



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5

Issue: V

Month of publication: May 2017

DOI:

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Text Encryption and Decryption using Triple Keys Symmetric Cryptography

Ritu¹, Girija Srikanth²

¹M.Tech Scholar, ²Assistant Professor, Dept. of CSE, BSAITM, Faridabad, India

Abstract: Interchange of information over the network is increasing very rapidly. Transferring any information on internet arises with the biggest issue that is security. Surety must be provided at any cost. Cryptography plays an important role in achieving security. For any type of business our primary focus is mainly on the security of information for that we require a robust and unbreakable process that provides great safety. When we transmit sensitive information over an insecure medium then various types of attacks like Brute force and Cryptanalytic attacks are possible in which message and key can be recovered. In recent years, many encryption technologies have taken advancements to secure the information that is transmitted over the network. In this paper, we proposed an algorithm, which uses triple keys for encryption and decryption of text to secure the information.

Keywords: ASCII value, Inverse key, Encryption, Authentication, Cryptography, Triple Keys, EEA.

I. INTRODUCTION

We are living in the information age. We need to keep information about every aspect of our life. In other words, information is a possession that needs to be secure from attacks. To be secured, information needs to be hidden from unauthorized access, protected from unauthorized change, and available to an authorized entity when it is needed. To provide security some security mechanism must be implemented. Cryptography, a word with Greek origin means “secret writing”. Cryptography is a technique that is associated with scrambling plaintext (ordinary text, also known as cleartext) into ciphertext (a process called encryption), then back again (known as decryption) into the original form i.e. plaintext. Encryption and Decryption are the synonyms of cryptography. Encryption converts plaintext into ciphertext and decryption performs reverse operation. There are mainly two categories of cryptography named as Symmetric key cryptography and asymmetric key cryptography. Symmetric key exercises similar key for encryption and decryption whereas asymmetric key exercises dissimilar or separate keys. The aim of cryptography is to achieve confidentiality, integrity, authenticity, non-repudiation. This paper presents a powerful encryption and decryption approach that uses triple keys for text protection against Brute force and cryptanalytic attacks. The whole architecture of this paper is organized as: section 1 includes introduction about cryptography. The literature survey is described in section 2. Section 3 describe the problem definition. Proposed technique is described in section 4. The practical implementation is carried out in section 5. The work is concluded with conclusion and future work in section 6.

II. LITERATURE SURVEY

S.No.	Paper Title	Author	Analysis	Findings
1.	A survey on cryptography techniques	Vikrant M.Adki, Shubhanand S.Hatkar	This paper includes a comparison of mostly used symmetric algorithms based on performance.	This paper shows the performance analysis of DES, 3DES, AES and BlowFish algorithms and above result demonstrate that BlowFish has higher performance regarding encryption and decryption time.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

2.	Text encryption and decryption with EEA combining with Linear Congruence Generator	Solanki Pattanayak, Dipankar Dey	This paper gives an algorithm which was designed for text encryption and decryption with the help of Extended Euclidean Algorithm combining the features of Linear Congruence Generator.	The proposed algorithm is encrypting the text which can be used for further research in cryptography. This method is so easy but third party cannot hack this algorithm.
3.	A new approach for complex encrypting and decrypting data	Obaida Mohammad Awad Al-Hazaimeh	The proposed algorithm is based on parallel programming to achieve higher speed with higher level of security. The proposed algorithm consists of combination of Public key infrastructure for hybrid system and RC6 algorithm. The speed of the algorithm can be characterized by measuring the time required for encryption and decryption.	The result of this paper shows that the proposed algorithm has less average time as compared to AES.
4.	An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks	Abhishek Joshi, Mohammad Wazid, R.H Goudar	This paper presents an efficient encryption and decryption technique. The proposed technique focus mainly on reducing the length of encrypted message hence increasing the complexity of decryption performed by the attacker.	The proposed algorithm will have no effect of Brute Force and Cryptanalytic attacks. The algorithm proposed will take lesser time compared to existing algorithms.
5.	An Efficient Symmetric Cipher Algorithm for Data Encryption	Prosper kandabongee yeng, joseph kobinapanford, james Bens Hayfron-Acquah, Frimpong Twum	This paper presents an efficient algorithm for a symmetric cipher named "YC1" that employs key space of varying length to encrypt and decrypt a plaintext.	A symmetric key algorithm is presented in this paper and simulation results indicate that the new algorithm, YC1, is good in terms of security and performance.

