TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 14997 - 15000

A Study on Encyrption Algorithm using Number theory in Cryptography.

[1]Rosa Mistica. J, [2]Rogith. A, [3]Anuabarna. S, [4]Sowbarnikaa. A
[1]PGScholar, [2] PG Scholar, [3] PG Scholar, [4] PG Scholar
Department of Mathematics with Big Data
Sri Krishna Arts and Science College
[1]kennedymistica@gmail.com, [2]rogith3pur@gmail.com , [3]anuabarnas@gmail.com
[4]sowbarnikaa2912@gmail.com

Article Info
Volume 82
Page Number: 14997 - 15000
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
"A Study on Encryption Algorithm using Number Theory in Cryptography" deals with data security using Number Theory in Cryptography. Data is a key factor in the field of Information Technology where Encryption can be an excellent choice for keeping the data safe from potential data theft. "Cryptography" is the method of secured information transfer by which no third party can access nor understand the message that sent. A mathematical procedure for performing encryption on data, is carried out by the use of an algorithm, where information is made into meaningless cipher text which requires the use of a key to transform the data back into its original form. The idea of encryption using Caesar Cipher and RSA public key cryptography is discussed in this paper. Mathematical concepts with prime, divisors, congruence and Euler's function are employed in cryptography for guarding data.

I. INTRODUCTION

In the modern world, people were trying to transmit the highly secured information in a pre-defined methodology. As of a tale in olden days, a ruler was in need for transmitting messages to the war generals who were in the battles. This was done with the violent idea of sending a servant with a message in his head which would be read by the general by shaving the servant's head. Even if the opposition party captures the servant, they won't be knowing where the message is. And hence the messages were transmitted in this method. As of now, the term cryptography refers to the method of hiding the open information to some secret information of non-readable text formats. In cryptography, Number Theory is the main concept.

I. BASIC DEFINITIONS:

Prime Number:

A number which is divisible by 1 and itself is a prime number. It should have distinct factor. It has only two factors.

For example: Primes numbers are 2, 3, 5, 7, 11, 13, 17 ……

Co-Prime Number:

Co-prime number is a number, in which two numbers does not have any common factor other than 1. All prime numbers are co-prime number.

For example: 35=7*5*1
39=3*13*1

Greatest Common Divisor:

Greatest Common Divisor is the number which divides each and every number without leaving a remainder.

For example: 15, 30
Divisors of 15: 1, 3, 5
Divisors of 30: 1, 2, 3, 5, 6, 15, 30
Here the GCD is 12.

Any two numbers are called as relatively prime or co prime if one is the GCD.

i.e. (a, b)=1

17 and 19 are the example for co-primes.

Congruence:

TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 14997 - 15000

If c and d are positive integers and n defines as positive integer, where c is congruent to d modulo n onlyif n divides c-d.

The notation c ≡ d (mod n) says that c is congruent to d modulo n and n is its modulus.

If two integers have the same remainder when divided by n, then it is congruent modulo n.

If c is not congruent to d modulo n, we write c≢ d (mod n)

27 ≡ 13(mod 4) is an example for congruence.

Euler's '□ ' Function:

If m is a positive integer, then □ (m) is defined to be the number of positive integers less than or equal to m and co-prime to m.

For example: □ (17)= 16 is relatively prime to 17 are given by 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16.

And □ (m,n)= □ (m) □ (n) where m, n are termed as relatively prime.

Some qualities of congruency are listed as follows:

- c≡d(mod n) iffc≡d(mod n)
- c≡d+e(mod n) iffc-e≡d(mod n)
- $c_1 \equiv d_1$(mod n) and $c_2 \equiv d_2$(mod n) then $c_1+c_2 \equiv d_1+d_2$(mod n)
- c≡d(mod n) and e is any integer then ec≡ed(mod n)
- c±nk=c(mod n) here k is termed as positive integer.

II. BASIC TERMS IN CRYPTOGRAPHY:

Cryptography is the art or the science of converting the clear information as an unclear information and then information into as a clearer information.

The messenger needs to send a information to the accepter.

An illegal user decides to crack the information.

In private key cryptography, the messenger and the acceptor uses an unique code and they share information with the help of that unique code.

In public key cryptography, we employ the method of encoding. Every person will be provided with an public key which help us for encryption along with that a secret key to extract the encoded message.

Actual intellectual message is called the Plain text.

Encrypted message is called Cipher text.

An algorithm for converting an clear information as unclearer information by transposition & substitution method is said to be Cipher.

The method where every charactertis transformed by a constant point is known as Caesar cipher.

III. CAESAR CIPHER KEY CRYPTOGRAPHY

Caesar cipher is one of the earliest known and simple cipher employed by Magesticking Julius Caesar during 50 B.C. Caesar sendeda information to Marcus Cicero through a rudimentary replacement where every character in the information is substituted with letter which occurs three places down the alphabet. In the last three letters cycling back to the first three letters. Underneath the characters in plain text is changed into corresponding characters which are given below:

A B C D E F G H I J K L
D E F G H I J K L M N O
M N O P Q R S T U V W P
Q R S T U V W X Y Z X Y Z
A B C

For example: TREATY IMPOSSIBLE is changed as WUHDWB LPSRVVLEOH.

