

# RANDOM KEY & THE NTH PRIME NUMBER BASED SYMMETRIC KEY ENCRYPTION ALGORITHM

**Mrs Mukta Sharma<sup>1</sup>, Dr. R B Garg<sup>2</sup>,**

<sup>1</sup>*Department of Computer Science, Research Scholar, TMU, Moradabad (India)*

<sup>2</sup>*Ex-Professor, Department of Computer Science, Delhi University, Delhi (India)*

## ABSTRACT

*The Online Banking Service is used extensively across the globe. Implementing security features for those networks are very critical as the communication is done via an insecure channel i.e. Internet. So there are more requirements to secure the data transmitted over different networks using different services. Different encryption methods are used to provide the security to the network and data. Encryption is the process of changing plain readable text into unreadable cipher text. Cryptographic algorithms play a vital role in the field of network security. There are two basic types of cryptosystems such as symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems are characterized by the fact that the same key is used in encryption and decryption transformations. Asymmetric cryptosystems use complementary pairs of keys for encryption and decryption transformations. One key, the private key is kept secret like the secret key in a symmetric cryptosystem. The other key, the public key, does not need to be kept secret [1]. This paper focuses on designing an encryption algorithm to secure the online transactions. As many users are a continually growing financial service of electronic commerce, Internet banking requires the development & implementation of a sound security algorithm.*

**Keywords:** *Cryptography, Symmetric & Asymmetric Cryptography, Plain Text, Cipher Text*

## I. INTRODUCTION

For the first few decades, internet was primarily used by military & university. Now millions of users are using internet today for a large variety of commercial and non-commercial purposes. Therefore, it is essential to secure the internet from various threats, spywares, malwares, hackers, phishers etc. Internet security is not about protecting hardware or the physical environment. It is about protecting information [1]. Ensuring the security is a serious business on which various researches are going on. One way to secure transmission is to use cryptography.

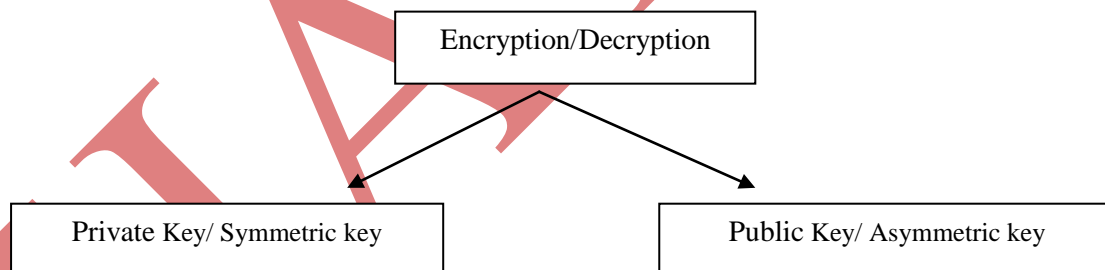
Cryptography has been derived from two Greek words Crypto (Secret) & Graphs (Writing) which means “Secret Writing”. Cryptography allows secure transmission of private information over insecure channels. It is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form. It is the mathematical “scrambling” of data so that only someone with the necessary key can “unscramble” it.

### 1.1. Characteristics of Cryptography

1. **AUTHENTICITY:** Is the sender (either client or server) of a message who they claim to be?
2. **PRIVACY:** Are the contents of a message secret and only known to the sender and receiver?
3. **INTEGRITY:** Have the contents of a message been modified during transmission?
4. **NON-REPUDIATION:** Can the sender of a message deny that they actually sent the message? It is the ability to limit parties from refuting that a legitimate transaction took place, usually by means of a signature.

### 1.2. Basic Terminology

- Plain text - the original message
- Cipher text - the coded message
- Cipher - algorithm for transforming plaintext to cipher text
- Key - info used in cipher known only to sender/receiver
- Encipher (encrypt) - converting plaintext to cipher text
- Decipher (decrypt) - recovering cipher text from plaintext
- Cryptography - study of encryption principles/methods
- Cryptanalysis is (code breaking) - the study of principles/ methods of deciphering cipher text without knowing key
- Cryptology - the field of both cryptography and Cryptanalysis



**Fig. 1: Type of Keys**

Secret key or Symmetric key- In this sender and receiver possess the same single key. It can be divided into stream ciphers and block ciphers. Stream cipher encrypts a single bit of plain text at a time, whereas block cipher encrypts a number of bits as a single unit.

