Renovated RSA Algorithm for Sending Secret Numbers using Primes and 3-Length Words Employing Gaussian Primes

Janaki G[*] and Gowri Shankari A[*1]

[*]*Associate Professor, Cauvery College for Women (Autonomous),*
(Affiliated to Bharathidasan University),Trichy – 18, India
[*1]*Assistant Professor, Cauvery College for Women (Autonomous),*
(Affiliated to Bharathidasan University),Trichy – 18, India

Abstract: Nowadays, it's normal practice to communicate sensitive information over the internet, including secret codes and CSV numbers for debit and credit cards. Electronic systems and data security are essential to our way of life. Communication across an insecure connection might result in issues. The RSA algorithm is one such popular algorithm. This paper alters the process of key generation while displaying the classical RSM algorithm. There will be two assignments for the alphabets. Here the only interest is in three lettered messages and three digit numbers.

Keywords: Cryptography, Encryption, Decryption.

MSC2020:11B37, 11C20, 11D09, 11T71.

1. Introduction

Early cryptography methods were mostly employed in the military. Maintaining information privacy has taken on more importance with the introduction of the internet and all its ancillary technologies that rely on networks.

Currently, practically all modern coding schemes can be supported by number theory [1,9,13]. Coding advanced significantly in the twentieth century.

G. Janaki and A. Gowri Shankari describe intriguing coding and decoding techniques based on the solutions to the Pell equation discovered in [10,11] and the new matrix Q8*. The authors also describe a coding and decoding strategy that uses large prime numbers in Gaussian integers to ensure great security [12].The RSA algorithm is based on the fact that finding prime factors for integers is difficult and takes a lot of time. The use of the Gaussian integer in the RSA method has previously received significant attention [2–8].Their drive constituted the foundation for this work.

This paper's basic idea is to simply rewrite the conventional RSA method using Gaussian primes. Factoring will be challenging when using Gaussian primes with strong real and imaginary parts. Additionally, while the standard alphabet is utilized for encryption, a task based on Gaussian primes is used for key creation. This paper was primarily created for exchanging secret codes or numbers.

Preliminaries:

Euler's totient function on natural numbers N :

- $\phi(n) = u \in \mathrm{N}$, if $u < n$ and $(u,n) = 1$
- $\phi(p) = p-1$, where p is prime
- $\phi(n) = (s-1)(t-1)$, if $n = st$ and $(s,t) = 1$

RSA Cryptography:
Making an open key:

1. Select two prime numbers say s and t
2. Find $n = st$ and $\phi(n)$.
3. Select g, provided $1 < g < \phi(n)$ and $(g, \phi(n)) = 1$
4. The open key is (n, g)

Making a private key:
The private key is j obtained by $gj \equiv 1(\bmod\, \phi(n))$

Encryption:

- Take into account the codes or numbers that must be sent as c.
- Find the encrypted data $e \equiv c^g\, (\bmod\, n)$ for e .

Decryption:

- Calculate $c \equiv e^j\, (\bmod\, n)$, which is the decrypted data.

Example: 1.1 for 3 digit numbers

Consider the Debit or Credit card CSV number is “255”

Making an open key:

Let $s = 13, t = 29$
$\therefore n = st = (13)(29) = 377$, Composite number
Now $\phi(n) = (s-1)(t-1) = 336$
Choose $g = 89$. Also $(89,336) = 1$.
Open key is $(377,89)$.

Making a private key:

$$gj \equiv 1(\bmod\, \phi(n))$$
$$\Rightarrow 89j \equiv 1(\bmod\, 336)$$
$$\Rightarrow j = 185$$

Encryption:

The message to be sent is “255”
Hence $c = 255$.
Now $e \equiv c^g\, (\bmod\, n)$
$\equiv 255^{89}\, (\bmod\, 377)$
$\equiv 112\, (\bmod\, 377)$
$\therefore e = 112.$

Decryption:

$c \equiv e^j\, (\bmod\, n)$
$\equiv 112^{185}\, (\bmod\, 377)$
$\equiv 255(\bmod\, 377)$
Therefore, our message is 255.

