International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

A Framework for Generating Multi Prime RSA using Sieve Function

Ariba Tariq, Ashish Bharti, Dalee Kumawat, Saima Naz
Motilal Nehru National Institute of Technology, Allahabad

ABSTRACT

RSA is the most widely used and tested public-key cryptosystem. In this paper, we have discussed the RSA algorithm, its complexity and security, the use of sieve function for the key generation process and its variant multi prime RSA which uses more than two prime numbers for the encryption process. It is based on a simple number theory idea; therefore it has been able to resist most cryptanalytic attacks. The idea makes use of a very clever fact that, while it is easy to multiply two large primes, it is extremely difficult to factorize their product. Thus, we have used the concept of multi prime RSA which is further more secure because it is difficult to factorize the key into more than two numbers. The primes themselves cannot be recovered from the product and are used for decryption. Two points need to be borne in mind however, while dealing with the RSA system: there is no formal proof whatsoever that factorization is intractable or is intractable in the special case needed for RSA, and that factorization is needed for the cryptanalysis of the RSA.

KEYWORDS

RSA, Sieve, Multi prime RSA

1. INTRODUCTION

1.1. CRYPTOGRAPHY

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography [1]is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc.

1.2. RSA

RSA is the most widely used and tested public-key cryptosystem. It stands for Rivest, Shamir, and Adleman. RSA was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a very simple number theory idea and therefore, it has been able to resist most cryptanalytic attacks. The idea uses a clever fact that, while it is easy to multiply two large primes, it is extremely difficult to factorize their product. Thus, the product can be publicized and is used as the encryption key. These primes cannot be recovered from the product and are used for decryption. Two points need to be kept in mind however, while dealing with the RSA system: there is no formal proof whatsoever that factorization is intractable or is intractable in the special case needed for RSA, and that factorization is needed for the cryptanalysis of the RSA. It involves three steps: Key Generation [2], Encryption, and Decryption.

1.2.1. KEY GENERATION

- Take two large prime numbers p and q(of the order of a few hundred bits).
- Compute their product n=p*q.
- Calculate Euler phi function (totient) φ (n) = (p-1)*(q-1).
- Choose e such that gcd (φ (n), e) =1; e will serve as public key.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

- Calculate d such that (e*d) ≡ 1(mod φ (n)); d will serve as private key.

1.2.2. ENCRYPTION ALGORITHM

- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as $C= P^e \bmod (n)$.
- In other words, the cipher text C is equal to the plaintext P multiplied by itself e times and then reduced modulo n. This means that C is also a number less than n.

1.2.3 DECRYPTION ALGORITHM

- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a cipher text C.
- Receiver calculate the plaintext $P =C^d \bmod n$.

2. LITERATURE REVIEW

The table below gives an account of the review done:

Table 1. Literature Review

Author	Year of Publication	Cryptographic Algorithm & Technical Details
Raushan Kumar Singh and Shobhit Kumar	2014	Optimization of RSA Algorithm
Sarthak R Patel, Prof. Khushbu Shah, Gaurav R Patel	2014	Study on Improvements in RSA Algorithm
M. Preetha, M. Nithya	2013	A Study and Performance of various Cryptographic Algorithm
B.Persis Urbana Ivy, PurshotamMandiwa. Mukesh Kumar	2012	A modified RSA cryptosystem based on ‘n’ prime numbers
Kumar R. Santosh, ChallaNarasimham, and PallamShettyS	2016	Cryptanalysis of Multi-prime RSA With Two Decryption Exponents

3. PROBLEM DESCRIPTION

During the study of the RSA algorithm, we identified that only two prime numbers are used, which is a fact already known by the attacker. But if more than two numbers are used for the encryption process, it becomes difficult for the attacker to factorize the key and find out the prime numbers used in the method. That is why we are using the concept of multiple prime numbers to enhance the security of the algorithm.

Further, we have used the Sieve function for key generation because it is easier and faster to implement.

4. PROPOSED ALGORITHM

4.1. SIEVE FUNCTION

The sieve of Eratosthenes was the first known means to test for primality and to factorize numbers. It simply verifies the divisibility of the number n to test by all the primes starting from 2 tosqrt(n) . It is very fast when testing with the first small primes but its computation time essentially grows linearly with n. It is practically unthinkable to use this kind of algorithm for generating primes as large as the ones used in cryptography.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Nevertheless, the sieve is nearly always used to rapidly eliminate the randomly chosen prime candidates having very small factors. The main point here is to find a superior bound on the number of small primes to use with the sieve to remain efficient. Choosing too many small primes will needlessly reduce the speed of the global process of prime number generation.

The function Q(x) where P_x is the set of all primes ≤ x may be defined as:

$Q(x) = \prod (1-1/p)$

For a n much larger than x , this function may be interpreted as the probability for n to be relatively prime with all primes in P_x. When sieving only with odd numbers, 2Q(x) gives the average ratio of composite numbers surviving to the sieve. Q(x) may thus also be used to size efficiently P_x when doing a sieve.

Practically, a sieve can be implemented by evaluating the GCD of the product of all the elements of P x with the number n to test. Indeed, in this case n is prime with all $p \in P_x$.

4.2. MULTI PRIME RSA

Multi-prime RSA is a variant of RSA in which the modulus is the product of more than two distinct primes. The advantage of Multi-prime RSA over standard RSA lies with the decryption process[4]. The encryption process is same as the standard RSA.

