# A NOVEL APPROACH TO PROVIDE SECURITY OVER MAILING SYSTEM USING CRYPTOGRAPHY

**Deepti Mittal[1], Mannu Khariwal[2],MeenaKumar[3]**

*[1,3] Assistant Professor , Department of Computer Applications, DIRD(GGSIPU), Delhi,(India)*

*[2]Director,Unnati Web Services, Jaipur,(India)*

## ABSTRACT

*Abstract- Security is the main aspect of any field, organization, company as well as to secure email data. Cryptography is one of the techniques which is used to secure the data over a network .It consists of two types asymmetric cryptography and symmetric cryptography. Using encryption and decryption algorithm we are having different types of algorithms of cryptography. Here we are proposing a cryptography algorithm which is hybrid in nature which is complex as well as cost effective. The main concern of cryptography algorithm is to secure the key, registration of client as well as proper encryption and decryption process. Here we are proposing an algorithm to provide the security over mailing system. The algorithm designed will have the following features: 1. it is cost effective in nature and provides security to email data.2. It is hybrid in nature so it is more complex.3. It is efficient as well as best for small organization.*

***Keywords: Cryptography, Hybrid Approach, Secret Key, Encryption, Decryption, ASCII, Cipher Text, Plaintext***

## I INTRODUCTION

Cryptography is a process which is associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. One of which is secret key cryptography, in which a single key is used for both encryption and decryption. Another one is public key cryptography or asymmetric key cryptography which involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. [1]

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the data which has sent to the receiver from the sender. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. It has been found that the algorithms which are available at this moment are more difficult or less complex in nature, and of-course it is quite obvious.

For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work is to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. Keeping this

goal in mind the proposed algorithm has been designed in a quite simple manner but of course not sacrificing the security issues.

## II PROPOSED ALGORITHM

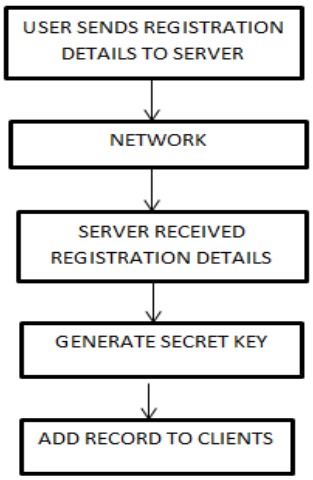
We proposed a hybrid approach of cryptography algorithm which helps in securing mailing system over a network .In this algorithm cost is main aspect which is taken care .it is cost effective in nature and very simple. The approach consists of registration of client, secret key generation, and encryption and decryption process.

There will be mail application server and mail application client is there. Here this proposed algorithm is a mixture of two algorithms which is based on ASCII based cryptography

**PROTOTYPE:**

### ALGORITHM 1

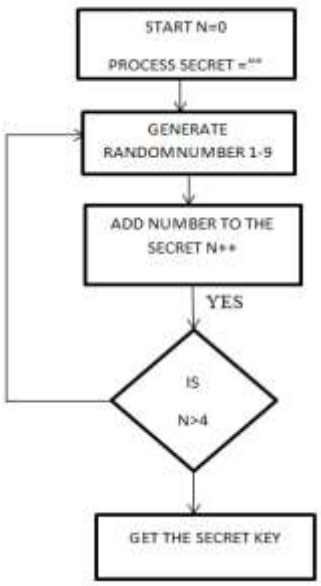
1. User sends registration details to server.
2. It will reach to the network.
3. Server received required details.
4. Generate secret key.
5. Add record to clients.




*A. Flowchart for Registration of Client*

### ALGORITHM 2

1. Start process n=0 secret =””;
2. Generate random number from 1-9.
3. Add number to the secret n++.
4. If n>4 then
5. Get the secret key otherwise
6. Go to step 2.

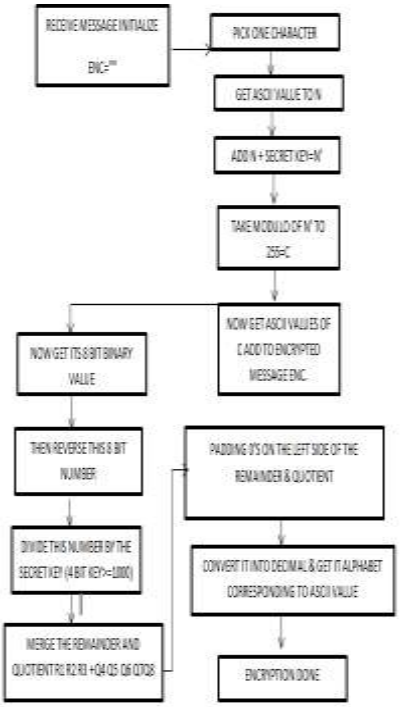



*B. Flowchart for Secret Key Generation*

### ALGORITHM 3

1. Initialize receive message ENC=””.
2. Pick one character.
3. Get ASCII value to n.
4. Add n+ secret key=n’.
5. Take modulo of n’ to 255=c.