Public key or Asymmetric key- Involves two related keys called a key-pair: one public key known to anyone and one private key that only the owner knows.

## II. THE GROUND WORK

Beginner's view about the algorithm was to make some use of the ASCII numbers & the Prime numbers. Considering a character as plain text & n as ASCII Value of character the Cipher Text can be nth Prime Number. But this had big flaw of no Key being used. So, easiest to decrypt. Certainly some key was to be used. Then different approaches were taken before finalizing the Key for the process.

Considering a complete String coming as a Plain Text.

### Approach – I - Minimum Value

Take ASCII values of characters in string.

Find the Minimum of them.

Key = Minimum Value.

### Flaws-

In a large text, zero has the highest probability of coming out as minimum value.

Same key will generate same cipher text every time.

Space Complexity of an array.

### Approach - II - Mid-Value

Take ASCII values of characters in string.

Sort the array.

Find the Mid value of them.

Key = Mid-Value.

Flaws- Two different users interacting with the system will have same key for same string being entered.

Example

User A -> Plain Text = "User". Cipher Text = 1234.

User B -> Plain Text = "User". Cipher Text = 1234.

However, for being more secure both should have different cipher text.

### Approach - III – Random Number

Random Number

Key = Absolute Value of Random Number.

This Approach was able to resolve the issues discussed in previous two approaches.

For any analysis purpose, it was necessary to observe the values of the variables with respect to reference variables and henceforth, the variables were correlated using repeating variable method (Edward, 2005). As mentioned above, total number of variables considered for present investigation, '6'. Three out of 6 variables were considered as fundamental variables and a functional relationship was established as  $\Phi(V, W, D, F, B, G)$

= 0. The derived groups were,  $V/(D^2.F)$ ,  $B/D$  and  $G/(D^2.F)$ . The relationship obtaining using Buckingham Pi Theorem as,  $G/(D^2.F) = f(B/D, V/D^2F)$ . Crack growth rate for specimen at fixing length 400 mm, 350 mm and 300 mm were calculated at frequency of 60 Hz, 80 Hz, 100 Hz and 120 Hz. Calculated value of 'G' were further calculated and plotted for useful analysis.

### III. PROPOSED ENCRYPTION ALGORITHM

The algorithm has two main steps:

Step One: Generate a Key.

- Generate A Random Number. (16 bits)
- Get Absolute Value of the Number generated

Key = Abs (RandomNo.)

So, the Algorithm is generating a 32 bits key for a plain text of 16 bits.

Step Two: Generate Cipher text using the Key, Prime No & the Plain Text.

Initialize nthPrime as ascii value of character of plain text & Cipher text as 0

The Objective is to find the nth Prime Number after the "Key".

For Example: Key generated is "4"

character entered is Space i.e. "A"

The ASCII Value = 65.

i.e. We need to find 65th Prime Number after 4.

Obtained Value: 331, which is a 32nd Prime Number post 4.

Add Constant to the Obtained value to give a Cipher Text. Constant can be the last 2 digits of the Key.

