International Journal of Information & Network Security (IJINS)
Vol.2, No.4, August 2014, pp. 322~326
ISSN: 2089-3299

A Modified Variant of RSA Algorithm for Gaussian Integers

SushmaPradhan*, Birendra Kumar Sharma**
* School of Studies in Mathematics, Pt. Ravishankar Shukla University
** School of Studies in Mathematics, Pt. Ravishankar Shukla University

Article Info

Article history:

Received Jun 15th, 2013
Revised Jun 30th, 2013
Accepted Jul 28th, 2013

Keyword:

RSA ,
Public-key cryptosystem,
Gaussian integers,
Multi-prime RSA.

ABSTRACT

In this paper, we propose a modified RSA variant using the domain of Gaussian integers providing more security as compare to the old one. The proposed varaint has significant specifics: the encryption is substantially faster than the decryption. There are certain settings where the sender has limited time to transmit the message: visual images or video, and receiver do not have such restriction. For instance, the sender is a system that urgently needs to transmit information prior to either collision with a target or before it is destroyed by a hostile action.

Corresponding Author:
Sushma Pradhan
School of Studies in Mathematics,
Pt. Ravishankar Shukla University,
Raipur, Chhattisgarh, India.
Email: sushpradhan@gmail.com

1. INTRODUCTION

RSA system is the one of most practical public key password systems. Inaddition to other domain, it has successfully provided security to the electronic based commerce. Encryption of plaintext in asymmetric key encryption is based on a public key and a corresponding private key.Document authentication and digital signature are other advantages of RSA public keycryptosystem.RSA provides security to the plaintext based on factorization problem. There are PKC's other than RSA.Those are Elgamal and Rabin'sPKC's. These PKC's provide security based discrete logarithm problem.

The classical RSA cryptosystem is described in the setting of the ring Zn, the ring of integers modulo a composite integer n = p q, where p and qare two distinct odd prime integers. Many aspects of arithmetic's over thedomain of integers can be carried out to the domain of Gaussian integersZ[i], the set of all complex numbers of the form a + bi, where a and b areintegers. The RSA cryptosystem was extended domain of Gaussian Integers in the papers [7] and [8]. In [7] and [8] the advantages of such extension ofRSA were briefly stated in these papers.

Now in this paper, another fast variants of RSA cryptosystems is proposed using arithmetic's modulo of Gaussian integers. Proposed scheme provides more security with same efficiency. Before doing so, in next section, we review the classical RSA PKC. Next, we introduced Gaussian integers and its properties in section 3. In section 4, we present a variant of RSA scheme based on factorization of Gaussian integers with a suitable example. Finally, we conclude with security analysis and comparison with the standard method.

2. CLASSICAL RSA PUBLIC KEY CRYPTOSYSYTEM

We begin with brief review of the classical RSA pubic key system and refer to [16] for more information. The Key generation, Encryption and Decryption of RSA are as follows:

2.1. Key Generation: To generate keys for the RSA scheme receiver R chooses two large primes p and q and computes n = pq. He then chooses an integer e less than and relatively prime to $\phi(n)$ and computes an integer d such that $ed = 1 \bmod \phi(n)$. The public key and the secret key for the receiver R is (e, n) and d respectively. Plaintext and the ciphertext space is 0, 1, 2… n − 1.

2.2. Encryption: To encrypt any plaintext M, the sender S computes $C = M^e \pmod n$ by using the public key of R and sends the ciphertext C to the receiver R.

2.3. Decryption: After getting the ciphertext C the receiver R computes $C^d \pmod n = M$ by using his secret key d.

3. GAUSSIAN INTEGERS

Gaussian integer is a complex number a + bi where both a and b is integers: Z[i] = a+bi: a, b∈ Z. Gaussian integers, with ordinary addition and multiplicationof complex numbers, form an integral domain, usually written as Z[i]. The norm of aGaussian integer is the natural number defined $|a + bi| = a^2 + b^2$.
Gaussian primesare Gaussian integer's z = a+bi satisfying one of the following properties:

1. If both a and b are nonzero then, (a+bi) is a Gaussian prime iff $(a^2 + b^2)$ is an ordinary prime.

2. If a = 0, then bi is a Gaussian prime iff $|b|$ is an ordinary prime and $|b|$ =3(mod4).

3. If b = 0, then a is a Gaussian.

J.T. Cross [2] gave a full description for complete residue systems modulo prime powers of Gaussian integers.

