Prime Numbers in Cryptography-RSA with Pseudoprime

A.Ananth Maria Pushpa

Department of Mathematics

PRIST Deemed to be University,

Thanjavur -613403.

Supervisor

Dr.S.Subramanian,Head of the Department

School of Arts and Science,

PRIST Deemed to be University,

Thanjavur-613403.

Abtract:

In previous paper we dealt with some basic ideas of number theory and cryptography.

In this paper,we are going to discuss about how the numbers especially prime numbers playing an important role in cryptography.In cryptography RSA algorithm is a main platform for secured communication.Here,we will see what . are the changes or difficulties occur when we use pseudoprimes instead of prime numbers.For high security we use large prime numbers in RSA cryptosystem.

Keywords: Prime number,Pseudoprime,Euler's phi function ,encryption,decryption,RSA public key cryptography

Introduction:

Prime numbers are taking a very important and an interesting role play in number theory.Also, Prime numbers plays an important role in cryptography because many encryption algorithms are based on the fact that it is very fast to multiply two large prime numbers but finding reverse is extremely computer intensive .Cryptography is the technique of concealing information,converting secret information from readable texts into non readable texts.

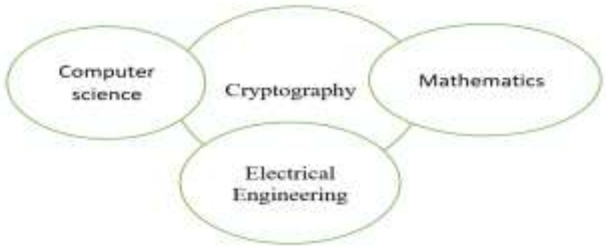
Many concepts in number theory like primes, divisors, congruences and Euler Ø function are used in cryptography for the security purpose.

Importance of Cryptography:

For many years,at different stages,people have sent secret messages by various means. In 1970 s,there was a radical changes when Fermat's theorem and Euler's theorem,popularly known as(a generalization of Fermat's theorem),along with other results in modular arithmetic,became fundamental techniques in many cryptographic systems.

Nowadays,people are doing online transaction,for buying or selling for all that we indirectly using Euler's theorem.

Cryptography is a combination of following subjects.



Rivest-Shamir-Adleman Algorithm: (RSA Algorithm)

* RSA algorithm is a main platform of Cryptosystem.

* RSA algorithm is a asymmetric cryptography algorithm.Here,the public key is given to everyone and private key is kept private.

* RSA algorithm is used in encryption type of public-key cryptography is used for data encryption of e-mail and other digital transaction over an insecure network such as internet.

*RSA is stronger than any other symmetric key algorithm.

Setup of RSA algorithm:

Step 1:

Choose two distinct sufficiently large random primes, p' and q'.

Step 2:

Compute m'= p'q'.

Step 3 :

Compute Euler’s totient function Ø(m’)=(p’-1)(q’-1).

Step 4:

Setting up the encryption key e’, which is a public one.

Select, e’ at randomly with 1< e’ < Ø(m’), so that gcd (e’,Ø(m’))=1.

Step 5:

Compute Decryption key d’, which is a private (secret) one.

i. e) d’= $\frac{1+k\text{Ø}(\text{m}')}{e\prime}$,it should be a non decimal value.

(OR) d’e’=1+ modulo Ø(m’).

The pair (d’,m’) is a private key,whereas (e’,m’) is a public key.

Encryption:

For encrypt the message,the public key is used.

Here ,the plain text m(readable form), is converted into cipher text c(non-readable form).

I.e) c= $m^{e\prime}$(mod m’).

Decryption:

For decrypt the message,the private key is used.

Here,the cipher text c(non-readable form),is converted into plain text m(readable form).

i.e) m=$c^{d\prime}$(mod m’).

The Euclidean Algorithm:

Let b and c be two integers whose greatest common divisor is desired.

Because gcd(|b|,|c|)=gcd(b,c),there is no harm in assuming that b≥c>0.

The first step is to apply the Division Algorithm to b and c to get

$$\begin{aligned}
&\mathrm{b} = \mathrm{q}_1\,\mathrm{c} + \mathrm{r}_{1,} \quad 0 < \mathrm{r}_1 < \mathrm{c},\\
&\mathrm{c} = \mathrm{q}_2\mathrm{r}_1 + \mathrm{r}_{2,} \quad 0 < \mathrm{r}_2 < \mathrm{r}_1,\\
&r_1 = q_3 r_2 + r_3, \;\; 0 < r_3 < r_2,\\
&\quad .\qquad .\qquad\qquad .\\
&\quad .\qquad .\qquad\qquad .\\
&\quad .\qquad .\qquad\qquad .\\
&r_{j-2} = r_{j-1}q_j + r_j, \;\; 0 < r_j < r_{j-1},\\
&r_{j-1} = r_j q_{j+1} + 0
\end{aligned}$$

The last nonzero remainder r_j, in the division process is equal to gcd(b,c).