Pictorial Representation of Encryption Algorithm

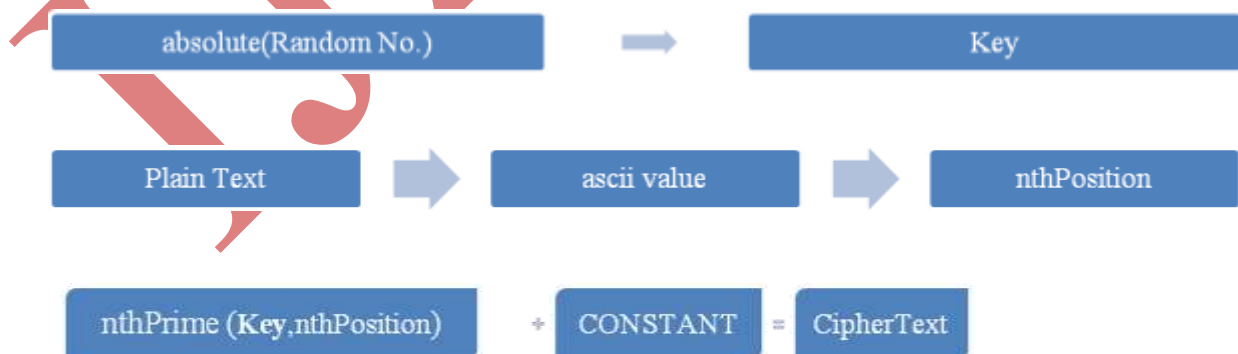


Fig. 2: Conversion of Plain Text to Cipher Text

Note: As we go higher in numbers the Prime Numbers turn sparse. The notion to add a Constant to the obtained prime number is to offer a larger set of Natural Numbers.

Key(Random No.)	Plain Text	Ascii value	nthPrime post Key	Add Constant (Eg. 2)	Cipher Text
4	A	65	331	333	333

**Table1: Encryption Table**

Pseudo Code for Step Two:

```

SET nthprime=0
SET Key=RandomNumber
GET Key = DETERMINE(AbsoluteValue(Key))
INIT Ciphertext =0
READ plaintext
FOR 1 to sizeof(plaintext)
SET nthVal = ascii(plaintext[i])
SET P=Key, count = 0
FOR P to count!=nthVal
SET status=1
IF P==2
nthprime=i
count++
ELSE IF P%2==0
nthprime=0
ELSE
    FOR j = 3 j <= Math.sqrt(i) j+=2
    IF P%j == 0
    status = 0;
    BREAK
    IF status != 0
    nthprime=i;
    count++;
    status = 1;
    FOREND
retStr.ADD(nthprime);
FOREND
Ciphertext = nthPrime+ Constant
    
```

#### IV. DECRYPTION ALGORITHM

##### Steps

- Obtain the Key.
- Read the Cipher Text.
- Subtract the CONSTANT from the Cipher Text. Obtain the value which is nth prime number post Key.
- The Decryption algorithm executes till the time it is able to generate the same nthPrime Number as obtained in step (iii). Keep a counter of it.
- Counter gives the ascii value.
- Get character from the obtained ascii value.

PlainText = Character.toString((char) counter(CipherTxt – CONSTANT ))



Fig. 3: Conversion of Cipher Text to Plain Text

Key (Random No)	Cipher Text	Nth Prime Post Key (Subtracted 2)	Counter	Plain Text
4	333	331	65	A

Table2: Decryption Table

Pseudo Code:

