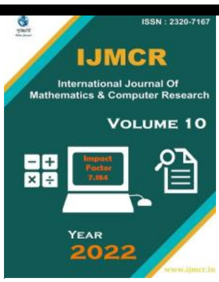
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 10 Issue 02 February 2022, Page no. – 2555-2558

Index Copernicus ICV: 57.55, Impact Factor: 7.184

DOI: 10.47191/ijmcr/v10i2.01



Remodeled RSA Algorithm for Messages of Length Two Employing G- Primes

J. Kannan[1], Manju Somanath[2], M. Mahalakshmi[3], K. Raja[4]

[1,3]Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University, Madurai), Sivakasi – 626 124, Tamil Nadu, India.

[2,4]Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University, Trichy), Trichy- 620001.

ARTICLE INFO

01 February 2022

Corresponding Author:
J. Kannan

ABSTRACT

Now - a- days, the exchange of sensitive information, such as credit card numbers, over the internet is common practice. Protecting data and electronic systems is crucial to our way of living. Cryptography deals with the study of communication over a channel may not be secure and problems related with them. One such well known algorithm is RSA algorithm. This paper displays the classical RSA algorithm and modifies the work in generation of keys. There will be two assignments for the alphabets. Here the only interest is on messages with two letters.

KEYWORDS: RSA Algorithm; Remodeled RSA algorithm; Encryption decryption algorithm; Gaussian primes; Cryptography.

I. INTRODUCTION

Cryptography is a concept of protecting information and conversations which are transmitted through a public source, so that the intended persons only read and process it. There are several encryption and decryption algorithm which involves mathematical concepts to provide more security to the text which has to be shared through a medium.

RSA algorithm is a well- known asymmetric cryptography algorithm which uses public and private keys. Public key is visible to all but private key is used by intended persons only. The idea of this algorithm depends on the fact that factorization of large integers into primes is hard. The larger the chosen primes, the more is the security. Initially, an example dealing RSA algorithm was provided.

Already there are some works regarding the Gaussian integer application on RSA algorithm [1,2,3]. Motivated by them, this work was built. The main idea in this paper is to just remodel the classical RSA algorithm by using Gaussian primes. Making use of Gaussian primes with large real and imaginary parts will leads to a difficulty in factorizing. Also for the process of key generation, assignment based on Gaussian primes is employed whereas for encryption, usual alphabet assignment is used. Furthermore, the differences between both the algorithms were provided. This paper was developed mainly for sharing two lettered messages.

II. PRELIMINARIES

Euler ϕ function on $\mathbb{N}$**:** Euler phi function $\varphi(n)$ is defined on natural numbers which counts the numbers which are less than n and prime to it.

1. $\varphi(n) = |\{k \in \mathbb{N}: k < n \text{ and } (k, n) = 1\}|$.
2. For a prime p, $\varphi(p) = p - 1$.
3. If $n = pq$ and $(p, q) = 1$, then $\varphi(n) = (p-1)(q-1)$.

Gaussian integers:

Gaussian integers are complex numbers $z = a + ib$ where a, b are integers and it is denoted by $\mathbb{Z}[i]$. The norm of $z = a + ib$ is given by $N(a + ib) = a^2 + b^2$.

Gaussian primes (G- primes):

$z = a + ib$ is a Gaussian prime if one of the following holds:

1. If $a \neq 0, b \neq 0$, then $a + ib$ is a Gaussian prime if and only if $N(a + ib) = a^2 + b^2$ is an integer prime.
2. If $a \neq 0$, then bi is a Gaussian prime if $|b|$ is an integer prime and $|b| \equiv 3(mod\ 4)$.
3. If $b \neq 0$, then a is a Gaussian prime if $|a|$ is an integer prime and $|a| \equiv 3(mod\ 4)$.

Note: If p is an integer prime such that $p \equiv 1(mod\ 4)$, then $p = x^2 + y^2$. Thus $x + iy, x < y$ is a Gaussian prime corresponding to p.

A. RSA Algorithm

Generating public key:

1. Select two integer primes p and q.
2. Find n such that $n = pq$ and $\varphi(n)$.
3. Choose e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
4. The public key is given by (n, e)

Generating private key:

The private key is d which is found from $ed \equiv 1(mod\ \varphi(n))$.

Encryption:

1. Consider the two lettered message which have to be sent. Convert the letters to numbers by assigning $1 - 26$ for $A - Z$ and take it as m.
2. Solve $c \equiv m^e(mod\ n)$for c. This c is the encrypted data.

Decryption:

1. Solve $m \equiv c^d(mod\ n)$ for m which is the decrypted data.
2. Convert the digits to alphabets.

All paragraphs must be indented as well as justified, i.e. both left-justified and right-justified.

Example 1:

Consider the message "HI".

Generating public key:

1. Let $p = 61$ and $q = 71$.
2. $n = pq = 4331, \varphi(n) = 4200$.
3. Choose $e = 11$.

The public key is $(4200{,}11)$.