III. PROBLEM DEFINITION

The current algorithm is having less effect on keys; as the new key is generated and transferred for every message. In spite of transferring a key for every message sent, still message length remains as of original size. That is the reason, the proposed work is proceeding with triple keys in order to achieve the secure communication.

IV. PROPOSED WORK

In this proposed technique, we focus mainly on providing security to the information from an unauthorized user by using triple key authentication algorithm. The algorithm uses triple keys i.e. k_1 , k_2 , k_3 . The key k_1 is generated from the message and also transferred along with the message. The cipher text obtained after applying encryption using key1 is considered as plaintext for the rest of the two keys. The PTK1 (plain text using k_1) is now encrypted with the help of two keys (k_2 , k_3) in order to obtain the final cipher text i.e. CT. In decryption the reverse operation is performed, the CT is decrypted with the help of two keys (k_2 , k_3) to obtain the PTK1. Thereafter PTK1 is decrypted using key 1 to obtain the final output which is the plaintext.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A. Enhanced Cryptographic Algorithm

The algorithm follows procedure

1) Encryption:

a) *Step 1:* Enter the plain text from the user.

Add the ASCII value of plain text starting from first alphabet with last alphabet i.e. moving right from first and left from last. If message is of odd length, then write the ASCII value of middle alphabet as it is.

b) *Step 2:* Store these values in an array and take modulus of these values from 26 i.e. (%26) and store the result in another array.

c) *Step 3:* To obtain the value of PTK1 i.e. (plain text encrypted with the help of key1) we perform the following steps:

Add the ASCII value of first half of message with the values stored in Array 2.

Now perform further calculations i.e. values obtained in step 1 – key1-ASCII value of first half of the message.

d) *Step 4:* Now PTK1 is considered as plaintext for rest of the two keys (K2, K3) in order to achieve triple keys algorithm.

e) *Step 5:* By entering encryption keys (K2, K3) from the user, encrypt the

PTK1 using the given formulae,

$$CT = ((PTK1 * K2) + K3) \text{ mod } 26$$

f) *Step 6:* Thus the CT (Cipher text) is obtained using the above formulae.

2) Decryption:

a) *Step 1:* Before proceeding the decryption, perform an algorithm for calculating modulo inverse of a number (MODINV), MODINV is used to calculate the inverse of K2 (one of the encryption key).

This algorithm is performed using Extended Euclidean Algorithm (EEA); EEA is explained at step 6.

Now K2 is given to EEA to get the output as INVK2.

b) *Step 2:* Decryption is done by using Ciphertext, (INVK2, and K3) pair.

For getting the plaintext, apply the formulae $PTK1 = (INVK2 (Ct - K3)) \text{ mod } 26$

Store the ASCII value of PTK1 in an array.

c) *Step 3:* Add the ASCII value of First + K1 + $(n/2 + 1)^{\text{th}}$ positions elements and perform this operation in right direction to obtain the array 3.

d) *Step 4:* Array 4 is equal to ASCII value of alphabets of Array 2 from position first to $n/2^{\text{th}}$ position - Array 3 mod 26.

e) *Step 5:* Array 5 can be computed by the expansion of Array 4. Fill the ASCII value up to $n/2^{\text{th}}$ position as it is. Calculate the remaining values of the message by n^{th} element of Array 3 - n^{th} element of Array 4 and store it in $(n/2 + 1)^{\text{th}}$ the position of Array 5 and so on.

f) *Step 6: EEA:* The Extended Euclidean Algorithm is used to calculate the modular multiplicative inverse of an integer a modulo m. The Euclidean Algorithm determines the greatest common divisor (gcd) of two integers say, a and m. If a has a multiplicative inverse modulo m, this gcd must be 1. The algorithm of EEA is described below.

```
r1 ← a; r2 ← b;
t1 ← 0; t2 ← 1;
while (r2 > 0)
{
q ← r1/r2;
r ← r1 - q*r2;
r1 ← r2;
r2 ← r;
t ← t1 - q*t2;
t1 ← t2;
t2 ← t;
}
gcd(a, b) ← r1; t ← t1
```

g) The EEA Algorithm:

Step 7: By doing all above steps, we will get back the Plaintext or original message.