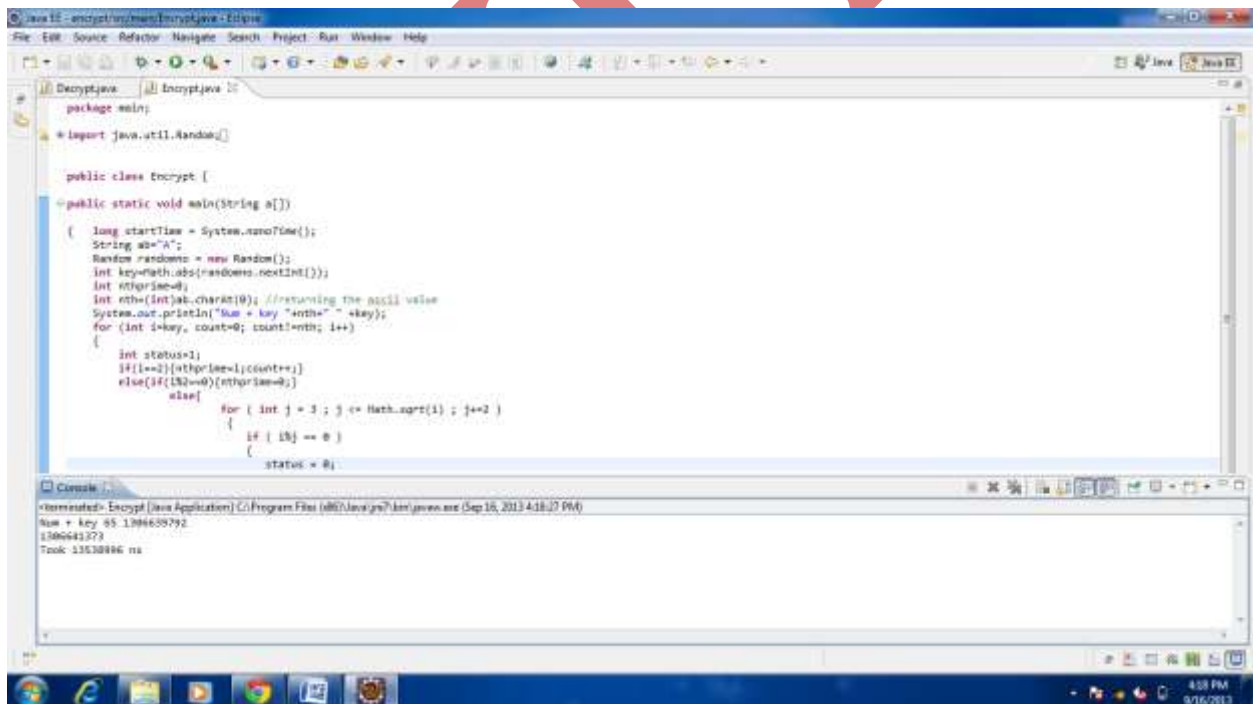
```

    READ cipher
    INIT i=0;
    INIT count;
    INIT nthprime=0;
    FOR SET i=key, count=0 nthprime!=cipher
        INIT status=1
        IF(i==2)nthprime=i
        count++
        ELSEIF i%2==0
    
```

```
nthprime=0  
ELSE  
FOR SET j = 3 , j <= Math.sqrt(i), j+=2  
IF i%j == 0  
status = 0  
BREAK  
FOREND  
IF status != 0  
    nthprime=i  
    count++  
status = 1
```

return plaintext.

Both the Algorithms are implemented in Eclipse IDE, Java 1.6 on Dell Laptop with Configuration: Intel Core i5 @2.60GHz 4GB RAM and 64 bit Windows 7 OS.

