International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

# Application to Cryptography Number of Theory Theoretic Functions

**Ramesh B.Ghadge**[1]

[1]AssistantProfessor & H.O.D, Department of Mathematics, Kalikadevi Arts, commerce & Science College, shirur kasar, Ta. shiurKasar, Dist. Beed, Maharashtra, India

**Article Info**
Volume 9, Issue 5
Page Number : 35-39

**Publication Issue :**
July-August-2021

**Article History**
Accepted : 02July2021
Published:25 July, 2021

## ABSTRACT

The cryptography is the art of achieving security by enclosing messages to make them non Readable.in Mathematics.A function domain is the set of natural numbers is called a number theoretic function. These types of functions having special importance in the discus some important number of theory in Mathematics. Theoretic function.

**Keywords: -** The military, Lovers, diarists, the diplomatic corps, secret writing functions Mobius function Theory of Numbers in Mathematics.

## I. INTRODUCTION

A cryptography comes from the Greek word which means it has a long and colorful history going back historically, four groups of people have used and contributed to the art of cryptography.

Out of the se the military has had the most important role and had shaped the field over the centuries by applying the cryptographic. Before discussing more about the cryptography some common terms used with the study of cryptography.

Let a function T (N) to give the number of positive integer divisors of any given positive integer n. such a function must be of very different from the functions usually studies in algebra or analysis for it depend in critical way not only upon the value of n, but also upon the standard representation of N.

If f (n) is an arithmetic function not identically zero such that f (m n) = f (m).f (n) for every pair of positive integers m, n satisfying (m, n) = 1.then f (n) is said to be multiplicative function.

It f (m n) = f (m) f (n) whether m and n are relatively prime .may or may not equal to.1 then f (n) is said to totally multiplicative. It f and g multiplicative functions such that f (p) = g (P) for all primes p and all positive integers then (n) = g (n) for all positive integers α.

## II. CRYPTOGRAPHY

The art of devising the ciphers is called cryptography.

**Decryption**: The process of converting ciphetext into plaintext is known as decryption or deciphering.

**Cryptanalysis:** -The art of breaking the cipher is known as cryptanalysis.

**Encryption:** - The process of converting plaintext into cipher text is known as encryption or enciphering.

**Cryptology**: - The cryptography and cryptanalysis together are called cryptography

**Ciphetext:** - The coded message is known as the cipher text.

**Plaintext:** -The original message the is to be encrypted is known as plaintext.

**Substitution Cipher Technique:** -Substitution cipher technique characters of a plain text message are replaced by other characters. Substitution cipher preserves the order of the plain text symbols but disguise some techniques using the substation cipher.

**Caesar cipher**:- This substitution technique was first proposed by the Julius Caesar and so is named as Caesar cipher in this technique each alphabet in the message is replaced by the third forthcoming alphabet in the series **scheme**.

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

**Encryption with modified Caesar cipher:** -The cipher text NKRRU LXOKTJ for the plain text message hello friend by replacing each alphabet of the original message by the next sixth alphabet in the sequence. On the other hand, decryption with modified Caesar cipher is not very simple. Each alphabet has 25 possibilities of replacement. We have to test all these possibilities to get the original message. Now suppose theorginal message from the cipher text NKRRU LXOKTJ. We have to try all the 25 possible replacement for each alphabet in the cipher text.

**The steps as shown in the table:-**

| Ciphertextreplacementorder (k) | N | K | R | R | U | | L | X | O | K | T | J |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | O | L | S | S | V | | M | Y | P | L | U | K |
| 2 | P | M | T | T | W | | N | Z | Q | M | V | L |
| 3 | Q | N | U | U | X | | O | A | R | N | W | M |
| 4 | R | O | V | V | Y | | P | B | S | O | X | N |
| 5 | S | P | W | W | Z | | Q | C | T | P | Y | O |
| 6 | T | Q | X | X | A | | R | D | U | Q | Z | P |
| 7 | U | R | Y | Y | B | | S | E | V | R | A | Q |
| 8 | V | S | Z | Z | C | | T | F | W | S | B | R |
| 9 | W | T | A | A | D | | U | G | X | T | C | S |
| 10 | X | U | B | B | E | | V | H | Y | U | D | T |
| 11 | Y | V | C | C | F | | W | I | Z | V | E | U |
| 12 | Z | W | D | D | G | | X | J | A | W | F | V |
| 13 | A | X | E | E | H | | Y | K | B | X | G | W |
| 14 | B | Y | F | F | I | | Z | L | C | Y | H | X |
| 15 | C | Z | G | G | J | | A | M | D | Z | I | Y |
| 16 | D | A | H | H | K | | B | N | E | A | J | Z |
| 17 | E | B | I | I | L | | C | O | F | B | K | A |
| 18 | F | C | J | J | M | | D | P | G | C | L | B |
| 19 | G | D | K | K | N | | E | Q | H | D | M | C |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | H | E | L | L | O | | F | R | I | E | N | D |
| 21 | I | F | M | M | P | | G | S | J | F | O | P |
| 22 | J | G | N | N | Q | | H | T | K | G | P | F |
| 23 | K | H | O | O | R | | I | U | L | H | Q | G |
| 24 | L | I | P | P | S | | J | V | M | I | R | H |
| 25 | M | J | Q | Q | T | | K | W | N | J | S | I |

