Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 1, pp. 143–150
DOI : 10.47974/JDMSC-1628

A novel improvement in RSA algorithm

Rajitha Ranasinghe *
Madusha Chathurangi †
Department of Mathematics
University of Peradeniya
Peradeniya 20400
Sri Lanka

Pabasara Athukorala §
NSBM Green University
Pitipana, Homagama 10206
Sri Lanka

Abstract

In this study, we propose a new cryptographic scheme based on the textbook RSA algorithm associating the concept of continued fractions. The algorithm is designed under the three primary steps of key generation, encryption, and decryption. The key generation of the system is improved to generate a large encryption key without affecting the decryption key. The use of continued fractions gives an additional advantage as it encrypts a string of plaintexts by encrypting only two integers which optimizes the time and the memory consumption. The encryption process and the decryption process are similar to that of the standard RSA algorithm, insomuch the implemented algorithm does not affect the security of the original RSA algorithm which depends on the factoring problem. In addition, as the algorithm uses a large encryption key, it has been proven that the system is secure against the Wiener's attack.

Subject Classification: *(2010) 11Z05, 11A07, 11T71, 94A60.*

Keywords: *Continued fraction, Factoring problem, RSA cryptosystem, Wiener's attack.*

* *E-mail:* **rajithamath@sci.pdn.ac.lk (Corresponding Author)**
† *E-mail:* **madushac@sci.pdn.ac.lk**
§ *E-mail:* **pabasara.a@nsbm.ac.lk**

© Taru Publications

1. Introduction

1.1 *Prologue*

Cryptography is the science of studying mathematical schemes for secure communications and involves two main techniques, namely Symmetric-key cryptography and Asymmetric-key cryptography. The encryption is the process which converts a plaintext into a secret format and the decryption is the reverse process. The first conception of Asymmetric cryptosystems (also known as public-key cryptosystems) in 1970 by Wilfred Diffie and Merkle Hellman provided a new pathway to cryptography. In contrast to Symmetric-key cryptosystems (also known as Private-key cryptosystems), in Aymmetric-key cryptosystems there are public keys which are made freely available to anyone and private keys which are kept as a secret. The most significant advantage of Public-key cryptosystems is that we don't require a private information link to share keys and it provides the authentication. The data can be encrypted using public keys and can be decrypted only using private keys. Malicious users can see the encrypted message but can't decrypt it because decryption keys are not publicly available.

In 1977, Ron Rivest, Adi Shamir, and Leonard Adelman proposed a new public-key cryptosystem [5], now known to the world as the RSA algorithm (the acronym RSA is attributed to honor its three founders). Over the years, this has become one of the most acclaimed members in the family of cryptographic algorithms due to its secure and hard to break nature, the factoring problem. A recent survey by Mumtaz and Ping, [4] provides a comprehensive study on its past, present advancements and upcoming challenges that needs concrete analysis and also possible threats according to its underlying algebraic structure. Many researchers are proposing new variants of the original RSA algorithm to overcome possible drawbacks and suggest possible improvements (see [1], [2], and the references therein). In 1989, Michael J. Wiener showed that the original RSA algorithm is vulnerable to an attack which was named after him as Wiener's attack [7] for a smaller encryption key. In the present study, we introduce an algorithm to encrypt messages based on the textbook RSA which preserves immunity against the Wiener's attack. Our present study is an extension of [3] which was motivated by the work of [6], where a new semantically secure cryptosystem was introduced as an improvement to the RSA cryptosystem.

1.2 *The RSA Cryptosystem*

In this section we discuss the well known textbook RSA algorithm in detail.

Suppose **A** and **B** are two parties who want to communicate over an insecure channel, where **A** is the receiver and **B** is the sender.

Key generation: The key generation is done by **A** and the general steps are given below [5].

Step 1 : Choose two large primes p and q (size of p and q is recommended to be at least 512 bits or more)

Step 2 : Calculate the modulus n as $n = p \times q$.

Step 3 : Calculate the Euler's totient function of n; $\varphi(n) = (p-1)\times(q-1)$.

Step 4 : Choose an integer e such that $1 < e < \varphi(n)$, (i.e., $\gcd(e, \varphi(n)) = 1$, where "gcd" stands for the greatest common divisor).

Step 5 : Calculate d such that $1 < d < \varphi(n)$ and $de \equiv 1 (\mathrm{mod}\ \varphi(n))$.

The encryption key is thus the pair of positive integers (e, n) which is accessible to public and the decryption key is the pair of positive integers (d, n) which is known only to the designer. The two large primes p and q are kept secret.

