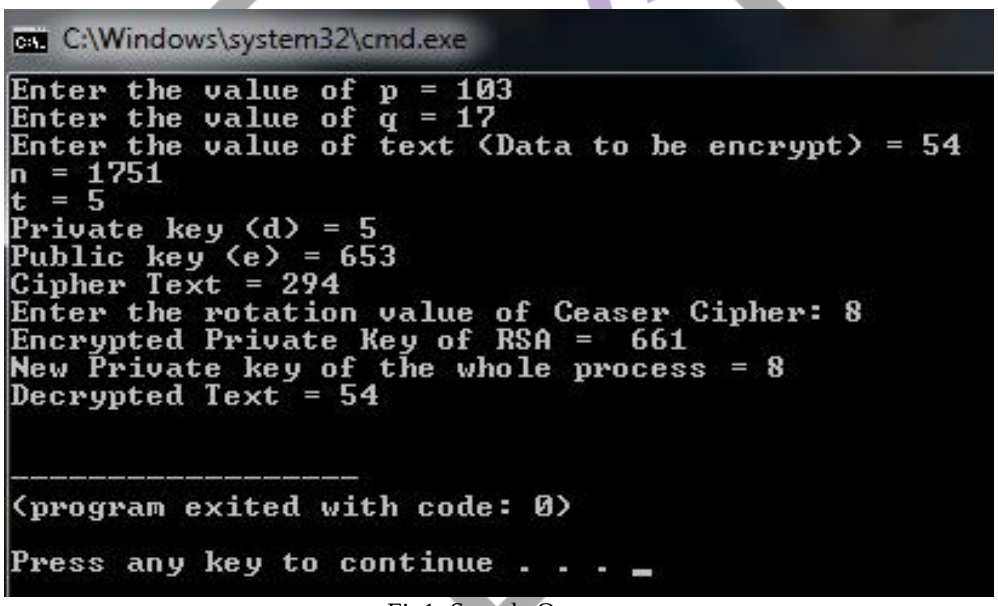

Fig1: Sample Output

Conclusion:

In this paper, we designed and implemented two-layer encryption system by encrypting the key also with another encryption algorithm. It may confuse attacker about the knowledge of actual key and decryption algorithm.

References:

[1] Ahmad, J. I., Din, R., & Ahmad, M. (2018). Analysis Review on Public Key Cryptography Algorithms. *International Journal of Electrical and Computer Engineering (IJECE)*, *12*(2), 447-454.

[2] Chowdhury, R., Bhattacharyya, D., Bandyopadhyay, S. K., & Kim, T. H. (2016). A view on LSB based audio steganography. *International Journal of Security and Its Applications*, *10*(2), 51-62.

[3] R L Rivest, A Shamir and L Adlernan, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications ACM Vol. 21 (2) (Feb 1978).

[4] Michael T. Goodrich and Roberto Tamassi, "Data Structures & Algorithms using Java",6th Edition, WILEY.