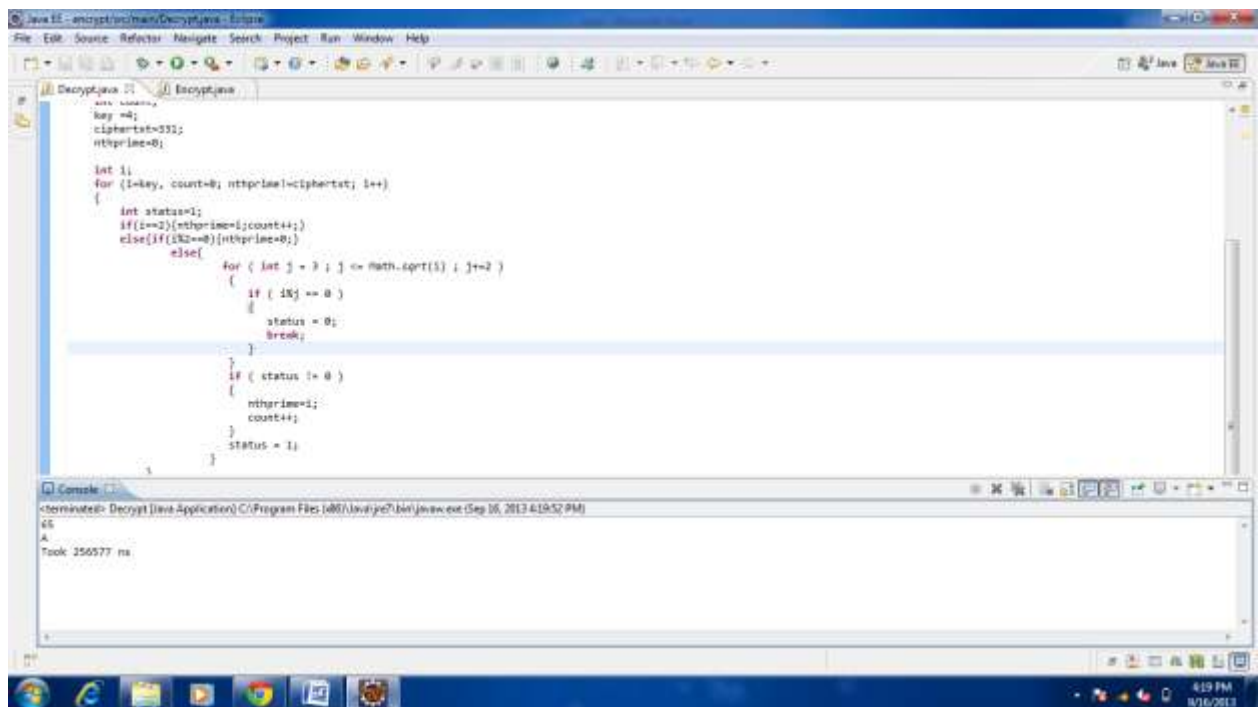


```
package main;  
  
import java.util.Random;  
  
public class Encrypt {  
  
    public static void main(String a[])  
    {  
        long startTime = System.nanoTime();  
        String ab="A";  
        Random randoms = new Random();  
        int key=Math.abs(randoms.nextInt());  
        int nthprime=0;  
        int nth=(int)ab.charAt(0); //returning the ascii value  
        System.out.println("Sum = key +nth=" +key);  
        for (int i=key, count=0; count<nth; i++)  
        {  
            int status=1;  
            if(i==2){nthprime=1;count++;}  
            else{if(i%2==0){nthprime=0;}  
            else{  
                for ( int j = 3 ; j <= Math.sqrt(i) ; j+=2 )  
                {  
                    if ( i%j == 0 )  
                    {  
                        status = 0;  
                    }  
                }  
            }  
        }  
    }  
}
```

Console

```
<terminated> Encrypt [Java Application] C:\Program Files (x86)\Java\jre7\bin\java.exe (Sep 16, 2013 4:18:27 PM)  
Sum = key 65 1306635792  
1306641373  
Trunk 13530886 na
```

Fig 4: Screen Shot of the Encryption Implementation Code



```
Decrypt.java 21 Encrypt.java
File Edit Source Refactor Navigate Search Project Run Window Help

Decrypt.java 21
    int key=4;
    ciphertext=331;
    ntpriime=0;

    int i;
    for (i=key, count=0; ntpriime<ciphertext; i++)
    {
        int status=1;
        if(i==2){ntpriime=i;count++;}
        else{if(i%2==0){ntpriime=0;}
            else{
                for ( int j = 3 ; j <= Math.sqrt(i) ; j+=2 )
                {
                    if ( i%j == 0 )
                    {
                        status = 0;
                        break;
                    }
                }
                if ( status != 0 )
                {
                    ntpriime=i;
                    count++;
                    status = 1;
                }
            }
        }
    }

Console
<terminated>: Decrypt [Java Application] C:/Program Files/Java/jre7/bin/javaw.exe (Sep 16, 2013 4:19:52 PM)
AS
A
Took 256577 ms
```

Fig. 5: Screen Shot of the Decryption Implementation Code

## V. CONCLUSION

The proposed algorithm implements a good strategy of making most out of the advantages of prime numbers and ASCII values. The Space complexity has also been dealt as an essential objective to be met in this algorithm.

In cryptography, key size or key length is the size measured in bits of the key used in a cryptographic algorithm (such as a cipher). An algorithm's key length is distinct from its cryptographic security, which is a logarithmic measure of the fastest known computational attack on the algorithm, also measured in bits. The security of an algorithm cannot exceed its key length (since any algorithm can be cracked by brute force), but it can be smaller. Most symmetric-key algorithms in common use are designed to have security equal to their key length.[3] The proposed algorithm is based on 32 bit key generation for a 16 bit plain text. Hence meeting the minimum requirement of the symmetric-key algorithm key generation factor.

