IMPORTANCE OF NUMBER THEORY IN CRYPTOGRAPHY

Pawanveer Singh[1], Dr. Amanpreet Singh[2], Shelja Jhamb[3]

[1]Post Graduate Department of Mathematics, Lajpat Rai D. A. V. College Jagraon, (India)

[2]Post Graduate Department of Mathematics, SGTB Khalsa College Anandpur Sahib Punjab, (India)

[3]Research Scholar I.K.G Punjab Technical Universiy, Jalandhar (India)

ABSTRACT

Number Theory plays an important role in encryption algorithm. Cryptography is the practice of hiding information, converting some secret information to not readable texts. The paper aims to introduce the reader to applications of Number Theory in cryptography. We will briefly talk about an idea of encryption in Caesar ciphering and RSA public key cryptography. Many tools in Number Theory like primes, divisors, congruencies and Euler's 'ϕ' function are used in cryptography for security.

Keywords: Cryptography, Divisors, Euler 'ϕ' function.

I. INTRODUCTION

For thousands of years people have searched for the way to send a message secretly. There is a story that, in ancient time, a king needed to send a secret message to his general in battle. The king took a servant, shaved his head and wrote the message on his head. He waited for the servant's hair to grow back and then sent the servant to the general. The general then shaved the servant's head and read the message. If the enemy had captured the servant, they presumably would not have known to shave his head and message would have been safe.

Cryptography is the study of methods to send and receive the secret messages. In general we have a sender who is trying to send a message to receiver. There is also an adversary, who wants to steal the message. We are successful if sender is able to communicate a message to the receiver without adversary learning what the message was.

We will use some important concepts of Number Theory and Cryptography which are given below:

Important concepts in Number Theory

Prime Numbers- A positive integer p is said to be a prime if it has only two factors namely 1 and p itself.

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

Divisors: A positive integer a is said to divide an integer b if there exist an integer c such that $b = a.c$ and written as $a \mid b$.

For Example $2 \mid 10$ as 10 = 2.5 but 3 do not divide 10 as there does not exist any integer c such that 10 = 3. c

Greatest Common Divisor: Let a and b be two positive integers then an integer d is called greatest common divisor of a and b if $d \mid a$ and $d \mid b$ i.e. d is common divisor of a and b.

And if any integer c is such that $c\,|\,a$ and $c\,|\,b$ then $c\,|\,d$ i.e. any other common divisor of a and b will divide d it is denoted by $d=(a,b)$

For Example: $6=(24,30)$

Two numbers a and b are said to relatively prime or co prime if their greatest common divisor is 1 i.e. $(a,b)=1$

For Example: 10 and 11 are co prime

Congruence: Let a and b be two integers and m is any positive integer then a is said to congruent to b modulo m if m divide difference of a and b i.e. $m\,|\,a-b$. It is denoted by $a\equiv b(\bmod m)$

For Example: $27\equiv 13(\bmod 4)$

Euler's 'ϕ' Function : An arithmetic function Euler's Toitent function 'ϕ' is defined as $\phi(n)$ = number of positive integers less than or equal to n and co prime to n i.e. $\phi(n)$= number of positive integers 'a' such that $1\le a\le n$ and g.c.d.$(a,n)=1$

For Example: $\phi(15)=8$ as primes relative to 15 are given by 1, 2, 4, 7, 8, 11, 13, and 14.

And $\phi(mn)=\phi(m)\,\phi(n)$ where m and n are relatively prime.

Some simple properties of congruence are given below:

(1) $a\equiv b(\bmod m)$ iff $b\equiv a(\bmod m)$

(2) $a\equiv b+c(\bmod m)$ iff $a-c\equiv b(\bmod m)$

(3) $a_1\equiv b_1(\bmod m)$ and $a_2\equiv b_2(\bmod m)$ then $a_1+a_2\equiv b_1+b_2\,(\bmod m)$

(4) $a\equiv b(\bmod m)$ and c is any integer then $ca\equiv cb\,(\bmod m)$

(5) $a\pm mk\equiv a\,(\bmod m)$ where k is any integer

Important concepts in Cryptography

(1) Cryptography is the study of methods to send and receive secret message.

(2) The sender wants to send a message to receiver.

(3) The adversary wants to steal the message.

(4) In private key cryptography, the sender and receiver agree in advance on a secret code, and then send message using that code.

(5) In public key cryptography the encoding method can be published. Each person has a public key used to encrypt message and a secret key used to encrypt an encrypted message.

(6) The original message is called the Plain text.

(7) The encoded text is called Cipher text.

(8) A Caesar cipher is one in which each letter of the alphabet is shifted by a fixed point.

II. CAESAR CIPHER KEY CRYPTOGRAPHY

One of the earliest cryptographic system was used by great Roman emperor Julius Caesar around 50 (B.C.). Caesar wrote to Marcus Cicero using a rudimentary substitution cipher in which each letter of the alphabet is replaced by letter that occurs three places down the alphabet. With the last three letters cycled back to the first three letters. Underneath the plain text letter the substitution alphabet for Caesar cipher is given by

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

For Example: NUMBER THEORY IS EASY is transformed into QXPEHU WKHRUB LV HDVB

With the help of congruence theory Caesar cipher can be easily described. Any plaintext is first expressed numerically by transforming the character of the text into digit by means of some correspondence such as

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z										
18	19	20	21	22	23	24	25										

Now if P is the plain text and C is the cipher text then $C \equiv P+3 (\bmod 26)$

For Example:

NUMBER	THEORY	IS	EASY
1320121417	1974141724	818	401824

Using congruence $C \equiv P+3 (\bmod 26)$, for each alphabet and corresponding digit we get

1623154720	2210717201	1121	73211
QXPEHU	WKHRUB	LV	HDVB

To recover plain text this procedure is reversed by using $C-3 \equiv P (\bmod 26)$ i.e. $P \equiv C-3 (\bmod 26)$.