Lemma:

If b=qc+r,then gcd(b,c)=gcd(c,r).

Proof:

If e=gcd(b,c),then the relations e/b and e/c together imply that

e/(b-qc), or d/r.

Thus,e is a common divisor of both c and r.On the other hand,if d is an arbitrary common divisor of c and r,then d/(qc+r),hence d/b.

This makes d is a common divisor of b and c,so that d≤e.

It now follows from the definition of gcd(c,r) that e=gcd(c,r).

Using this result,we obtain the system of equations,

gcd(b,c)=gcd(c,r_1)=…=gcd($r_{n-1,}r_n$)=gcd(r_n, 0)=r_n.

Result:

Consider the important theorem,

Given integers b and c,not both of which are zero,there exist integers x and y such that gcd(b,c)=bx+cy.

For determining the integers x and y,we consider the equation from Euclidean algorithm,

$$r_j = r_{j-2} - r_{j-1}q_j$$

i.e) $r_j = r_{j-2} - (r_{j-3} - r_{j-2}q_{j-1})q_j$

$$= r_{j-2} - r_{j-3}q_j + r_{j-2}q_{j-1}q_j$$

$$= (1 + q_{j-1}q_j)r_{j-2} + (-q_j)r_{j-3}.$$

This represents r_j as a linear combination of r_{j-2} and r_{j-3}.Continuing this process,we successively eliminate the remainders $r_{n-1}r_{n-2}\ldots r_2 r_1$ until a stage is reached where r_j=gcd(b,c) is expressed as a linear combination of b and c.

Let us consider the example of RSA using an example from Silverman.

Here,we are going to write the messages using only the alphabets in uppercase.Assigning the letters,

A=11

B=12

.

.

.

Z=36

Setting up RSA:

We select two large primes p’ and q’ such that

p’=12553 and q’=13007.

Therefore,m’=p’q’

=163,276,871.

And

(p’-1)(q’-1)=163,251,312.

Next,select the public key e’,at randomly,which satisfy the conditions,

(i) 1< e’ < (p’-1)(q’-1) and

(ii) Gcd(e’,(p’-1)(q’-1)) =1.

And then finds the inverse d’ of e’ modulo(p’-1)(q’-1),by extended

Euclidean algorithm.

Thus we have,

d’=145,604,785.

i.e) (145,604,785).79921-71282.(163,251,312)=1,

Which confirms that d' is indeed the inverse of e' mod(163,251,312).

Then the receiver,get the message in the following form,which is broken in blocks of atmost 9 digits,because m'=163,276,871 has 9 digits.

145387828 47164891 152020614 27279275 35356191.

After ,receiving the message the receiver decrypts the above message using his private key (d',m'),where d'=145,604,785,using the repeated squaring method,and we get,

$$145387828^{145,604,785} \equiv 30182523\ (mod\ 163{,}276{,}871)$$

$$47164891^{145,604,785} \equiv 26292524\ (mod\ 163{,}276{,}871)$$

$$152020614^{145,604,785} \equiv 19291924\ (mod\ 163{,}276{,}871)$$

$$27279275^{145,604,785} \equiv 30282531\ (mod\ 163{,}276{,}871)$$

$$35356191^{145,604,785} \equiv 122215 \quad (mod\ 163{,}276{,}871)$$

Finally we get the message

30182523 26292524 19291924 30282531 12215,

And converting into corresponding characters,we get the message

T H O M P S O N I S I N T R O U B L E.

It would be useful to encrypt the decoded message

30182523 26292524 19291924 30282531 12215,

using the public key e'=79921.

After decryption,we should get our original message

145387828 47164891 152020614 27279275 35356191.

A short notes on Prime numbers:

Definition:

An integer p'>1 is called a prime number,or a prime,in case there is no divisor d' of p' satisfying 1< d'< p'. If an integer a>1 is not a prime,it is called a composite number.

For example,2,3,5,7 and 11..,are primes, whereas 4,6,8,9 and12…, are composite.

Theorem:

Every integer n' larger than 1 can be expressed as a product of primes.(with perhaps only one factor).

Theorem:(The fundamental theorem of arithmetic,or the unique factorization theorem)

The factoring of any integer n'>1 into primes is unique apart from the order of the prime factors.

Theorem: (Euclid)

The number of primes is infinite.That is,there is no end to the sequence of primes 2,3,5,7,11,13,17,…

Importance of congruences in cryptography:

Congruences are playing an important role in the study of divisibility and also in Cryptography.Using congruence concept we send the messages in Cryptogrphy.