3) Example:

a) Encryption:

STEP 1:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enter the plain text from the user. Say "Symmetry" for this example.

Array 1:

S+y=204	y+r=235	m+t=225	m+e=210
---------	---------	---------	---------

STEP 2: Array 2= Array 1%26

22	1	17	2
----	---	----	---

STEP 3: To obtain the value of PTK1 the steps are as follows.

PTK1= Add ASCII value of first half of message with the values stored in Array 2. Remaining values are calculated by (values stored in Array 1 – key 1 – right half of values obtained for PTK1)

105	122	100	111
-----	-----	-----	-----

83	97	109	83
----	----	-----	----

STEP 4: PTK1= value obtained by performing encryption to the plaintext with the help of key1. PTK1 is considered as plaintext for the rest of the two keys in order to achieve triple key algorithm.

PTK1= "izdoSamS"

STEP 5: Enter the encryption keys (k2, k3) from the user. Now the ciphertext is obtained by using the formulae

CT= ((PTK1* K2) +K3) mod 26

104	119	121	120	80	100	106	80
-----	-----	-----	-----	----	-----	-----	----

H	w	y	x	P	d	J	P
---	---	---	---	---	---	---	---

STEP 6:

CT= "hwyxPdJp"

b) Decryption:

STEP 1: Before proceeding the decryption process, we perform an algorithm for calculating the module inverse of K2 i.e. one of the encryption key. This algorithm is performed using EEA (Extended Euclidean Algorithm)

INVK2= MODINVK2 by using EEA.

STEP 2:

Decryption is done by using following pair

(CT, INVK2, K3) to get the PTK1.

For getting PTK1 apply the formulae

PTK1= (INVK2 (Ct-K3)) mod 26

After applying the formulae, the value of PTK1 is obtained and store in an array.

Array 1:

105	122	100	111	83	97	109	83
-----	-----	-----	-----	----	----	-----	----

I	z	d	o	S	a	M	S
---	---	---	---	---	---	---	---

PTK1= "izdoSamS"

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Array 2= ASCII value of PTK1 stored in array 1.

105	122	100	111
83	97	109	83

STEP 3: Array 3= Add ASCII values of $(1^{st} \text{ to } n/2)^{th} + K1 + (n/2+1)^{th}$ in right direction and so on.

204	235	225	210
-----	-----	-----	-----

STEP 4: Array 4: ASCII value of alphabets of Array 2 from first to $n/2$ position – Array 3 mod 26