## FUTURE SCOPE

In the future work related to proposed algorithm, the encrypting and decrypting data with least execution time. The concept of block wise parallel encryption using multithreading technique can enhance the speed of encryption system.



## REFERENCES

- [1] Bhati,S., Bhati,A.,Sharma K, S. (2012), A New Approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm, Proceedings of the World Congress on Engineering and Computer Science 2012 Vol II
- [2] Gupta, V.,Singh, G., Gupta, R. (2012), Advance cryptography algorithm for improving data security,
- [3] [http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption\\_perf/](http://www.cs.wustl.edu/~jain/cse567-06/ftp/encryption_perf/)
- [4] <http://www.eg.bucknell.edu/~xmeng/Course/CS6337/Note/master/node37.html>
- [5] [http://en.wikipedia.org/wiki/Cryptographically\\_secure\\_pseudorandom\\_number\\_generator](http://en.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator)
- [6] [http://en.wikipedia.org/wiki/Key\\_size](http://en.wikipedia.org/wiki/Key_size)
- [7] <http://www.randomnumbers.info/content/Random.htm>
- [8] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, issue 1, January 2012
- [9] Kannan Muthu, P., Asthana, A. (2012), Secured Encryption Algorithm for Two Factor Biometric Keys, International Journal of Latest Research in Science and Technology , Vol.1,Issue 2 ;Page No.102-105 ,July .August
- [10]Kumar, A., Jakhar, S., Makkar, S., (2012), Comparative Analysis between DES and RSA Algorithm's, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 7
- [11]Mathur, A.(2012), A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms, International Journal on Computer Science and Engineering (IJCSE), Vol 4, No.9
- [12]Verma,S., Choubey,R., Soni, R. (2012), Design and Implementation of New Encryption algorithm Based on Block Cipher Substitution Technique (Effect on Image file), International Journal of Computer Technology and Electronics Communication.
- [13]Chinchalkar, S., “Determination of Crack Location in Beams using Natural Frequencies”, Journal of Sound and Vibration Volume 247 (3), 2001, 417-429.
- [14]Batabyal, A. K., Sankar, P., and Paul, T. K., “Crack Detection in Cantilever Beam using Vibration Response”, ‘Vibration Problems ICOVP-2007’, Springer Netherlands, 2008, Pages 27-33.
- [15]Srinivasarao, D. Rao, K. M. and Raju, G.V., Crack identification on a beam by vibration measurement and wavelet analysis, International Journal of Engineering Science and Technology 2(5), 2010, 907-912 .
- [16]Zhong, S. and Oyadiji, S.O., Detection of cracks in simply-supported beams by continuous wavelet transform of reconstructed modal data, Computers and Structures 89, 2011, 127-148.
- [17]Jiang, X., John Ma, Z. and Ren W.X., Crack detection from the slop of the mode shape using complex continuous wavelet transform, Computer- Aided Civil and Infrastructure Engineering 27, 2012, 187-201
- [18]Ghadami, A. Maghsoodi, H. R. Mirdamadi, “A new adaptable multiple-crack detection algorithm in beam-like structures” Arch. Mech., Volume(65) 6, Warszawa 2013,1–15.

### Biographical Notes

**Mr. Md. Meraz** is presently pursuing M. Tech. final year in Mechanical Engineering Department (Specialization in Machine Design) from B.I.T Sindri, Dhanbad, India.

**Mr. J. N. Mahto** is working as a Assistant Professor in Mechanical Engineering Department, B.I.T Sindri, Dhanbad and presently pursuing Ph. D. from B.I.T sindri, Dhanbad, India.

**Dr. R. S. Prasad** is working as a Professor & Head in Mechanical Engineering Department, RKGIT, Ghaziabad, India.

**Dr. S. C. Roy** is working as a Professor & Head in Mechanical Engineering Department, B.I.T Sindri, Dhanbad, India.

**Mr Vivek Sagar** is presently pursuing M. Tech. final year in Mechanical Engineering Department (Specialization in Machine Design) from B.I.T Sindri, Dhanbad, India.

UJATES