Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 3495-3500

http://www.ripublication.com

Number Theory: Backbone Of RSA Cryptography

Ch.JL Padmaja,

Lecturer in Mathematics,
MBTS Government Polytechnic, Guntur, Andhra Pradesh

Abstract

Number theory is a branch of pure mathematics devoted primarily to the study of integers. Although it was considered useless in the ancient days, it gained its prominence in the modern days of digital revolution. The RSA cryptosystem is an asymmetric cryptographic system in which the encryption keys are made completely public. The security of the RSA lies in an algorithm based on Euler's theorem and Fermat's Little theorem. This RSA system is a classic example of how the theorems of ancient mathematicians are being used in this technological age.

Keywords: Congruence, Cryptosystem, Number theory, RSA.

INTRODUCTION

Number theory is a branch of pure mathematics involving primarily the study of integers. It is a vast and fascinating field of mathematics consisting of the study of the properties of whole numbers. It is also sometimes referred as "higher arithmetic" and is among the oldest and most natural mathematical pursuits. The especially important areas are prime and prime factorization and functions such as divisor function and totient functions [1].

When all the important theorems of numbers were proposed (before and around 1700) no one dreamed that these theorems would be of use in secured communication some hundreds of years later. Now, these theorems, proofs and lemmas from proposed in ancient period are manipulated in advancing computer technology.

According the British number theorist, G. H. Hardy:
"The Theory of Numbers has always been regarded as one of the most obviously useless branches of Pure Mathematics."

But his statement is proved wrong. Though they were not of much use in the older days, number theory has an important and vital application today, particularly in

cryptography. The digital revolution in the mid 20th century could find the answers for many real-world problems in Number Theory [2].
Cryptography is the practice of encoding a piece of given information into an unreadable (scrambled) text and decoding the scrambled text into the original information. Here, encoding is technically called *encryption* and decoding is called *decryption*. The original information is referred to as *plain text* and the coded (scrambled) message is called *cipher text*.

CONCEPTS OF NUMBER THEORY

Some basic concepts of number theory and important theorems are reviewed hereunder.

Prime numbers:

Definition: An integer p >1 is called a prime number if it has exactly two positive divisors, namely 1 and p.
The first ten prime numbers are 2,3,5,7,11,13,17,19,23, 29.

Divisibility:

We say that a divides n if there is an integer b such that n=ab
Here, a is called divisor of n, n is called multiple of a, we write a | n. We also say that n is divisible by a.
Ex: 13 | 182, because 182=14*13.

Greatest Common Divisor:

Definition: A common divisor of a and b is an integer that divides both a and b.
Among all the common divisors of two integers a and b which are not both zero, there is exactly one greatest. It is called the greatest common divisor (gcd) of a and b.
Ex: The greatest common divisor of 18 and 30 is 6.

Congruence:

Definition: We say, a is congruent to b modulo m if m divides b-a and we write $a \equiv b \pmod{m}$.
Ex: $10 \equiv 0 \pmod{2}$ and $-2 \equiv 19 \pmod{21}$.

Chinese remainder theorem:

Theorem: Let p,q be co-prime. Then the system of equations
$x \equiv a \pmod{p}$
$x \equiv b \pmod{q}$
has a unique solution for x modulo pq.

Proof: Since p and q are co-prime, let $p1 \equiv p-1 \pmod{q}$ and $q1 \equiv q-1 \pmod{p}$.
Then we claim that if y is an integer such that
$y \equiv aqq1+bpp1 \pmod{pq}$

then y satisfies both equations:
Modulo p, we have y ≡ aqq1 ≡ a(modp) since qq1 ≡ 1(modp). Similarly y ≡ b(modq). Thus y is a solution for x.
It remains to show no other solutions exist modulo pq. If z ≡ a(modp) then z−y is a multiple of p. If z ≡ b(modq) as well, then z−y is also a multiple of q. Since p and q are coprime, this implies z−y is a multiple of pq, hence z ≡ y(modpq).

Fermat little theorem:
Theorem: *Let p be a prime which does not divide the integer a, then* $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Start by listing the first p-1 positive multiples of a:
a, 2a, 3a, ... (p -1)a
Suppose that ra and sa are the same modulo p, then we have $r = s \pmod{p}$, so the p-1 multiples of a above are distinct and nonzero; that is, they must be congruent to 1, 2, 3, ..., p-1 in some order.
Multiply all these congruences together and we find
$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$ or better,
$a^{(p-1)}(p-1)! \equiv (p-1)! \pmod{p}$.
Divide both side by (p-1)!
Then $a^{p-1} = 1 \pmod{p}$.

Euler-Fermat theorem:
If n is a positive integer, ϕ(n) is the number of integers in the range{1,….,n}which are relatively prime to n. ϕ is called the Euler phi-function.

Theorem: *Let a and m be coprime. Then* $a^{\varphi(m)} = 1 \pmod{m}$.

Proof: The proof is completely analogous to that of the Fermat's Theorem except that instead of the set of non-negative remainders {1,2,...,m-1}, we now consider the set $\{m_1, m_2, ..., m_{\varphi(m)}\}$ of the remainders of division by m coprime to m.
In exactly the same manner as before, multiplication by a results in a permutation (but now) of the set $\{m_1, m_2, ..., m_{\varphi(m)}\}$. Therefore, two products are congruent:
$m_1 m_2 \ldots m_{\varphi(m)} = (am_1)(am_2) \ldots (am_{\varphi(m)}) \pmod{m}$
dividing by the left-hand side, $a^{\varphi(m)} = 1 \pmod{m}$.