Public Keys : e, n and Private Keys : d, n

Encryption: B divides the message into blocks, then encrypts the message M as follows:

$$C \equiv M^e (\mathrm{mod}\ n), \text{ where } C \text{ denotes the ciphertext.}$$

Decryption: A receives the ciphertext C and decrypts it as follows.

$$M \equiv C^d (\mathrm{mod}\ n)$$
$$M \equiv (M^e)^d (\mathrm{mod}\ n)$$

2. Proposed Algorithm

Our algorithm is designed under three basic steps: key generation, encryption, and decryption. We will first explain the general procedure of our scheme and next illustrate it with a simple example.

2.1 *General Procedure*

Key Generation: Consider two parties **A** and **B** and suppose that **A** wants to send messages to **B** secretly. First, the key generation is done by the receiver **B**, generating asymmetric keys and making the corresponding keys publicly available.

Step 1 : Choose two large primes p and q

Step 2 : Calculate $n = p \times q$

Step 3 : Let the encryption key e be chosen such that $\gcd(e, \varphi(n)) = 1$, where $\varphi(n)$ is the Euler's totient function of n.

Step 4 : Now choose the deciphering key d as the multiplicative inverse of e modulo $\varphi(n)$. i.e., $de \equiv 1 (\text{mod } \varphi(n))$.

Step 5 : Then **B** selects e' such that $e' = e^{(1+ms)}$, where $m \geq 1$ and $s = \varphi(\varphi(n))$.

Public keys : (e', n)
Private keys : (d, n)

Encryption: Let **A** has a string of plaintexts and then encrypts it as follows:

A converts the string of plaintexts as partial quotients of a finite continued fraction representation and obtains the coresponding rational number and makes sure that the denominator and numerator are both in their lowest form. Let $\frac{P_1}{P_2} = [a; b, c, \ldots, r]$ denote the continued fraction representation and **A** computes two congruences:

$$C_1 \equiv P_1^{e'} (\text{mod } n)$$
$$C_2 \equiv P_2^{e'} (\text{mod } n)$$

Ciphertext = (C_1, C_2)

Decryption: Once **B** receives the ciphertext, he computes the followings:

$$P_1 \equiv C_1^{d} (\text{mod } n)$$
$$P_2 \equiv C_2^{d} (\text{mod } n)$$

B can recover the plaintext from C_1 and C_2 since,

$$e'd \equiv e^{(1+ms)}d \pmod{\varphi(n)}$$
$$e'd \equiv ee^{ms}d \pmod{\varphi(n)}$$
$$e'd \equiv e(e^{(\varphi(\varphi(n))})^m d \pmod{\varphi(n)}$$
$$e'd \equiv ed \equiv 1 \pmod{\varphi(n)}.$$

and consequently we obtain

$$C_1^d \equiv (P_1)^{e'd} \equiv (P_1)^{ed} \equiv P_1 \pmod{n} \text{ and}$$
$$C_2^d \equiv (P_2)^{e'd} \equiv (P_2)^{ed} \equiv P_2 \pmod{n}.$$

Now he converts the partial quotients $\frac{P_1}{P_2}$ into a continued fraction in order to obtain the string of plaintexts.

2.2 *Example*

Now we will illustrate our algorithm with a simple example. Note that, here the values are chosen merely for the ease of simplification without considering its security.

Key generation:

- Let $p = 7$ and $q = 5$. Then $n = 7 \times 5 = 35$. Note that $\varphi(n) = 6 \times 4 = 24$
- Let $e = 5$ since $\gcd(5, 24) = 1$. Then $d \equiv 5 \pmod{24}$
- Compute $s = \varphi(\varphi(35)) = \varphi(24) = 8$ and let $m = 1$ and the $e' = e^{(1+8)} = e^9 = 1,953,125$

Private keys : $(d, n) = (5, 35)$
Public keys: $(e', n) = (5^9, 35)$

Encryption: Consider the string of plaintexts $\{0, 1, 5, 2, 2\}$ and denote it as a continued fraction $\frac{27}{32} = [0; 1, 5, 2, 2]$. Compute the followings:

$$C_1 \equiv 27^{(5^9)} \pmod{35} \equiv 27 \pmod{35}$$
$$C_2 \equiv 32^{(5^9)} \pmod{35} \equiv 2 \pmod{35}$$

Ciphertext : $(C_1, C_2) = (27, 2)$

Decryption: Once the ciphertext is received, find P_1 and P_2,

$$P_1 \equiv 27^5 \pmod{35} \equiv 27 \pmod{35}$$
$$P_2 \equiv 2^5 \pmod{35} \equiv 32 \pmod{35}$$

Recover the plaintext using the Euclid's algorithm as follows:

$$\begin{aligned} 27 &= 32\times\ 0+\ 27 \\ 32 &= 27\times\ 1+\ 5 \\ 27 &= 5\times\ 5+\ 2 \\ 5 &= 2\times\ 2+\ 1 \\ 2 &= 1\times\ 2+\ 0 \end{aligned}$$

Thus, the string of plaintext $\{0,1,5,2,2\}$ is recovered.