Thus we obtain the plain text message HELLO FRIEND against cipher text NKRRU LXOKTJ from the table thus breaking the code with modified clear cipher is not as simple as was in Caesar cipher. Modified Caesar cipher is also not very secure. An attacker has only 25 possibilities to try out. An attacker just need the three information to break the code substitution technique is used encrypt the message. 25 possibilities to try. Language of plain text is English .thus by knowing the above information one can easily break the code produced by the modified Caesar cipher technique. Mono alphabetic cipher the main disadvantage with Caesar cipher technique is its predictability and brute force attack to break the code an attack is said to a brute force attack if an attacker attempts to use all possible permutation and combination for breaking the code for example in modified Caesar cipher there are only 25 possibilities for break-in the code and the attacker is assured of a success. The uniform substitution scheme for all the alphabets in a given text message but a random substitution scheme. In words in a given text message each A can be replaced alphabet B through Z each B can be replace by random alphabet like A,C,D the possibilities of permutations or combinations this scheme becomes hard to break.

**Definition: -Positive Divisors: -**For each positive integer n, Z (n) is the number of positive divisors of n including 1and n.

Where,$\sum 1$ denotes the sum of as many 1,s as there are **positive divisors** of n.

**Example**(1) Evaluate$\sum$ (12) and $\sum$ (28).

**Solution: -**Let, positive divisors of 12 are 1, 2, 3, 4, 6, and 12.

So, $\sum (12) = 1+2+3+4+6+12=28$

The positive divisors of 28 are 1, 2, 4,7,14 and 28.

SO, $\sum (28) = 1+2+4+7+14+28=$**56**

**Theorem: -** If f is a multiplicative function and S (n) $=\sum f(d)$ then S (n) is also multiplicative.

**Proof:** Let m, nbe relatively prime integers.

$S(mn) = \sum f(d)$

$= \sum f(d_1 d_2)$

$= \sum f(d_1) f(d_2)$

$= (\sum f(d_1)) (\sum f(d_2))$

= **S (M) S (N).**

**Example**:Evaluate T and $\sum$ for N = 3000?

**Solution:**-Let, N= 3000

$3000 = 2^3.3^1.5^3$.

T (3000) = (3+1). (1+1). (3+1)

= 4.2.4

= 32

$\sum (3000) = (2^4-1)/2-1. (3^2-1)/3-1. (5^4-1)/5-1$

= (16-1)/1. (9-1)/2. (625-1)/4

= 15.4.156

= 9360

Mobius function the number of divisors is given.

F is a multiplicative function. = **9360.**

**Definition: - Function Euler:-**The Euler function phi function is widely used number theoretic function represented by p (n).for n = 1we p (1) = 1 and when n > 1we define p (n) to be the mumble of positive integers less than n and relationally prime n.

**Example:** - The p (12) = 4 because the only positive integers less than 12 and relatively prime to 12are 1, 5,7,11.

**Recurrence Functions:** -The arithmetic function f (n) satisfies a linear recurrence or recursion

If f (n) = a, f (n -1) + bf (n-2) for n = 2, 3 ……

Where, a, and b are fixed number which may be real or complex.

**Integers square free:** -A number a is said to be square free if 1 is the largest square dividing a.

Thus, a is square free if and only if the exponents take only the values o and 1.

In other words an integer > 0 is called square free if it is not divisible any square greater 1.

**General form** the general form of a square free integer is $P_1 P_2 \ldots P_n$ where each $P_i$ are distinct primes.

Function: - The function p (n) as p (n) = p (1) + p (2)…..+ P (8)

$=\sum_{r=1}^{n} p(r)$

It is known as symmetry function of p (n).

**Example:** p (8) = p (1) + (2) ……..+ p (8)

P = 1+1+2+2+4+2+6+4 = **22.**

Integer function greatest: - If x is any real number then the largest integer less the or

Equal to x dented by (x) is the unique integer such that, x-1<(x), <x.