4. RSA ALGORITHM OVER THE FIELD OF GUASSAIN

A Gaussian prime is a Gaussian integer that cannot be expressed in the form of the product of other Gaussian integers. The concept of Gaussian integer was introduced by Gauss who proved its unique factorization domain. In paper [8] the RSA is extended into the field of Gaussian integers. It is presented as follows:

Key Generation:
Generate two large Gaussian primes P and Q. Compute N = PQ.
Compute ϕ (N) = ($|p|$-1)($|q|$-1). Select a random integer e such that 1 < e < ϕ (N) and gcd (e, ϕ (N) = 1.
Compute $d = e^{-1} \bmod \phi(N)$. Pair N and e is a publickey, and d is the private key.

Encryption:
Given a message M (represented as a Gaussian integer) compute ciphertext
$C := m^e \pmod n$.

Decryption:
Compute the original message $M := c^d \pmod n$.

5. PROPOSED NEW SCHEME

Now we propose the algorithms for the variant of RSA cryptosystem in Z[i] as below:

Key Generation:
Generate b distinct large Gaussian primes α, β and γ each n/b bits long.

Compute $N = \alpha\beta\gamma$.

Compute ϕ (N) = $(|\alpha|-1)(|\beta|-1)(|\gamma|-1)$.

Select a random integer e such that 1 < e < ϕ (N) and gcd (e, ϕ (N) = 1.

Compute $d = e^{-1} \bmod \phi(N)$.

Pair (N, e) is a public key, and $(\alpha, \beta, \gamma, d)$ is the private key.

Encryption:

Given a message M (represented as a Gaussian integer) compute cipher text

$C = m^e (\bmod N)$

Decryption:

Compute the original message $M = c^d (\bmod N)$.

Following is the example in support of proposed algorithm.

Example:

Key generation

Let's select α = 19 and β = 5 and γ = 3,

Compute the product N = $\alpha\beta\gamma$ = 285,

ϕ (N) = $(19^2-1)(5^2-1)(3^2-1)$ = 69120.

Choose e = 3331.

Then $d = e^{-1} \bmod \phi(N)$ = 3331^{-1} mod 69120 = 29611

The public key is n = 285, e = 3331

Encryption

Let message M = m1; m2 = (555, 444)

C = (c1; c2) = $m^e (\bmod N)$

= $(555,444)^{3331}$ mod 285

= (270, 159)

Decryption

$M = c^d (\bmod N)$

= (270, 159) mod 285

= (555, 444)

6. SECURITY ANALYSIS OF PROPOSED SCHEME

The comparison of the classical RSA [16] and its Gaussian Integer Domain in Z[i] [8] and our proposed scheme is as follows:

- The generation of primes p, q in classical scheme and Gaussian primes a, b in Z[i] require the same amount of computation. Same in the case with our proposed scheme where an additional prime g in the form of 4k+3 would be generated with the same computation.
- The modified Gaussian variant provides more security than the classical method since the number of elements which are chosen to represent the message m is about square of those used in the classical case. Our proposed scheme would provide security as compare to Gaussian variant. Because, domain Z[i] in our proposed scheme provides a more extension to the range of chosen messages, which make trails more complicated as compare to the Gaussian integer domain [4].

- In [4], Euler phi function is $\phi = (p^2 - 1)(q^2 - 1)$ where as in proposed scheme it is $\phi = (\alpha^2 - 1)(\beta^2 - 1)(\gamma^2 - 1)$ .This make the attempt to find the private key d from the public key more complicated as compare to the Gaussian variant [4] in Z[i]. Thus, our proposed scheme provides more security than the [4]. More so, the computations involved in the Gaussian variant do not require computational procedures different from those of the classical method. Same would be the case with our scheme.
- It is noted that the complexity for programs depends on the complexity of generating the public-key. Thus, the classical and proposed algorithms are equivalent since their public-key generation algorithms are identical when restricting the choice of primes to those of the form 4k+3. However, our scheme is recommended since it provides a better extension to the message space and the public exponent range as compare to classical one.