III. RSA PUBLIC KEY CRYPTOGRAPHY

In 1977; R. Rivest, A. Shamir and L. Adelman proposed a public key system that includes only elementary ideas from Number Theory. Their enciphering system is called RSA.

Public key cryptography overcomes the problems associated with using codebook. In a public key cryptosystem, the sender and receiver (often called Alice and Bob respectively) do not have to agree in advance on a secret code. In fact they each publish part of their code in public directory. Further an adversary with access to the encoded message and the public directory still cannot decode message. More precisely Alice and Bob will each have two keys a public key and a secret key

In RSA cryptosystem Bob choose two prime numbers p and q (which in practice each nave at least hundred digits) and compute the number $n = p.q$. He also chooses a number $e \neq 1$ which indeed not have large number of digits but is relative prime to $(p-1)(q-1) = \phi(n)$, so that it has inverse with modulo

$[\ (p-1)(q-1)=\phi(n)\ ]$and compute $d=e^{-1}$with given modulo. Bob publish e and$n$. The number d is called his public key.

The encryption process begins with the conversion of message to be sent into an integer M by means of digit alphabet in which each letter, number or punctuation mark of the plaintext is replaced by two digit integer

For Instance:

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

Here it is assumed$M<n$, otherwise M is broken up into blocks of digits $M_1, M_2 ...., M_s$ of the approximate size. And each block is encrypted separately.

The sender disguises the plaintext number M as a cipher text number ‘ r ’ by raising ‘ e ’ power to M and by taking modulus n i.e. $M^e \equiv r\,(\bmod n)$

At other end the authorized recipient decipher transmitted information by first determining the integer j , the secret recovery exponent for which $e.j \equiv 1[\ \bmod \phi(n)\ ]$

Raising the cipher text number to the ‘ j ’ power and reducing it modulo n recovers the original plain text number M i. e. $r^j \equiv M\,(\bmod n)$

For Example:

We select two primes $p=59$ and $q=41$

And $n=2419=59.41$ and $\phi(n)=\phi(2419)=\phi(59)\phi(41)=58.40=2320$

We may choose $e=3$to be enciphering exponent where 3 and 2320 are co prime to each other

Then recovery exponent the unique integer j satisfying the congruence $3.j \equiv 1(\bmod 2320)$ and $j=1547$ satisfy the given congruence

The given message is GOLD MEDAL

The plain text number is 061411031204030011

Since$M>n$, so split M into blocks of three digit numbers i.e. 061 411 031 204 030 011

$$061^3 \equiv 2014(\bmod 2419) \qquad 411^3 \equiv 1231(\bmod 2419) \qquad 031^3 \equiv 0763(\bmod 2419)$$

$$204^3 \equiv 1393(\bmod 2419) \qquad 030^3 \equiv 0391(\bmod 2419) \qquad 011^3 \equiv 1331(\bmod 2419)$$

The encrypting of the given message is 2014 1231 0763 1393 0391 1331

IV. USES OF CRYPTOGRAPHY

Cryptography has remained important over the centuries, used mainly for military and diplomatic communication with the advent of internet and electronic commerce. Cryptography has become vital for the functioning of the global economy. Sensitive information such as bank records, credit card reports, password or private is encrypted modified in such a way that hopefully, it is only understandable to people who should be allowed to have access to it, and undecipherable to others. Cryptography is also known practical means for protecting information transmitted through public communication networks, such as those using telephone lines, microwaves or satellites.

V. CONCLUSION

In this paper we perceive that every Number Theory tool plays an important role in cryptography to hide information. Many tools in Number Theory like primes, divisors, congruencies and Euler's 'ϕ' function plays important role in cryptography for security purpose. The congruencies are used in Caesar ciphering key cryptography and also in RSA public key cryptography. This gives an idea of cryptosystem in the context of Algebra and Number Theory.

REFERENCES

[1] David, M. Burton, *Elementary Number Theory*, 2nd Edition, UBS Publishers.

[2] G. H. Hardy, and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, 1979

[3] Gilles Brasssard, Modern Cryptography : *A Tutorial , Lecture Notes in Computer Science, Vol.325, Springer-verlag,1988*

[4] Niven, Zuckerman and Montgomery, *An Introduction to the Theory of Numbers* , 5th ed., New York: John Wiley and Sons,1991

[5] Neal Koblitz, *A course in Number Theory and Cryptography*, New York: Springer Verlag,1994

[6] R. Cramer and V. shoup, *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher text Attack*. In *crypto*'98, LNCS1716, pages13-25, *Springer-Verlag, Berlin,1998*

[7] Simon Singh, *The codebook, Anchor Books*, 1999.

[8] T. M. Apostol, *Introduction to Analytic Number Theory* , Springer-Verlag (New York),1976