(5)= 5

(20/3)= 6

(-5/2) = - 3

(p) = 3

(2//3) =0

(e)= 2

X=(x) +(x) where (x) is the fractional part of **x.**

**Public key cryptography in mathematics:** -The RSA algorithm is based on the asymmetric key cryptography, also called as public key cryptography. With public key cryptography there are two different keys for encryption decrypting public key cryptography requires the surety that each user must have two keys public key a public key is used by all the parties for encrypting the message to be sent to that user a private key a private key is used for decrypting the message private key is kept secret

Suppose user X wants to send a message to user Y.X encrypts his message with the public key of user Y. Sends this message to user Y. user Y decrypts the message of X by using Y. s private key .only Y knows his private key. User-X-Encrypts text with user Y, s public key –cipher text -Decrypts the cipher text with Y, s private key -plaintext-User -SENDER-RECEIVER. RSA A algorithmThe RSA algorithm is the most popular public key cryptography this scheme was developed by divest,Shamir and adleman.The RSA method is based onsome pimples from Number Theory.The rsa scheme works.

**Simple Columnar Transposition Technique**:-In this technique, we write the plaintext message in a predefined size of rectangle row by row .then we read the message column by column in any random order. The sequence of characters obtained in this manner will be cipher text message .look at the suppose we decided the size of rectangle with seven columns and want to encrypt the plain text message simple columnar technique. Arrange this text into rectangle of seven columns.

| C1 | C2 | C3 | C4 | Cs | C6 | C7 |
|---|---|---|---|---|---|---|
| S | I | M | P | L | E | C |
| O | L | U | M | N | A | R |
| T | E | C | H | N | I | Q |
| U | E | | | | | |

Now,we have to decide the random sequence of column readings suppose -4,2,6,7,1,3,5.by reading columns in the sequence we get the cipher text message .

| PMH | ILEE | EAI | CRQ | SOTU | MUC | LNN |
|---|---|---|---|---|---|---|
| C1 | C2 | C6 | C7 | C1 | C3 | C5 |

This technique is also very simple to break crypt analyst has to try few permutations and combinations of rectangle size and column orders to get the original plaintext message cipher text also contains the frequencies of the alphabets as in original plaintext message diagram and trigram frequency sequence can also be useful to decrypt the message to add more

complexity to the simple columnar transposition technique more than once.

The plaintext message N is assumed to be less than in the enciphering modulus so that it would be possible to distinguish n from any larger integer congruent to modulo the message is very lengthen and possible to handle a single integer the numeric form n of the plaintext is converted into cipher text R as a number the transmitted message the authorized person the user chooses an arbitrary positive integer is placed in a public file but the factors of n are kept secret.

**Example:** - Encrypt the message no using N=1415 RSA system?

**Solution:** - First convert plaintext number of the message is given by N = 1415

Let, p =19

q = 23

n = 19.23=437

p = (n) = (19-1) (23—1)

= 18.22

= 396.

Since, we require N < n we split Nin to blocks of two digits each given

$N_1$ = 14

$N_2$ =15

K= 29

We, have

Ki ≡≡ 1 (mod p (n))

29j ≡ 1 (mod 396)

This gives j = 41

Now, $N_1$ encrypts as $14^{29} \equiv 203$ (mod 437)

$(203)^{41}$ = 14 (437)

Thus the secret transmission of N is 203

The authorized recipient recovers calculating

$(203)^{41}$ = (mod 437) $N_2$ =15

15 = -35 (mod 437)

= 402 (mod 437)

Thus secret transmission of $N_2$is402

Therefore .cipher text is **203402.**

RSA system to be safe it must not be computationally feasible to recover the plaintext from the public key the large is the enciphering modulus the safer is the message coded from deciphering.If d is a positive divisor of a positive integer m the number of integers in the complete residue system modulom, with m have the greaest common divisor d is we know that in completeresidue system modulo the multiples of dare of the for the number of k is p m/n.the fundamental theorem of arithmetic on being expressed in canoniccalform if d is any positive divisor of n the p d is equal to the value of one and only one term in the product rail fence technique is the simplest example of transposition cipher in the technique plaintext is written down as the sequence of diagonal and then read row by row to produce the cipher text for example to encrypt the message rail fence transposition manner.

## III. REFERENCES


[1]. Inan Niven, herbet Zuckerman An introduction to theory of numbers Ltd NewDelhi1997.

[2]. S.G Telang Number Theory Tata MeGraw hills New Delhi-1988.

[3]. C.Y hsing elementary theory of numbers allied publishers Ltd New Delhi-1992.

[4]. S.B. Malik basic Number Theoryallied publishers Ltd New Delhi-1987.

[5]. Pundir Theory of Numbers pragati Prakash a Meerut-2004.

[6]. G.E.Andrews Number Theory Hindustan publishing corporation New Delhi-2003.

[7]. David Burton Elementary Number Theory MeGraw Hill Education India Edition- 2012.

[8]. Hari Kishan Number Theory Krishna Prakash and media (p) Ltd. - 2004.

[9]. Dr.Rimple pundir Theory of Numbers pragati Prakash and Meerut First Editon-2009.

[10]. Dr.Sudhir k. pundir Theory of Numbers pragati prakashan Meerut fifth Editon-2017.