By the method of Caesar cipher it can be easily expressed. The actual text which is known as plaintext is first denoted numerically. The characters in the text is changed into corresponding digit which are as follows:

A B C D E F G H I J K 0
1 2 3 4 5 6 7 8 9 10
L M N O P Q R S T U V 11 12
13 14 15 16 17 18 19 20 21

January-February 2020
ISSN: 0193-4120 Page No. 14997 - 15000

W X Y Z
22 23 24 25

Here A be the Plain text and B be the Cipher text then B≡A+3(mod 26)

For example:

The plain text TREATY IMPOSSIBLE is changed as

1917401924 8121514181881114.

By the properties of congruence,

B≡A+3(mod 26), from each corresponding digits we get,

222073221 1115182121114147

WUHDWB LPSRVVLEOH

To find the Plain text A this same procedure can be reversed.

B-3≡A(mod 26)

A≡B-3(mod 26).

IV. RSA PUBLIC KEY CRYPTOGRAPHY

In 1977; R. Rivest, A. Shamir, L. Adelman invented the first public-key cryptosystems which comprises of one basic ideas from Numerical Analysis. This enciphering system is termed RSA. In a public key cryptosystem, the messenger and the acceptor is known as Alice and Bob. Alice and Bob is provide with two keys a public and a secret key. The encryption key is known as public and the decryption key is kept secret which is known as private key.

In RSA cryptosystem Bob select two prime numbers R and S and calculate the integer n=r*s, then he selects a integer c which is not equal to one that does not have many number of digits, still it will be co-prime to (r-1)(s-1)=□ (m) and it's inverse modulo is (r-1)(s-1)=□ (m) and compute e=c^{-1} with given modulo. Bob displays c and m. The number e is defined as its public key.

The encoding procedure starts from the conversation of information, it is to be transferred into a number N with digit in place of alphabets. Punctuations of the plain text is substituted with 2 digit number.

For Instance:

A B C D E F G H I J K L
00 01 02 03 04 05 06 07 08 09 10 11
M N O P Q R S T U V W X
12 13 14 15 16 17 18 19 20 21 22 23
Y Z . , ? 0 1 2 3 4 5 6 7
24 25 26 27 28 29 30 31 32 33 34 35 36
8 9 !
37 38 39

We are considering N<n, or else N will be splitted as block of digit. N_1, N_2, ……., N_s as respective size. Every block will be encoded in particular.

Sender camouflage the plaintext integer N into a Cipher text number 't' of rising 'e' power to M and by taking modulus n.

$N^e \equiv t \pmod n$

The legal beneficiary decode the message which is send by determining the integer j.

e.j ≡1[mod □ (n)]

Rising the encrypted message to the 'i' power and decreasing its modulo n then the actual text number N can be changed.

$r^j \equiv N \pmod n$

For example:

We select two primes r=5 and s=3

And n=15=3*5

□ (n)=□ (15)=□ (3)□ (5)=2*4 =8

Here we select e=3 to be ciphering exponent where 3 and 8 are co-prime to each other. Then recovery exponent the unique integer j satisfies the congruence 3.j≡1(mod 15) and j=3.

The original information is

STAY STRONG

The Corresponding number are

18190024181917141306 which is the Plain text.

Hence N>n, split N into blocks of two digit numbers.

N=2

$18^2 \equiv 12 \pmod{15}$

$19^2 \equiv 4 \pmod{15}$

$24^2 \equiv 9 \pmod{15}$

$18^2 \equiv 12 \pmod{15}$

$19^2 \equiv 4 \pmod{15}$

$17^2 \equiv 8 \pmod{15}$

$14^2 \equiv 14 \pmod{15}$

January-February 2020
ISSN: 0193-4120 Page No. 14997 - 15000

$13^2 \equiv 7 (\text{mod} 15)$
$06^2 \equiv 6 (\text{mod} 15)$
The encrypting of given message is
12 4 9 12 4 8 14 7 6

V. USES OF CRYPTOGRAPHY

With the advent use of internet and electronic commerce, Cryptography has been mainly used in military and diplomatic commerce and it has been remained for centuries. Cryptography plays major role in the functioning of the global economy. Cryptography aid in providing secured services such as withdrawal of cash from ATM, authentication, time stamping, e-money, storage of files using PGP. Cryptography is also used to secure socket layer, Kerberos etc. from encrypted process.

CONCLUSION

From the research article we come into understanding by which all the Number Theory tools makes a vital performance in cryptography in hiding the data. Similarly there are enormous tools in Number Theory which have been used for security purposes such as primes, divisors, Euler's '□' function and congruence. Caesar cipher key cryptography and also in RSA public key cryptography are relevantly used. By which we could observe that varied view at the contest in Algebra and Number Theory.

REFERENCES

1. AtuKahate, Cryptography and Network Security, 3rd Edition.
2. C. Cocks, A note on Non-Secret Encryption. Available online at http://cryptocellar.org/cesg/notense.pdf
3. Jim Sauerberg, From Private to public key Ciphers in three Easy Steps.
4. John Wiley & Sons, Applied Cryptography.
5. Kahn, David, The Codebreakers: The comprehensive History of secret Communication from Ancient Times to the Internet.
6. M. WelledaBaldoni and CiroCiliberto, Elementary number Theory, Cryptograpy and codes.
7. MihirBellare, Philip Rogaway, Introduction to Modern Cryptography.
8. Neal Koblitz, A course in Number Theory and Cryptography, 2nd Edition. Simon and Schuster, The Cracking Code Book.
9. Pachghare, Cryptography and Information Security.
10. R. L Rivest, A. Shamir, L. Adelman, A Method for obtaining Digital Signatures and Public-key Cryptosystems. Available online at http://people.csail.mit.edu/rivest/Rsapaper.pdf