83	121	109	109
----	-----	-----	-----

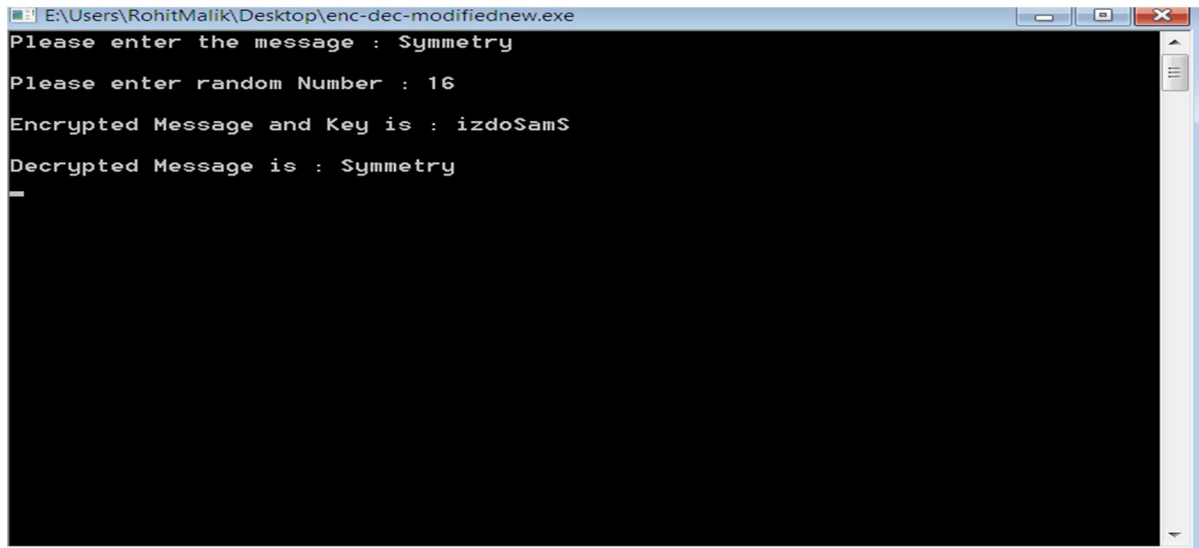
STEP 5: Array 5: Array 5 can be computed by the expansion of Array 4. Place the ASCII value up to $n/2^{th}$ position as it is. Remaining values are calculated by n^{th} element of Array 3 – n^{th} element of Array 4 and store these values in $n/2+1^{th}$ position of array 5 and so on.

83	121	109	109
101	116	114	121

Hence by doing all above steps we are able to achieve the plaintext which is entered by the user i.e. “Symmetry”..

V. PRACTICAL IMPLEMENTATION

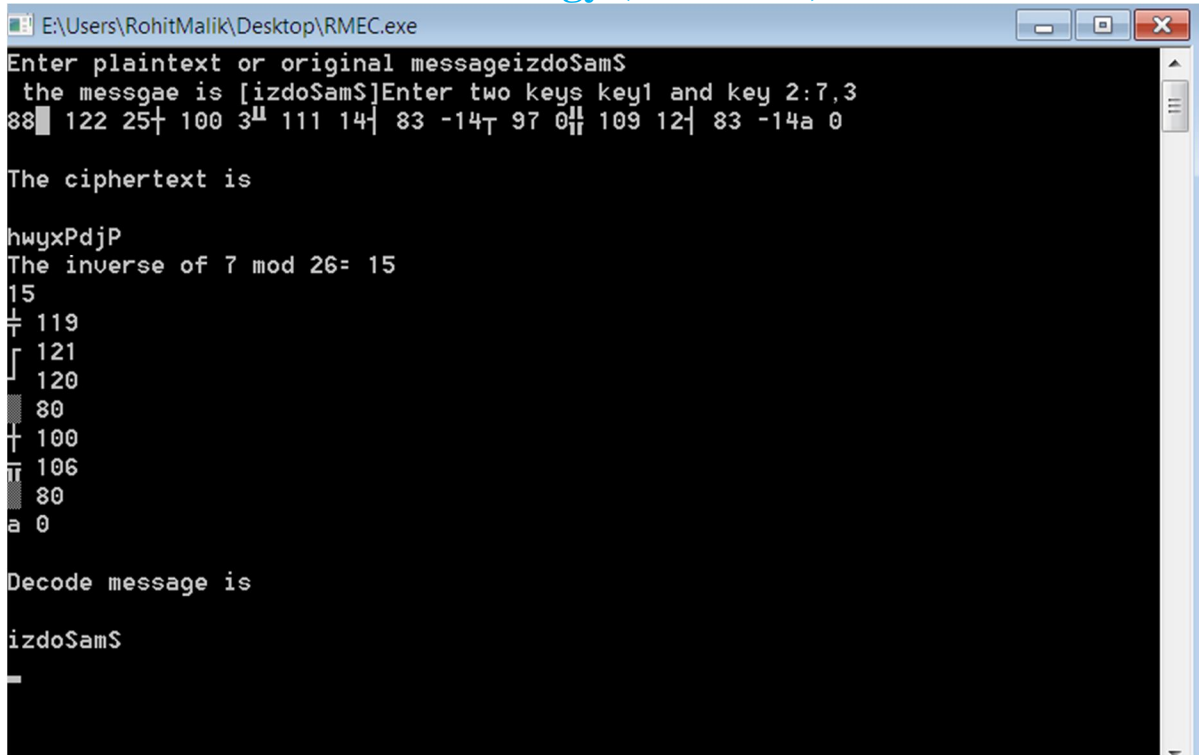
We have implemented the proposed encryption decryption algorithm by the help of a C/C++ program. Program automatically performs the encryption and decryption operations within few milliseconds.



```
E:\Users\RohitMalik\Desktop\enc-dec-modifiednew.exe
Please enter the message : Symmetry
Please enter random Number : 16
Encrypted Message and Key is : izdoSamS
Decrypted Message is : Symmetry
```