3. Cryptanalytic Approach

The proposed system does not alter the security of the original RSA algorithm which depends on the difficulty of factoring the modulus n into two large primes and is known as the factoring problem. In addition, the new system is secured against the Wiener's attack for large exponent values, e'.

First, we will state the Wiener's theorem as it is appeared in [1] to comply with the present setting.

Theorem 3.1 : *Let* $n = p\times\ q$ *with* $p < q < 2q$. *Also, let the secret exponent key d satisfies* $d < \frac{n^{0.25}}{3}$ *with the pair* $\{e,n\}$ *satisfying* $ed \equiv 1(\text{mod } \varphi(n))$. *Then d can be efficiently recovered.*

However, since the encryption key becomes large, the implemented system preserves immunity against the Wiener's attack which can be proved as follows.

From $e'd \equiv 1(\text{mod } \varphi(n))$, for a positive integer k greater than, we can write

$$e'd = 1+\ k\varphi(n).$$

Since $\varphi(n) = pq-\ p-\ q+\ 1,$ it follows that

$$\frac{e'd}{pq} = k\left(\ 1-\ \left\{\frac{1}{p}+\ \frac{1}{q}-\ \frac{1}{pq}-\ \frac{1}{pqk}\right\}\right).$$

Set $\delta = \left\{\frac{1}{p}+\ \frac{1}{q}-\ \frac{1}{pq}-\ \frac{1}{pqk}\right\} = \frac{p+\ q-\ 1-1/k}{pq},$ which yields

$$\left|\frac{e'}{n}-\ \frac{k}{d}\right| = \frac{k}{d}\,\delta.$$

Here $\gcd(d,k)=1$, which implies that $\frac{k}{d}$ is convergent to the simple continued fraction of $\frac{e}{n}$ [1]. If $e' > n^{3/2}$, then $\frac{e'}{n} > n^{1/2}$. Thus, we have

$$\frac{e'}{n} = \frac{k}{d}(1-\delta) > n^{1/2}$$
$$\frac{k}{d} > n^{1/2}$$
$$k > dn^{1/2}.$$

Moreover, for large p and q values, $\delta = \frac{p+q}{pq}$ and in 1989, Wiener in [7] showed that $\delta < \frac{1}{3/2 d_m n_m}$ where d_m and n_m are the denominator and the numerator of a simple continued fraction f respectively.

Combining the above results, we can obtain

$$\delta < \frac{1}{\frac{3}{2} d_m n_m}$$
$$\frac{p+q}{pq} < \frac{2}{3 d_m n_m}$$
$$d_m n_m < \frac{2n}{3(p+q)}$$

Since $\frac{k}{d}$ is a convergent of the continued fraction $\frac{e}{n}$, the two substitutions $n_m = k$ and $d_m = d$ gives

$$kd < \frac{2n}{3(p+q)}$$
$$dn^{\frac{1}{2}} d < kd < \frac{2n}{3(p+q)}$$
$$d^2 n^{\frac{1}{2}} < \frac{2n}{3(p+q)}$$
$$d^2 < \frac{2n^{\frac{1}{2}}}{3(p+q)}$$
$$d < 1.$$

Therefore, if $e' > n^{1.5}$, the continued fraction algorithm used in Wiener's attack is not guaranteed to work for any size of secret exponent.

4. Conclusion and Future work

We have proposed a new cryptographic scheme based on the RSA algorithm together with the notion of continued fractions. The key

generation of the system is modified by generating a larger encryption key without affecting the decryption key. The security of the new scheme rests upon the factoring problem as it doesn't alter the encryption process and the decryption process of the original RSA algorithm. Not only that, the use of a large encryption key prevents the Wiener's attack which is an additional advantage compared to the RSA algorithm. Although the use of a large encryption key increases the encryption time, it has been positively addressed by using continued fractions and reducing the string of plaintexts into just two plaintexts before the encryption. Our current focus is on developing the present scheme further to overcome possible attacks and on implementing a computer program to handle practical scenarios.

References

[1] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203–213, 1999.

[2] M. J. Hinek. *Cryptanalysis of RSA and its variants*. Taylor and Francis group: CRC Press, 2009.

[3] P.G.R.S. Ranasinghe, A.P. Madhushani, and H.M.M. Chathurangi. Novel improvement in RSA algorithm, Proceedings of PGIS Research Congress 2021, Vol. 8, pg. 61., Postgraduate Institute of Science, University of Peradeniya.

[4] M. Mumtaz and L. Ping. Forty years of attacks on the rsa cryptosystem: A brief survey. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(1):9–29, 2019.

[5] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[6] S. Verma and D. Garg. Improvement in RSA Cryptosystem. *Journal of Advances in Information Technology*, 2(3):146–151, 2011.

[7] M. J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information theory*, 36(3):553–558, 1990.

Received August, 2021

Revised February, 2022