Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Number Theory in Providing Security

Ms. Radha K. ,
M. Sc, M. Tech
Assistant Prof, KKC Institute of PG studies, Puttur, India

Sri. BALAJI G. ,
M. Sc, M. C. A, M. Sc (Psychology) Assistant Prof,
KKC Institute of PG studies, Puttur, India

Ms. Jaya Sudha VP,
B. Tech, MBA,
M. Tech (Pursuing) Student, SWETHA Institute of Technology & Science, Tirupati, India

Abstract:* Number theory plays a important role in encryption algorithm. Here I show if we are not using prime number and congruence's and some statistical tools what are problems will occur in encryption and decryption process in providing security. This paper provides importance of number theory in providing security for transmitting messages and data. At this juncture paper provides importance of prime number, congruence's and divisibility , which is set to be the number theory and it is various perspective in cryptography the process mean for security.

Key words: Prime Number, Modular Arithmetic, Cryptography, Key Management, Security, Divisibility

I. Introduction:

Number theory is crucial for encryption algorithms. Of at most importance to everyone from bill Gates, to the CIA, as the whole world revolves only through mathematics. Before the dawn of computers, many viewed number theory as last bastion of" pure math" which could not be useful and must be enjoyed only for its aesthetic beauty. The encryption algorithms depend heavily on modular arithmetic. We need to develop various machinery (notations and techniques) for manipulating numbers before can describe algorithms in a natural fashion. We first review basic concepts from elementary number theory ,including the notion of primes, greatest common divisors, congruence's and Euler's phi function .The number theoretic concepts and Sage commands introduced will be referred to in later sections when we present the RSA algorithm.

A "Cryptosystem" is comprised of a pair of related encryption and decryption processes. In Cryptography parlance, our message is called "Plain Text". The process of scrambling our message is referred to as "Encryption". After encrypting our message, the scrambled version is called "Cipher text". From the Cipher text we can recover our original unscrambled message via "Decryption".

II. Number Theory:

Basic concepts from elementary number theory, including the notion of primes, greatest common divisors, congruence's and Euler's Phi function.

PRIME NUMBER:

Public key Cryptography uses many fundamental concepts from number theory such as Prime numbers and greatest common divisors. A positive integer is said to be prime if its factors are exclusively 1 and itself. Her I show the first 20 prime numbers.

Eg;2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71.

DIVISORS:

Let a, b, c are integers such that a=b.c. Then b and c are said to **Divide** (or factors) of ***a*** , while ***a*** is said to be a ***multiple*** of b (as well as of c).The pipe symbol "|" denotes "Divide" so the situation is summarized by $b \mid a \ \wedge c \mid a$ .Here I shows some examples.

1. 1. 77 | 7: false bigger number can't divide smaller positive number
2. 7 | 77: true because 77 = 7 · 11
3. 24 | 24: true because 24 = 24 · 1
4. 0 | 24: false, only 0 is divisible by 0
5. 24 | 0: true, 0 is divisible by every number (0 = 24 · 0)

GREATEST COMMON DIVISORS:

Let a and b are integers, not both zero .Then the greatest common divisors (GCD) is the largest positive integer which is a factor of both (a, b).We use G.C.D to denote largest positive factor. Some examples are,

E.g.: 1. gcd (3, 59) is 1
2. gcd (18,27) is 9

CONGRUENCE'S:

When one integerded is divided by a non-zero integer, we usually get a remainder. For example upon dividing 23 by 5,we get a reminder of 3,when 8 is divided by 5 the remainder is again 3.The notion of congruence helps us to describe the situation in which two integers have the same remainder upon division by a non-zero integer .Let $a, b, n \in \mathbf{Z}$ such that

$n \neq 0$.If *a* and *b* have the same remainder upon division by n, then we say that *a is congruencen's to b* modulo *n* and denote this relationship by $a \equiv b \pmod{n}$

This definition is equivalent to saying that *n* divides the difference of *a* and *b* i.e., $n \mid (a-b)$.Thus $23 \equiv 8 \pmod{5}$ because when both 23 and 8 are divide by 5.The answer becomes 3.The command mod allows us to compute such a remainder.

Ex: mod(23,5)=3.