Generating private key:

$$ed \equiv 1\big(mod\ \varphi(n)\big) \Longrightarrow 11d \equiv 1(mod\ 4200)$$
$$\Longrightarrow d = 2291.$$

Encryption:

1. The message to be sent is "HI". From its positions, one can see that $m = 89$.
2. $c \equiv m^e(mod\ n) \Longrightarrow c \equiv 89^{11}(mod\ 4331)$
$$\Longrightarrow c = 1802.$$

Decryption:

1. $m \equiv c^d(mod\ n) \Longrightarrow m \equiv 1802^{2291}(mod\ 4331)$

$\Longrightarrow m = 89.$

2. Converting it to alphabets one can get "HI".

III. REMODELED RSA ALGORITHM FOR TWO LETTERED MESSAGES

Here is a little modified RSA algorithm which employs Gaussian primes. Some places of RSA algorithm is modified and this algorithm is created to improve the secrecy of messages. The discussion is made only for messages of length 2. Before entering into the algorithm, the differences of both algorithms are presented.

S. No	RSA Algorithm	Modified RSA Algorithm
1.	For a message to be sent, there is only one assignment of digits which is made only on encryption phase.	There are two assignments for messages. One is made when generating public key and other happens on encryption phase.
2.	e is chosen such that it is relatively prime to $\varphi(n)$	$e$is chosen such that it is relatively prime to $\varphi\big(N(n)\big)$ where N is the norm of Gaussian integer.
3.	Modulo n is used on both encryption and decryption.	Modulo $N(n)$, ie., norm of n is used on encryption and decryption.

B. Assignments:

Assignment – 1:

This is used in public key generation. Let $\{\mathrm{p_n}\}$ be the sequence of all integer primes in ascending order. Make a short- term assignment by fixing any 26 elements in $\{\mathrm{p_n}\}$to $\mathrm{A - Z}$. If the assigned prime p is of the form $4\mathrm{k} + 3$, the alphabet is given the name $\mathrm{p} + 0\mathrm{i}$. If the assigned prime p is of the form $4\mathrm{k} + 1$, then $\mathrm{p} = \mathrm{x}^2 + \mathrm{y}^2$. So name the alphabet as $\mathrm{x} + \mathrm{iy}$ where $\mathrm{x} < y$.

Assignment – 2:

This is used on encryption phase. It is the usual assignment for $A\ to\ Z$ as $1\ to\ 26$.

C. Modified RSA Algorithm:

Generating public key:

1. Assign positions of alphabets by Assignment – 1.
2. Consider two G- primes p and q such that p and q are the positions of alphabets on the message to be sent based on Assignment – 1.
3. Find n such that $\mathrm{n} = \mathrm{pq}$and $\mathrm{N(n)}$. Also find $\varphi\big(\mathrm{N(n)}\big)$.
4. Choose e such that $1 < e < \varphi\big(\mathrm{N(n)}\big)$ and gcd $\Big(\mathrm{e}, \varphi\big(\mathrm{N(n)}\big)\Big) = 1$.

The public key is given by (n, e).

Generating private key:

The private key is d *which is found from* $ed \equiv 1\Big(mod\ \varphi\big(N(n)\big)\Big)$.

Encryption

1. Consider the two lettered message which have to be sent. Convert the letters to numbers based on Assignment - 2and take it as m.
2. Solve $\mathrm{c} \equiv \mathrm{m^e(mod\ N(n))}$for c. This c is the encrypted data.

Decryption

1. Solve $\mathrm{m} \equiv \mathrm{c}^{\mathrm{d}}(\mathrm{mod\,N(n)})$ for m which is the decrypted data.
2. Convert the digits to alphabets based on Assignment – 2.

Example 2:

Consider the message "HI"

Generating public key:

1. Suppose the short- term assignment is taken as

2	3	5	7	11	13	17	19	23	29	31	37	41
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
43	47	53	59	61	67	71	73	79	83	89	97	101

This gives Assignment 1.

2.

A	**B**	**C**	**D**	**E**
$1+i$	$3+0i$	$1+2i$	$7+0i$	$11+0i$
F	**G**	**H**	**I**	**J**
$2+3i$	$1+4i$	$19+0i$	$23+0i$	$2+5i$
K	**L**	**M**	**N**	**O**
$31+0i$	$1+6i$	$4+5i$	$43+0i$	$47+0i$
P	**Q**	**R**	**S**	**T**
$2+7i$	$59+0i$	$5+6i$	$67+0i$	$71+0i$
U	**V**	**W**	**X**	**Y**
$3+8i$	$79+0i$	$83+0i$	$5+8i$	$4+9i$
Z				
$1+0i$				

Choose $p = 19 + 0i$ and $q = 23 + 0i$.

3. $n = pq = 437 + 0i$, $N(n) = 437^2 = 190969$. $\varphi(N(n)) = \varphi(190969) = 173052$.
4. Choose $e = 7$.

The public key is $(n, e) = (437 + 0i, 7)$.