Example: 1.2

Consider the Debit or Credit card CSV number is “144”

Making an open key:
Let $s = 11, t = 29$

$\therefore n = st = (11)(29) = 319$, Composite number

Now $\phi(n) = (s-1)(t-1) = 280$

Choose $g = 23$. Also $(23,280) = 1$.

Open key is $(319,23)$.

Making a private key:

$$gj \equiv 1(\bmod \phi(n))$$
$$\Rightarrow 23j \equiv 1(\bmod 280)$$
$$\Rightarrow j = 207$$

Encryption:

The message to be sent is “144”
Hence $c = 144$.

Now $e \equiv c^g (\bmod n)$

$\equiv 144^{23} (\bmod 319)$

$\equiv 144 (\bmod 319)$

$\therefore e = 144.$

Decryption:

$c \equiv e^j (\bmod n)$

$\equiv 144^{207} (\bmod 319)$

$\equiv 144(\bmod 377)$

Therefore, our message is 144.

2. Renovated RSA Algorithm for three lettered messages

Two text assignments fall under this kind. One is used to create open keys, and the other is used to encrypt data.

Assignment 1:
This is used to generate open keys. The assignment is a Gaussian prime range from *a* toz.

Assignment 2:
The encryption phase will utilise this. It is customary to designate *a* tozas 1 to 26.

Modified RSA Algorithm:

Making anopen key:

- Use Assignment 1 to assign alphabetical positions.
- Consider three Gaussian primes r, s and t such that r, s and t are the place of alphabets on the text to be sent based on Assignment 1
- Find $N(n) = rst$. Noted that if any one or more of r, s, t is of the form $x + iy$, then find its norm as $x^2 + y^2$ and then multiply it
- Find $\phi(N(n))$
- Select g, provided $1 < g < \phi(N(n))$ and $(g, \phi(N(n)) = 1$
- The open key is $(N(n), g)$

Making a private key:

The private key is j which is calculated from $gj \equiv 1(\bmod \phi(N(n)))$

Encryption:

- Take into account the required three-letter message.
- Based on Assignment 2, convert the letters to numbers and use it as c
- Find encrypted data $e \equiv c^{g} (\bmod N(n))$ for e.

Decryption:

- Calculate the decrypted data $c \equiv e^{j} (\bmod N(n))$. .
- In accordance with Assignment 2, change the numerals into alphabets.

Example: 2.1 for prime assignment:

Consider the text "bee"

Gaussian Assignment: 1 for first 26 prime numbers

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*
1+i	*3+0i*	*1+2i*	*7+0i*	*11+0i*	*2+3i*	*1+4i*	*19+0i*	*23+0i*
j	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*
2+5i	*31+0i*	*1+6i*	*4+5i*	*43+0i*	*47+0i*	*2+7i*	*59+0i*	*5+6i*
s	*t*	*u*	*v*	*w*	*x*	*y*	*z*	
67+0i	*71+0i*	*3+8i*	*79+0i*	*83+0i*	*5+8i*	*4+9i*	*1+10i*	

Usual Assignment: 2

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
14	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*

Making an open key:

Choose $r = 3 + 0i, s = 11 + 0i, t = 11 + 0i$

$\therefore N(n) = rst = (3)(11)(11) = 363$

Now $\phi(N(n)) = \phi(363) = 220$

Choose $g = 23$. Also $(23,220) = 1$.

Open key is $(363,23)$.

Making a private key:

$$gj \equiv 1(\bmod \phi(N(n))$$
$$\Rightarrow 23j \equiv 1(\bmod 220)$$
$$\Rightarrow j = 67$$

Encryption:

The message to be sent is "bee"
Using Assignment:2, $c = 255$.

Now $e \equiv c^g \,(\text{mod}\, N(n))$

$\equiv 255^{23} (\text{mod}\, 363)$

$\equiv 327\, (\text{mod}\, 363)$

$\therefore e = 327.$

Decryption:

$c \equiv e^j \,(\text{mod}\, N(n))$

$\equiv 327^{67} (\text{mod}\, 363)$

$\equiv 255 (\text{mod}\, 377)$

$\therefore c = 255$

Converting *c*, into alphabets one can get “bee”.