EULER'S FUNCTION:

Euler's Phi Function counts the number of integers *a* with $1 \leq a \leq n$ such that gcd (*a*,*n*)=1.This number is denoted by $\varphi(n)$.Euler's Phi Function is sometimes referred to as "Euler's Totient Function".

Ex: To compute $\varphi(20)$ as 1,3,7,9,11,13,17,19.

This paper presents the important of number theory while providing security for transmitting the messages. First we know the meaning for Surety is "Cryptography".

III. Cryptography:

A Cryptosystem is comprised of a pair of related encryption and decryption processes. In cryptography parlance, our message is called "*Plain Text*" .The process of scrambling our message is referred to as *"Encryption.".*After encryption our message, the scrambled version is called "*Cipher Text*". From the *Cipher Text.* We can recover our original unscrambled message via"*Decryption*".

HOW TO KEEP A SECRET:

Cryptography is the science (some might say art) of concealing data. Imagine that we are composing a confidential email to someone. Having written the email, we can send it in one of two ways. The first, and usually convenient, way is to simply press the send button and not care about how our email will be delivered. Sending an email in this manner is similar to writing our confidential message on a postcard can see our message. On the other hand ,before sending our email, we can scramble the confidential message and then press the send button. Scrambling our Message is similar to enclosing our postcard inside an envelope .While not 100% secure, at least we know that anyone wanting to read our postcard has to open the envelope.

In Cryptography parlance, our message is called "***Plaintext***" .The process of scrambling our message is referred to as ***"Encryption".*** After encryption our message, the scrambled version is called "***Cipher Text***."From the Cipher text, we can recover our original unscrambled message via "***Decryption".*** The following figure illustrates the processes of encryption and decryption.

A ***Cryptosystem*** is comprised of a pair of related encryption and decryption processes.

```
+--------------+encrypt +-------------+decrypt+----------+
   Plaintext---------->cipher text---------->plaintext
+--------------+          +--------------+          +----------+
```

IV. Simple Encryption:

Variations on the following have been used to encrypt messages for thousands of years

1. Convert a message to capitals.
2. Think of each letter as a number between 1 and 26
3. Apply an invertible modular function to each number.
4. Convert back to letters (0 becomes 26)

Letter←→ Number Conversion Table:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**

ENCRYPTION FUNCTION:

f (*a*) = (3*a* + 9) **mod** 26

Encrypt "Stop Thief" STOP THIEF (capitals)

1. 19,20,15,16 20,8,9,5,6
2. 14,17,2,5 17,7,10,24,1
3. NQBE QGJXA

DECRYPTION FUNCTION:

Decryption works the same, except that you apply the inverse function.

$g(a) = 9(a - 9)$ **mod** $26 = (9a - 3)$ **mod** 26

1.NQBE QGJXA

2.14,17,2,5 17,7,10,24,1

3.19,20,15,16 20, 8,9,5,6

4. STOP THIEF

Here if we r not using ***mod*** then it is simple to know how the data encrypted then after some attempts. You see the original message. It is easy to see the original message .That's why we use mod function for providing secrete. Suppose we not using the ***mod*** function then it is so simple to identify the original message. Here it shows the Impotence of Number Theory tool Mod in providing Security.

V. Classical Encryption Technique:

HILL CIPHER:

This is one type of encryption technique..In this method the encryption function is defined by

C=KP mod 26

Where C and P are column vectors of length is 3x3 matrices represents the encryption key. Operations are performed mod 26.In this method also we "***Mod*** "function in encryption process this is number theory tool. So the Number theory functions are so important in providing security while transmitting messages

Some of the functions are so important in number theory while providing security in transmitting messages in network and in internet.

VI. Conclusion:

In this paper we perceive every Number Theory tool plays an important role in providing security for transmitting messages. For the reason that by Mod we calculate the encryption and decryption of messages. The Number Theory function Mod plays important role in Hill cipher technique and also in RSA algorithm also in some encryption Algorithms. The Number theory Functions are used in almost all encryption and decryption algorithms in Crypto Graphy.

References:

1. Security Analysis, Benjamin Graham &David L. Dodd
2. Network security Essentials, 3rd edition, William Stallings
3. Network Security, 2nd Edition, Charlie Kaufman.
4. Network Security, 2nd Edition, AnkitFadia
5. Express Learning cryptography and network security, ITL education solution
6. Limited.
7. Cryptography and network security, William Stallings.