Generating private key:

$$ed \equiv 1\left(mod\ \varphi(N(n))\right) \Longrightarrow 7d \equiv 1(mod\ 73052)$$
$$\Longrightarrow d = 98887$$

Encryption:

1. The message to be sent is "HI". From its positions (Assignment-2), one can see that $m = 89$.
2. $c \equiv m^e(mod\ N(n)) \Longrightarrow c \equiv 89^7(mod\ 190969)$
$$\Longrightarrow c = 117620$$

Decryption:

1. $m \equiv c^d(mod\ N(n))$
$$\Longrightarrow m \equiv 117620^{98887}(mod\ 190969) \Longrightarrow m = 89$$
2. Converting it to alphabets one can get "HI"

Example 3:

Consider the message "TN".

Generating public key:

1. Suppose the short- term assignment is taken as

3	7	13	19	29	37	43	53	61	71
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
79	89	101	107	113	131	139	151	163	173
191	197	2	7	11	17				
U	**V**	**W**	**X**	**Y**	**Z**				

2. Assignment -1 as

A	**B**	**C**	**D**
$3+0i$	$\mathbf{7+0i}$	$\mathbf{2+3i}$	$\mathbf{19+0i}$
D	**F**	**G**	**H**
$2+5i$	$1+6i$	$43+0i$	$2+7i$
I	**J**	**K**	**L**
$5+6i$	$71+0i$	$79+0i$	$5+8i$
M	**N**	**O**	**P**
$1+10i$	$107+0i$	$163+0i$	$2+13i$
Q	**R**	**S**	**T**
$191+0i$	$1+14i$	$1+i$	$1+2i$
U	**V**	**W**	**X**
$11+0i$	$1+4i$		
Y	**Z**		

Choose $p = 2 + i13$ and $q = 107 + 0i$.

3. $n = pq = 214 + 139i, N(n) = 65117$. $\varphi(N(n)) = \varphi(65117) = 60096$.
4. Choose $e = 5$.

The public key is $(214 + 139i, 5)$.

Generating private key:

$$ed \equiv 1\left(mod\ \varphi(N(n))\right) \Longrightarrow 5d \equiv 1(mod\ 60096)$$
$$\Longrightarrow d = 48077$$

Encryption:

1. The message to be sent is "TN". From its positions (AS-2), one can see that $m = 2014$.
2. $c \equiv m^e(mod\ N(n)) \Longrightarrow c \equiv 2014^5(mod\ 65117)$
$$\Longrightarrow c = 11751$$

Decryption:

1. $m \equiv c^d(mod\ N(n)) \Longrightarrow m \equiv 11751^{48077}(mod\ 65117)$

$\Longrightarrow m = 2014.$

2. Converting it to alphabets one can get "TN".

IV. CONCLUSION

In this paper, the classical RSA algorithm was displayed along with an illustration. Then its remodeled form is provided with the same example which was dealt previously. Decryption is difficult in large cases since the prime factorization is hard. Here the concentration is only on messages of length two. One can initiate to extend this algorithm for messages of any finite length.

REFERENCES

1. Elkamchouchi, H., Elshenawy, K., &Shaban, H. 2002, Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In The 8th International Conference on Communication Systems, 2002, 91-95.
2. El-Kassar, A. N., Haraty, R. A., Awad, Y. A., & Debnath, N. C. 2005, Modified RSA in the Domains of Gaussian Integers and Polynomials Over Finite Fields. In CAINE 298-303.
3. Manju Somanath, J. Kannan and K. Raja, 2017 “On a Class of Solutions for a Diophantine Equation of Second Degree”, International Journal of Pure and Applied Mathematics, 117(12), 55 – 62.
4. Manju Somanath and J. Kannan, 2016 “Congruum Problem”, International Journal of Pure and Applied Mathematical Sciences (IJPAMS), 9(2), 123-131.
5. Manju Somanath, K. Raja, J. Kannan and M. Mahalakshmi, “On A Class of Solutions for A Quadratic Diophantine Equation”, Advances and Applications in Mathematical Sciences, 19(11), 1097 – 1103.
6. Manju Somanath, J. Kannan and K. Raja, 2016 “Lattice Points of an Infinite Cone $x^2 + y^2 = (\alpha^{2n} + \beta^{2n})z^2$”, International Journal of Mathematical Trends and Technology, 38(2), 95 - 98.
7. Manju Somanath, K. Raja, J. Kannan and V. Sangeetha, “On the Gaussian Integer Solutions for an Elliptic Diophantine Equation”, Advances and Applications in Mathematical Sciences, 20(5), 2021, 815 – 822.
8. Manju Somanath, K. Raja, J. Kannan and B. Jeyashree, “Non Trivial Integral Solutions of Ternary Quadratic Diophantine Equation”, Advances and Applications in Mathematical Sciences, 19(11), 2020, 1105 – 1112.
9. Manju Somanath, J. Kannan and K. Raja, 2017 “On Polynomial Solutions of Quadratic Equation”, International Journal of Mathematics and its Applications (IJMAA), 5(4 – F), 839 – 844.
10. Pradhan, S., & Sharma, B. K. 2014, A modified variant of RSA algorithm for Gaussian integers. In Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28-30, 2012 (pp. 183-187). Springer, New Delhi.
11. Trappe, W., & Washington, L. C. 2006, Introduction to Cryptography. Prentice Hall.