Example: 2.2(Consider the Assignments 1 &2 same as Example 2.1)

Consider the text “fit”

Making an open key:

Choose $r = 2 + 3i, s = 23 + 0i, t = 71 + 0i$

$\therefore N(n) = (13)(23)(71) = 21229$

Now $\phi(N(n)) = \phi(21229) = 18480$

Choose $g = 17$. Also $(17,18480) = 1$.

Open key is $(21229, 17)$.

Making a private key:

$gj \equiv 1 (\text{mod}\, \phi(N(n))$

$\Rightarrow 17j \equiv 1 (\text{mod}\, 18480)$

$\Rightarrow j = 17393$

Encryption:

The message to be sent is “fit”

Using Assignment: 2, $c = 6920$.

Now $e \equiv c^g \,(\text{mod}\, N(n))$

$\equiv 6920^{17} (\text{mod}\, 21229)$

$\equiv 21213 (\text{mod}\, 21229)$

$\therefore e = 21213.$

Decryption:

$c \equiv e^j \,(\text{mod}\, N(n))$

$\equiv 21213^{17393} (\text{mod}\, 21229)$

$\equiv 6920 (\text{mod}\, 21229)$

$\therefore c = 6920$

Converting *c*, into alphabets one can get “fit”.

3. Conclusion

The classical RSA technique was demonstrated in this paper with examples for transmitting CSV Numbers. Later its renovated form is given with other examples with length three messages. One can extend its length with different Gaussian assignments.

References

[1]. Dickson, L. E. History of the theory of numbers, Chelsia Publishing Co., New York, Vol.2, 1952.

[2]. Elkamchouchi, H.; Elshenawy, K.; Shaban, H. Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In the 8th International Conference Systems, 2002, 91-95.

[3]. El- Kassar, A. N.; Haraty, R.A.;Awad, Y. A.; Debnath, N. C. Modified RSA in the Domains of Gaussian Integers and Polynomials Over Finite Fields. In CAINE 2005, 298-303.

[4]. May, C.A. Application of the Euler Phi Function in the Set of Gaussian Integers, 2015.

[5]. Pradhan, S.; Sharma, B. K. 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, 183-187, Springer, New Delhi.

[6]. Sumeyra, U. C. A. R.; Nihal T. A. S.; Ozgur N. Y. A new application to coding theory via Fibonacci and Lucas numbers, Mathematical Sciences and Applications E-Notes, 7(1), 2019, 62-70

[7]. Tas, N.; Ucar, S.; Ozgur, N. Y.; Kaymak, O.O. A new coding/ decoding algoirithm using Fibonacci numbers, Discrete Mathematics, Algorithms and Applications, 10(2), 2018, 1850028.

[8]. Thiagarajan, K.; Balasubramanian, P.; Nagaraj, J.;Padmashree, J. Encryption and decryption algorithm using algebraic matrix approach. In Journal of Physics: Conference Series (Vol. 1000, No. 1, p. 012148). IOP Publishing, 2018.

[9]. Trappe, W.; Washington, L. C. Introduction to Cryptography, Prentice Hall, 2006.

[10]. Janaki, G.; Gowri Shankari, A.; Cryptographic Algorithm Using Binary Quadratic Equation $x^2 - 7y^2 = 1$ with Exponent Assignment of Alphabets, Aryabhatta Journal of Mathematics and Informatics, 14(2), 2022, 203-208.

[11]. Janaki, G.; Gowri Shankari, A.; Algebraic coding theory using Pell equation x^2-8y^2=1, Ratio Mathematica, Volume 46, 2023, 101-108

[12]. Janaki, G.; and Gowri Shankari, A.;A Cryptographic Algorithm Based on Large Gaussian Primes and Primes,Research Highlights in Mathematics and Computer Science, B P International,Volume 2, 2022, 65-78.

[13]. Janaki, G.;and Gowri Shankari, A.; Encryption and Decryption Algorithm Using Balancing Numbers, Explorations in Diophantine Equations, B P International, 2023, 109-117.