Fig 1. C++ console screen showing plain text as “Symmetry” entered by the user, producing izdoSamS as encrypted message and key, further producing “Symmetry as output.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)



```
E:\Users\RohitMalik\Desktop\RMEC.exe
Enter plaintext or original messageizdoSamS
the messgae is [izdoSamS]Enter two keys key1 and key 2:7,3
88 122 25 100 3 111 14 83 -14 97 0 109 12 83 -14a 0

The ciphertext is
hwyxPdJp
The inverse of 7 mod 26= 15
15
t 119
r 121
l 120
s 80
t 100
r 106
l 80
a 0

Decode message is
izdoSamS
```

Fig 2. C++ console screen taking above encrypted message and key as plaintext and producing the same as decoded message.

VI. CONCLUSION

A symmetric key algorithm is presented in this paper. This algorithm provides security of transmitted message by making use of triple keys and the simulation results are shown in the paper which shows that the new algorithm is good in terms of security. Although it has some weakness just like other algorithms do. In future we concentrate on more security with less time and less power consumption and also including the schemes and techniques over different data types such as sound, video and rising a stronger encryption algorithm with high speed and minimum energy consumption.

REFERENCES

- [1] Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings.
- [2] Atul kahate "Cryptography and Network Security", tata McGraw-Hill Companies, 2008
- [3] Vikrant M.Adki, Prof.. Shubhanand S.Hatkar,"A Survey on Cyptograjhic Techniques"International Journal of Advanced Research in Computer Science and Softwaew Engineering. Volume 6, Issue 6, June 2016, ISSN:2277128X
- [4] Solanki Patnayak and Dipankar Dey,"Text Encryption and Decryption with Extended Euclidean Algorithm and Combining the Features of Linear Congruence Generator", International journal of Development Research, Vol. 06, Issue, 07, July 2016, ISSN:2230-9926.
- [5] Obaida Mohammad Awad Al-Hazaimeh,"A New Approach For Complex Encrypting And Decrypting Data", International Journal of Computer Network & Communications(IJCNC) Vol 5, No 2, March 2013
- [6] Abhishek Joshi, Mohammad Wazid, R.H Goudar,"An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks", International Conference on Intelligent Computing, Communication & Convergence(ICCC-2015)
- [7] Prosper Kandabongee Yeng, Joseph KobinaPanford, James Ben Hayfron-Acquah, Frimpong Twum,"An Efficient Symmetric Cipher Algorithm for Data Encryption", International Research Journal of Engineering and Technology(IRJET), Vol 03,Issue:05, May 2016
- [8] Karthik, S, Muruganadam. A,"Data Encryption and Decryption by using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER), Vol 2, Issue 11, November 2014
- [9] Om Prakash Verma, Ritu Agarwal, Dhirai Dafouti,Shobha Tyagi, "Peformance analysi of data encryption algorithms", 3rd IEEE International Conference on Electronics Computer Technology (ICECT), 2011.
- [10] Cryptography and Network Security by Behrouz A. Forouzan .



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)