RSA CRYPTOGRAPHY
Applications of number theory in cryptography are very important in constructions of public key cryptosystems. The most popular public key cryptosystem RSA is based on the problem of factorization of large integers.
The RSA cryptosystem is named after Ron Rivest, Adi Shamir and Len Adleman who invented it in 1977. This is the most widely used public key cryptography in the world. There is no need to exchange a secret key separately in order to encrypt a given message. Its security is based on the difficulty of factoring large integers [3].

The process of the RSA cryptosystem begins with the intended recipient sending the originator two integers. These integers are chosen as follows. First, he decides on two prime integers p and q. Then, he calculates n = pq, and $\phi(n) = \phi(pq) = \phi(p)\,\phi(q) = (p-1)(q-1)$.
Lastly, he chooses an integer e such that $1<e<\phi(n)$ with $\gcd(e, \phi(n)) = 1$. The reason the $\gcd(e, \phi(n))$ must be 1 is to ensure $d = e^{-1} \pmod{\phi(n)}$ exists. If $\gcd(e, \phi(n)) \neq 1$, the inverse of e $(\text{mod } \phi(n))$ does not exist.
The intended recipient then sends only the values for e and n to the originator. Thus, these values are made public while p and q are kept secret. Only the intended recipient knows p and q.
When the originator receives the two values for e and n, he then has all the information he needs to encrypt the message he plans to send over insecure channels to the intended recipient. The public encryption key is e, and the encryption function is $y \equiv x^e \pmod{n}$, where y is the integer value equivalent to the cipher text, and x is the integer value equivalent to the plaintext. The originator can then send the encrypted text to the intended recipient.
When the intended recipient receives the encrypted cipher text, he first finds an integer d such that $d \equiv e^{-1} \pmod{\phi(n)}$. This d is the private decryption key. He knows such a $d \in Z$ exists since $\gcd(e; \phi(n)) = 1$. He can find d by using the Euclidean Algorithm. The decryption function is given by $x \equiv y^d \pmod{n}$.
The American Standard Code for Information Interchange, or ASCII, is a list of numbers and their corresponding characters. These characters include all 95 printable keyboard characters, denoted by integers 32 through 126. The messages are converted into integer counterparts using this ASCII table [4].

Example: Let Ram be the intended recipient and Sitha be the originator. Sitha needs to relay a top secret message to Ram.
Ram starts the process by deciding on two primes, p = 13 and q = 29. Ram finds n = 377 and $\phi(n) = (p-1)(q-1) = (13-1)(29-1) = 336$. He then decides on an $e \in Z$, such that $1 < e < 336$ and $\gcd(e; 336) = 1$. He picks e = 11. He sends the two integer values, 11 and 377, to Sitha across an insecure communication network. It means these values are made public.
Sitha receives Ram's public key, (11; 377), and now begins the encryption process using the encryption key 11 and the encryption function $y \equiv x^{11} \pmod{377}$. Sitha wants to encrypt the message, "now". She first converts the plaintext characters into their integer counterparts using the ASCII table. The plaintext becomes 110, 111, 119. She can now begin the encryption process.
$y \equiv 110^{11} \equiv 310 \pmod{377}$
$y \equiv 111^{11} \equiv 132 \pmod{377}$
$y \equiv 119^{11} \equiv 189 \pmod{377}$

Sitha now sends the encryption cipher text, 310, 132, 189, to Ram.
In order to decrypt this message, Ram first finds d such that $11d \equiv 1 \pmod{336}$, that is, $d = 11^{-1} \pmod{336}$. Since $11(275) \equiv 1 \pmod{336}$, Ram deduces that the decryption

key d is 275; thus, the decryption function becomes $x \equiv y^{275} \pmod{377}$. Ram now begins the decryption process.

$x \equiv 310^{275} \pmod{377} \equiv 110 \pmod{377}$

$x \equiv 132^{275} \pmod{377} \equiv 111 \pmod{377}$

$x \equiv 189^{275} \pmod{377} \equiv 119 \pmod{377}$

Ram now converts these values into the corresponding values according to the ASCII table. Then he uncovers the plaintext message: "now"

This example of the RSA used only small primes. But in real world, in order for the system to work effectively, the primes must be more than 100 digits in length.

CONCLUSION

One of the amazing things about theoretical mathematics is that sometimes purely theoretical discoveries can turn out to have completely unexpected practical applications. One such branch of pure mathematics is Number Theory. Number theory studies the properties of the natural numbers. This study of numbers gained its prominence in this digital age and often called as "queen of mathematics".

In the age of the internet, traditional security technologies such as armed guards, cameras and x-ray machines will be of not much use in case of internet business or bank transactions or take cash out of an ATM. While sending private data though a public network, there is every danger that anyone can intercept and obtain the information. The field of Cryptography comes here as a new kind of security technological system in order to protect the information people send online.

This paper presented that Number Theory tools play an important role in providing security for transmission of messages, especially greatest common divisor and congruence in RSA cryptography. The key to the functioning of the RSA algorithm is the important but easy-to-understand Euler-Fermat Theorem. Encryption of a message is carried in this system by picking two large prime numbers and using mod function. Breaking RSA is hard as factoring large numbers. This proves the efficiency of the congruence in making the RSA secure.

References

[1] N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[2] Luis Finotti, *A Gentle Introduction to Number Theory and Cryptography*, Notes for the Project GRAD, 2009.

[3] D.R. Stinson: *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2002.

[4] Megan Maxey, *A Modern Day Application of Euler's Theorem: The RSA Cryptosystem*, Capstone Project, Georgia college Mathematics Department, 2012.

[5] David Burton, *Elementary Number Theory*, Fifth Edition, McGraw-Hill, 2002.

[6] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.