We begin by describing a simplified version multi-prime RSA. For any integer r≥2, r -prime RSA consists of the following three algorithms:

- Key Generation: Let N be the product of r randomly chosen distinct primes $p_1,....,p_r$ using the Sieve function. Compute Euler's totient function of N: $\varphi(N) = \prod(p_i - 1)$, $1 \le i \le r$. Choose an integer e, $1<e<\varphi(N)$, such that gcd(e, φ (N)) = 1. The pair (N, e) is the public key. Compute the unique $d \in Z_N$ such that $e*d \equiv 1 \bmod \varphi(N)$ (i.e., compute $d= e^{-1} \bmod \varphi(N)$). The private key is the pair (N, d).
- Encryption: For any message $m \in Z_N$, the cipher text is computed as $c= m^e \bmod (N)$.
- Decryption: For any cipher text $c \in Z_N$, the plaintext is recovered by computing $m= c^d \bmod (N)$.

We call N the multi-prime RSA modulus, the RSA modulus (when r=2), or simply the modulus. The integer e is called the public (or encrypting) exponent and d is called the private (or decrypting) exponent.

4.2.1. EXAMPLE

An example[3] illustrating the use of four primes to implement the RSA algorithm:

Let the prime numbers be:

p=2,q=3,r=5,s=17

- Calculate n=p*q*r*s
- n=2*3*5*17 =510
- Calculate f (n) =(p-1)*(q-1)*(r-1)*(s-1)
- f(510) =(2-1) (3-1) (5-1) (17-1) =128 ; f(n) =128
- Select any number 1<e<128. F(n) must not be divisible by e.
- Let e=3.
- Select d, multiplicative of e modf(n), d=43
- The public key is (n=510,e=3), private key is (n=510,d=43).

If the message is m=11.

- Encryption:

  $C=11^3 \bmod (510) =311$

  C=311
- Decryption using Standard Method:

  $M=311^{43} \bmod (510) =11$
- Decryption using Chinese Remainder Theorem:

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

$d_i = d(\text{ mod } (p_i - 1))$

$Mi = C^{di} (\text{mod } p_i)$

$M = M_i (\text{mod } p_i)$

Eg:

C=311,d=43,n=510

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 17$

So, d_i's:

- $d_1 = 43(\text{mod}(2-1))$
- $d_2 = 43(\text{mod}(3-1))$
- $d_3 = 43(\text{mod}(5-1))$
- $d_4 = 43(\text{mod}(17-1))$

And, M_i's:

- $M_1 = (311)^0 \text{mod } 2$
- $M_2 = (311)^1 \text{ mod } 3$
- $M_3 = (311)^2 \text{ mod } 5$
- $M_4 = (311)^{11} \text{ mod} 17$

$M = M_i \text{ mod } p_i$

- $M = 1(\text{mod } 2)$
- $M = 2(\text{mod } 3)$
- $M = 1(\text{mod } 5)$
- $M = 11(\text{mod } 17)$

Applying CRT, $M = \sum a_i k_i y_i \text{ modk}$

Let $K = \prod p_i = 510$; $k_i = K / p_i$

- $k_1 = 255$
- $k_2 = 170$
- $k_3 = 102$
- $k_4 = 30$

Furthermore,

- $y_1 = k_1^{-1} \text{ mod } p_1$
- $y_2 = k_2^{-1} \text{ mod } p_2$
- $y_3 = k_3^{-1} \text{ mod } p_3$
- $y_4 = k_4^{-1} \text{ mod } p_4$

$M = (1*255*1+2*170*2+1*102*3+11*30*4) \text{ mod}510 = 2561(\text{mod}510) = 11$ (Message)

5. RESULTS AND DISCUSSION

While implementing the above stated methodology, we came across various advantages of using the multi prime RSA. The advantages are as follows:

The first advantage is “time”; using the Chinese Remainder Theorem(CRT) and performing calculations in parallel, the number of bit operations needed to decrypt a cipher text is at most $3/2r^3 (\log_2 N)/3$ (using standard arithmetic). So, the time needed for decryption decreases with each additional prime in the modulus.

The second advantage is “space”; again, using the Chinese Remainder Theorem(CRT), the space needed for all decryption computations until the very last (recombining step) require only $(\log_2 p_r)$ space, where p_r is the largest prime in the modulus. If all the primes are roughly $(\log_2 N)/r$ -bits large (balanced primes), the space required decreases with each additional prime added to the modulus.

REFERENCES

[1] Malhotra, Mini, and Aman Singh. "Study of various cryptographic algorithms." *IJSER* 1.3 (2013): 77-88.

[2] Patel Sarthak R., Prof. Khushbu Shah, Patel GauravR.."Study on Improvements in RSA Algorithm", International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939, Vol.1, Issue 3, pp.142 - 145, Dec 2014

[3] Ivy, B. Persis Urbana, PurshotamMandiwa, and Mukesh Kumar. "A modified RSA cryptosystem based on 'n'prime numbers."*International Journal Of Engineering And Computer Science* 1.2 (2012): 63-66.

[4] Santosh, Kumar R., ChallaNarasimham, and P. Shetty. "Cryptanalysis of multi-prime RSA with two decryption exponents."*International Journal of Electronics and Information Engineering* 4.1 (2016): 40-44.

[5] Preetha, M., and M. Nithya. "A study and Performance Analysis of RSA Algorithm."*IJCSMC* 2 (2013): 126-139.