Definition: (Congruence)

If a and b are integers and n>0,we write a $\equiv$ b(mod n) to mean n/(b-a).

In words we write as " a is congruent to b modulo n"(mod n).

Example:

34≡ 2(mod 4)

40≡ 0(mod 8).

In Setting up the RSA public key cryptosytem,we should pick the prime numbers which are very large numbers for the purpose of high security .

Next,we will check that ,what will happen if we choose pseudoprimes instead of prime numbers?

Can we use pseudoprime numbers in Cryptography?

At first, we give some important notes on pseudoprime.

What is pseudoprime?

A pseudoprime is a probable prime (an integer that shares a property common to all prime numbers)that is not actually prime.Pseudoprime,a composite,or nonprime,number n that fulfills a mathematical condition that most other composite numbers fail.

For example,

let a=2,n=645,then a and n are relatively prime and 645 divides exactly into $2^{645} - 2$.

Thus,645=3*5*43,so it is a composite number.

Thus,645 is a Fermat pseudoprime to the base 2.

Note: 341 is a smallest Fermat pseudoprime.

Theorem:(Fermat' s Theorem)

Let p be a prime and suppose that p ∤ a.Then $a^{p-1} \equiv 1(mod\ p)$.

Corollary:

If p is a prime,then then $a^p \equiv a(mod\ p)$,for any integer a.

Lemma:

If p and q are distinct primes with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$,then $a^{pq} \equiv a(mod\ pq)$.

Definition:

The number Ø(m) is the number of positive integer less than or equal to m that are relatively prime to m.This Ø is called Euler's function.

Theorem:(Euler's Theorem)

If (a,m)=1,then $a^{\emptyset(m)} \equiv 1(mod\ m)$.

Note:

* Euler phi function, Ø(n)=n $\prod_{p/n}(1-\frac{1}{p})$.

* Simply ,we define

If n is prime, Ø(n)=n-1.

If n is composite, Ø(n)=n(1-$\frac{1}{p}$)(1-$\frac{1}{q}$),where p,q are factors.

Example:

1. If n=5 (prime),

then Ø(5)=5-1

=4

= number of positive integers less than 5 and is relatively prime to 5.

2. If n=10 (composite),

then Ø(10)=10$(1-\frac{1}{2})(1-\frac{1}{5})$

=10$(\frac{1}{2})(\frac{4}{5})$

=4

=number of positive integers less than 10 and is relatively prime to 10.

Euler's totient function:

Euler's totient function Ø(n) for an input n is

the count of numbers in {1,2,3,…n} that are relatively prime to n.

i.e) The numbers whose GCD (Greatest common divisor)with n is 1.

Use of Euler's Theorem in Cryptography:

*Euler's theorem underlies RSA cryptosystem which is widely used in internet communications.

* In cryptosystem ,Euler's theorem is used with n being a product of two large prime numbers,and the security of the system is based on the difficulty of factoring such an integer.

RSA with pseudoprimes:

In setup RSA public key algorithm ,we have the first condition as assigning two large prime numbers.There is a complication in the first step that when we assign two pseudoprimes,which were not prime.

Also, calculation of Ø in next step is wrong.

Why don't we choose p and q are pseudoprimes?

Let us check the cases .

Case(i):

Consider p and q are prime numbers.

Take p=7 and q=13

Setting up RSA:

(i) p=7 and q=13

(ii)n=pq=91

(iii) Ø(n)=6*12=72.

(iv) Choose the encryption(public) key e=11,such that 1<e<Ø(n)

(v)Find the decryption(private) key d such that,

d= $\frac{1+k\text{Ø}(\text{n})}{e}$.

=29.

Case(ii):

Consider p is pseudoprime and q is prime.

Take p=561 and q=283.Here p is a pseudoprime for base 2,

i.e) $2^{560} \equiv 1\, mod(561)$.

Here, the value of q is pseudoprime.so our calculation of Ø(n) becomes wrong.

i.e)n=pq=158763.

In this case ,we can set up the encryption key,but the reverse process the decryption key sometimes gives the original message sometime not.

Hence,by the RSA public key encryption often point out that large pseudoprimes are very rare.So it is not a problem to choose pseudoprimes,but when we select the pseudoprimes,decryption might succeed or it might fail.

REFERENCES

[1] Fundamentals of Cryptography,Introducing Mathematical and Algorithmic Foundations,Duncan Buell.

[2] Ivan Niven,Herbert S.Zuckerman,

Hugh L.Montgomery:An introduction to Theory of Numbers

[3] Elementary Number Theory,David M.BURTON.

[4] An introduction to Mathematical Cryptography,Jeffrey Hoffstein,Jill Pipher,Joseph H.Silverman.

[5] An introduction to Number Theory with Cryptography,James S.Kraft,Lawrence C.Washington.