7. CONCLUSION

We modify the computational methods in the domain of Gaussian integers. We show how the modified computational methods can be used to extend the RSA algorithm to the domain Z[i]. Also, the modified method provides an extension to the range of chosen messages and the trials will be more complicated. Lastly, we show that the modified algorithm requires alittle additional computational effort than the classical one and accomplishes much greater security.

REFERENCES

[1] B. Verkhovsky, "Selection of Entanglements in Informa-tion Assurance Protocols and Optimal Retrieval of Original Blocks," *Journal of Telecommunications Man-agement*, Vol. 2, No. 2, pp. 186-194, (2009).

[2] B.Verkhovsky, "*Accelerated Cybersecure Communica-tion Based on Reduced Encryption/Decryption and In-formation Assurance Protocols*," Journal of Telecommu-nication Managements, Vol. 2, No. 3, pp. 284-293, (2009).

[3] B. Verkhovsky ," *Cubic Root Extractors of Gaussian Integers and Their Application in Fast Encryption for Time-Constrained Secure Communication*", Int. J. Communications, Network and System Sciences, 4, pp.197-204 **, (**2011). doi:10.4236/ijcns.2011.44024

[4] Collins, T., Hopkins, D., Langford, S., Sabin, M., *Public Key Cryptographic Apparatus and Method*. U.S.Patent #5, 848, 159, (1997).

[5] Cross, J.T., *The Eulers f -function in the Gaussian integers*. Amer. Math. 55, pp. 518–528, (1995).

[6] Diffie, W., and Hellman, M, New *Directions in Cryptography*. IEEE Trans. on Inform. Theory IT-22, pp. 644–654, (1976).

[7] Elkamchouchi, H., Elshenawy, K., Shaban, H., *Extended RSA cryptosystem and digital signatureschemes in the domain of Gaussian integers*, The 8th International Conference on Communication Systems, 1 (ICCS'02), pp. 91–95 (2002)

[8] El-Kassar, A.N., Haraty, R., Awad, Y., Debnath, N.C., *Modified RSA in the domains of Gaussianintegers and polynomials over finite fields*. Proc. Intl. Conf. Computer Applications in Industry and Engineering - CAINE, pp. 298-303 (2005)

[9] Gauss, C.F., *Theoria residuo rumbiquadraticorum.* Comm. Soc. Reg. Sci. Gottingen 7, pp. 1–34 (1832)

[10] Jason Hinek, M., *Low Public Exponent Partial Key and Low private Exponent Attacks on Multi-prime rsa*., Master Thesis, Waterloo, Ontario-Canada (2002)

[11] Haraty, R.A., El-Kassar, A.N., Shibaro, B., *A Comparative Study of RSA Based Digital Signature Algorithms*, Journal of Mathematics and Statistics 2, pp. 354–359, (2006).

[12] H. Elkamchouchi, K. Elshenawy and H. Shaban,"Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers," *The 8th Interna-tional Conference on Communication System*, pp. 91-95, (2002).

[13] Menezes, A., Van Oorshot, J., Vanstone, P.C.S.A., *Handbook of Applied Cryptography*, CRCPress, (1997).

[14] Niven, I., Zukerman, H.S., Montegomery, H.L.: *An introduction to the theory of number*, John Wiley, New York, (1991).

[15] S. Kak, "The Cubic Public-Key Transformation," *Cir-cuits Systems Signal Processing*, Vol. 26, No. 3, pp. 353-359, (2007). doi:10.1007/s00034-006-0309-x

[16] Rivest, R., Shamir, A., Adleman, L., *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM 21, pp.120–126, (1978).

BIOGRAPHIES OF AUTHORS

Sushma Pradhan received the B.Sc, M.Sc and M.Phill degree in Mathematics Pt. Ravishankar Shukla University, Raipur, Chattigarh, India in 2002, 2004 and 2007. She joined School of Studies in Mathematics, Pt. Ravishnakra Shukla University, and Raipur, India for her Research work. She is a life time member of Cryptology Research Society of India (CRSI). Her area of interest is Public Key Cryptography and Integer factorization Problem.

Birendra Kumar Sharma Professor, School of Studies in Mathematics, Pt.Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.