USES OF QUEEN OF MATHEMATICS IN CRYPTOGRAPHY

Mrs. Sapna Atish Bhusare

Asst.prof.in Ashoka center for business and computer studies, Nashik.

Smt. Rameshwari Hullule

Asst.prof.in Ashoka center for business and computer studies ,Nashik.

Smt. Madhuri Ashok Gaikwad (Shirsath)

Asst.Prof. in PCMCS College ,Nashik.

Objective- Aim of the paper to introduce the reader applications of Number Theory in cryptography. The main role of Cryptography is to converting some secret information to not readable texts. We will talk in detail about an idea of encryption in Caesar ciphering and RSA public key cryptography.

Introduction

The greatest mathematicians Carl Friedrich Gauss, said that "Mathematics is the queen of the sciences and **Number theory** is the **Queen of Mathematics**." Number theory plays very important role in encryption algorithm. Many tools in Number Theory like prime number, divisors, congruence relation and Euler's ' phi ' function are used in cryptography for security..

Aristotle defined mathematics as "the science of quantity" and this definition persuade until the 18th century. Aristotle also noted that focusing on quantities alone could not distinguish mathematics from sciences such as physics; His view distinguished mathematics from the examples of abstraction and reality, studying property as "separated in thought" [1].

There are number of scientist are working in mathematics. Some of them great mathematicians are Aryabhatta, Bhaskaracharya, Pythagorous, Newton, Carl Guass, Euclid , Leonhard Euler, Shrinivasa Ramanujan ,Fermat, Shakuntala devi

Albert Einstein ,David Hilbert ,Stephan Hawking etc.

Mathematics is the Universe's natural tongue. Since the beginning of our existence as a species, numbers have deeply fascinated us. The oldest branch of mathematics is to invite your great thinkers to unravel the many mysteries of the universe, to count the numbers, to count the numbers.[2]

Number theory is a theory focusing on numbers. More than 3,000 years ago,

the concept of arithmetic and numbers has occurred. In early period, the term of number theory was arithmetic and was succeed by "number theory" in the early twentieth century. [3]Number theory basically deals with the nature of integers.

We will discuss 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 p and 1 itself.

Prime numbers are {2,3,5,7,11,.....}

Divisors: If there exist integer k such that a=bk ,then we say that a positive integer a is divisible by b and it is written as b|a.

For Example 1) 12 |24 as 24 = 12*2.

Greatest Common Divisor: A positive integers d is called as greatest common divisor of a and b if d |a and d |b i.e. d is common divisor of a and b ,where a an b are two positive integers

2)If any common divisor c is such that c|a and c|b then c|d i.e. any common divisor of a and b will divide d.It is denoted by d= (a,b) For Example: (42,49) =7.

Two numbers a and b are said to relatively prime or co prime to each other if their gcd is 1 i.e(a,b)=
1.

For Example: 10 and 11 are relatively prime.

RSA Public key Cryptography

In 1977; R. Rivest, A. Shamir and L. Adelman suggest a public key system that includes only elementary ideas from Number Theory. RSA method is nothing but their enciphering system. Public Key Cryptography reduce the difficulties associated with using codebooks. In this system the receiver & sender (often called Alice and Bob respectively) do not have to agree in advance on a secret code. Forward an opponent to enter encoded message and public directory can't decode message yet. More precisely Alice and Bob will give everyoneThe two keys are a public key and a secret key.

In RSA cryptosystem Bob choose two prime numbers p and q (which in practice we take p & q at least hundred digits) & compute the number n = p.q . He also chooses a number e is not equal to 1 but (e,phi(n)) =1(relatively prime to each other) where phi(n)=(p-1)(q-1).so that it has inverse with modulo phi(n)and compute d is equal to inverse of e with given modulo phi(n). Bob publish e and n & the number d is called his public key.

In begining with encryption method the conversion of message to be sent into an integer M,that is the digit alphabet in which each letter, punctuation mark or number of the plaintext is replaced by two digit integer

For instance:

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

we assumed that 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 elevating ' e ' power to M and by taking modulus n i.e. M^e r(mod n)

Posterior the authorized recipient decipher transmitted information by first determining the integer j , the secret recovery exponent for which e.j 1 modn 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 M (mod n)

Example: 1

1. Select two prime numbers, p=17 and q=11
2. Calculate n= p q =17*11=187
3. Calculate φ(n)=(p-1)(q-1)
   =(17-1)(11-1)
   =16*10=160
4. Select e such that e is relatively prime to
   φ(n)=160.

So, we select e=7

5. Determine d such that e d 1 mod φ(n)
   7d 1 mod (160)
   7*23 1 mod (160)
   1611 mod (160)

(d is calculated using extended Euclid's Algorithm)

Here, Public key PU(e, n)=(7, 187)

Private key PR(d, n)=(23, 187)

Suppose, the Plaintext value (M) is 88 then,

6. For Encryption,
   Ciphertext C Me mod (n)

(88)7 mod (187)

888832 mod (187)

11

7. For Decryption,

Plaintext P Cd mod (n)

1123 mod (187)

79720245 mod (187)

88

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 Marvelous 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.

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 ‘ ’ 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

Acknowledgement-

We are very much thankful to Ashoka center for business &computer studies, Nashik for motivating us . I would also thanks to Principal ,vice principal and Head of the Department of computer science of our college, for his constant guidance and extensive support to encourage for this work.

References

[1]Franklin, J. (2014). *An Aristotelian realist philosophy of mathematics: Mathematics as the science of quantity and structure*. Springer.

[2]Kragh, H. S. (2007). *Conceptions of cosmos: from myths to the accelerating universe: a history of cosmology*. Oxford University Press.

[3]Yan, K. (2019, October). A Review of the Development and Applications of Number Theory. In *Journal of Physics: Conference Series* (Vol. 1325, No. 1, p. 012128). IOP Publishing.