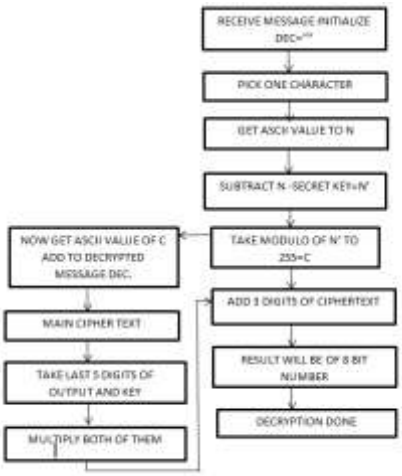
6. Now get ASCII value of c add to encrypted message enc.
7. Generate the ASCII value of the alphabet.
8. Generate the corresponding binary value of it.
9. Reverse the 8 digit's binary number
10. Take a 4 digits divisor (>=1000) as the Key
11. Divide the reversed number with the divisor.
12. Store the remainder in first 3 digits & quotient in next 5 digits. If any of these are less than 3 and 5 digits then we need to add padding 0s (zeros) in the left hand side. Output will get.




## ALGORITHM 4

*C. Flowchart for Encryption Process*

1. Initialize receives message DEC="".
2. Pick one character.
3. Get ASCII value to n.
4. Subtract n-secret key=n'.
5. Take modulo of n' to 255=c.
6. Now get ASCII value of c add to encrypted message enc.
7. Multiply last 5 digits of the cipher text by the Key
8. Add first 3 digits of the cipher text with the result Produced in the previous step.
9. If the result produced in the previous step i.e. step2 is not an 8-bit number we need to make it an 8-bit number.
10. Reverse the number to get the original text i.e. the plain text.




*D.Flowchart for Decryption Process*

## III ADVANTAGES OF THE PROPOSED ALGORITHM

1. The Algorithm is very simple in nature.
2. It works best for a small organization because it is cost effective.
3. For a small amount of data this algorithm will work very smoothly.
4. This algorithm is a hybrid approach which is more complex and effective in nature.

## IV IMPLEMENTATION

Here for the implementation of this algorithm Java is used. Java is a general-purpose, object-oriented language that is specifically designed so that few implementation dependencies may occur. JAVA is used mainly for client server applications. Java platform and Netbeans are used to implement the algorithm.

## V CONCLUSION AND FUTURE WORK

This algorithm provides security to mailing system and its data. This algorithm will be helpful in securing the private and confidential data of email. This algorithm is hybrid in nature so it is complex and efficient. The prototype of the algorithm is difficult to decode. This is cost effective which makes it more valuable. Future work on this field is never ending till any loop hole is found in the algorithm.

## REFERENCES

[1] An Overview of Cryptography from http://www.garykessler.net/library/crypto.html

[2] Mohammad Zakir Hossain Sarker and Md. Shafiul Parvez Department of CSE, East West University, 43, Mohakhali, Dhaka-1212, Bangladesh ,"A Cost Cutting Symmetric Key Cryptographic Algorithm for Small Amount of Data."

[3] Dominic Bucerzan, Department of Mathematics and Computer Science "AurelVlaicu" University of Arad, Arad, Romania,"A Cryptographic Algorithm Based on a Pseudorandom Number Generator ".

[4] Victor Foo Siang Fook Systems and Security Department Institute for Infocomm Research, Singapore" AES Security Protocol Implementation for Automobile Remote Keyless System ".

[5] D. Bucerzan and M. Gheorghita, "Henkos a new stream cipher: Algorithmic aspects," in The 6th NATO Regional Conference on Military Communications and Information Systems, Zegrze, Poland, October 2004

[6] F. Hao, R. Anderson and J. Daugman, "Combining Crypto with Biometrics Effectively", *IEEE Transactions on Computers*, pp. 1081-1088, 2006

[7] ASCII Table Referred from http://www.asciitable.com/index/asciifull.gif

[8] Stallings W (2007),"Network Security and Cryptography, Pearson Education", New Delhi.

[9] Study On Evolutionary Computation Methods in Cryptography by Faculty of Electrical Engineering and Computing, Zagreb, Croatia Year 2009.

[10] Yusupov S.Yu, Medetov S.K. Tashkent University of Information Technologies" Application of biometric methods in cryptography", 2010.

[11] Hong Tang Chongqing University of Posts and Telecommunications, Chongqing 400065, China tanghong@cqupt.edu.cn,"A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key."

[12] Information about eclipse http://www.eclipse.org/jdt/overview.php

[13] Rail Fence Encoder http://www.math.temple.edu/~renault/cryptology/railfence.html

[14] Noel McCullagh ,"Securing E-Mail with Identity-Based Encryption ".

[15] Daniel A. Menascé ,George Mason University , menasce@cs.gmu.edu "Security Performance".