International Journal of Cryptology Research 11(1): 1 - 12 (2021)

Simple Cryptanalysis on the Phony Rivest-Shamir-Adleman cryptosystem

Muhammad Danial Abd Jafri[1], **Nor Haniza Sarmin**[1], **Amir Hamzah Abd Ghafar**[*2,3], and **Muhammad Asyraf Asbullah**[2,4]

[1]*Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, Malaysia*
[2]*Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia*
[3]*Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.*
[4]*Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.*

E-mail: amir_hamzah@upm.edu.my
[*]*Corresponding author*

ABSTRACT

In this advanced era, public key cryptography is essential in the field of data communication. The Rivest-Shamir-Adleman (RSA) is regarded as one of the most powerful algorithms in the public key cryptosystem. While the original RSA used two prime numbers, p, and q the RSA variant in this paper used four prime numbers, namely Phony-RSA cryptosystem. The RSA variant with phony modulus intends to prevent the limitations of an integer factorization attack by increasing the complexity of the factorization process by using a phony public key exponent and a phony modulus. This work presents successful cryptanalysis of the said Phony-RSA cryptosystem via elementary mathematical proving. Furthermore, an algorithm and numerical examples of the cryptanalysis were elaborated. Based on the result, the RSA variant with phony modulus is deemed insecure.

Keywords: RSA, Phony modulus, cryptanalysis, public key, prime number

1 INTRODUCTION

Cryptography is the activity and study of encryption and decryption, is also known as the study of secure communication. According to Stinson (2005) cryptography's main objective is to let two parties communicate over an unsecured channel without enabling third parties to decrypt the original conversation. Cryptography distinguishes between two types of cryptosystems: secret key cryptosystems and public key cryptosystems. According to Lone and Khalique (2016), the public key is used to encrypt plaintext or verify a digital signature, whereas the private key is used to decode text or create a digital signature. Both the sender and receiver must possess the key to carry out encryption and decryption operations, respectively. According to Aumasson (2017), cryptography's primary use is the encryption algorithm. Cryptography is usually confined to ciphers or techniques that involve the substitution of extra letters or symbols for the message's original contentsWong et al. (2015). Cryptography's four primary security goals are confidentiality, integrity, authentication, and non-repudiation.

Cryptanalysis is the science of decrypting and reading specific encrypted communications without permission. Cryptanalysis is the process of decrypting ciphertext in order to retrieve the plaintext or original text Isa et al. (2019). According to Holden (2018), cryptanalysis is studying how to read such encrypted communications without authorization. Cryptanalysis is the act of decrypting a cryptosystem in order to recover the plaintext, while cryptography is the process of transmitting secret communications through codes and ciphers. The presence of cryptanalysis enables us to determine the RSA cryptosystem's security level. Sarbini et al. (2018) stated that the security level of cryptographic systems is determined by how difficult it is for a cryptanalyst to uncover plaintext without knowing the key.

Rivest-Shamir-Adleman's (RSA) cryptosystem is one of the examples of public-key cryptography. The RSA cryptosystem was introduced in the year

1977 by Rivest et al. (1978). Cryptography has been a commonly used technique in communications, networking, and computer security mechanisms. Susilo et al. (2021) explained that RSA is one of the most common ciphers used in the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) system protocol, which enables the secure transmission of sensitive information over the internet. According to Raghunandan et al. (2020), the RSA method entails three processes: key creation, encryption, and decryption.

The RSA algorithm uses two keys: a public key with a modulus of e and a private key with a modulus of d. Rivest et al. (1978) stated that two numbers e and d are selected so that $ed \equiv 1 \pmod{\phi(N)}$, where $\phi(N) = (p-1)(q-1)$ is the order of the multiplicative group. The public key exponent is represented by the integer e, whereas the private key exponent is denoted by the integer d. The encryption algorithm takes as inputs a message m and a public key pair (N, e), and outputs ciphertext $c \equiv m^e \pmod{N}$. The decryption will determine the value of $m \equiv c^d \pmod{N}$. For decryption, the ciphertext c will be used in conjunction with the private key d, with the result being the message m.

Thangavel et al. (2015) and Al_Barazanchi et al. (2019) developed an improved RSA technique that utilizes four prime factors rather than two, increasing the difficulty of finding prime factors. Raghunandan et al. (2019) presented a novel RSA model by replacing the public key e and private key d with two additional parameters (f, g) in the key generation method, where f is multiplied by e and g is the division of d. The modified RSA method is used to mitigate the Integer Factorization Attack's vulnerabilities by increasing the difficulty of factorization by employing a phony (fake) public key exponent f instead of e and a phony modulus X instead of N.

Raghunandan et al. (2020) stated that the sender sends the fake modulus f as a public key parameter to encrypt plaintext. From here on, the cryptosystem, as mentioned earlier, will be referred to as the Phony-RSA cryptosystem. Their suggested approach computes modulus N using four prime integers (p, q, r, s), making it difficult for the intruder to factorize the abbreviations. The Phony-RSA cryptosystem in detail will be described in Section 2.2. The RSA cryptosystem with phony modulus was claimed to have better security compared to standard RSA. Using more than two keys by the suggested method increases the RSA security algorithm proposed by Al_Barazanchi et al. (2019). Al_Barazanchi et al. (2019) introduced a phony modulus to address the weaknesses of the integer factorization attack.

Al_Barazanchi et al. (2019) stated that this suggested model has better factoring due to higher prime numbers and large encryption exponents. The RSA algorithm's security has been significantly improved due to the twofold encryption and decryption procedure. In terms of privacy, Raghunandan et al. (2019) claim that the proposed model is superior to the conventional RSA paradigm. According to the preliminary literature analysis, the RSA with fake modulus is much more secure than the regular RSA. However, there is a dearth of security analysis of the RSA using a fake modulus in the literature. As such, this article will examine the security of the RSA phony modulus and its implementation.

The following is the outline of the paper. Section 2 describes the background of the study and works on elementary number theory. Furthermore, the RSA with phony modulus is presented in this section. Following that, the methods and numerical examples for the Phony-RSA cryptosystem are described. Section 3 provides propositional cryptanalysis of the Phony-RSA cryptosystem. Next, two simulation of numerical examples that illustrates the successful attacks of the Phony-RSA cryptosystem. Finally, Section 4 brings the paper to a close.

2 PRELIMINARIES

This section discusses basic number theory and the Phony-RSA cryptosystem in general. Additionally, the algorithms for the Phony-RSA cryptosystem are given, along with a numerical example.

2.1 Mathematical Background

To date, one of the most well-known problems in mathematics, especially number theory, is known as the integer factorization problem, which displays properties of a hard cryptographic problem Jin et al. (2013), Sarbini et al. (2018). It is assumed to be very difficult to solve and is supported by decades of evidence for its hardness.

Theorem 2.1 (Fundamental Theorem of Arithmetic, Rosen (2011))**.** *Let $N \geq 2$ be an integer. Then N can be factored as a product of prime numbers*

$$N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$$

where p_i are distinct primes and integers $r_i \geq 1$ for $i = 1, 2, \cdots, s$. Moreover,this expression is unique, regardless of its ordering.

Definition 2.1 (Integer Factorization Problem, Paar and Pelzl (2009))**.** *Let N be a positive integer. Then, the integer factorization problem (IFP) is defined as the problem to find the prime factorization of N such that, $N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ where p_i are distinct primes and $r_i \geq 1$.*

Definition 2.2 (Euler's ϕ Function, Paar and Pelzl (2009))**.** *Let a complete residue system modulo N is a set of elements $\{0, 1, \cdots, N-1\}$. The number of invertible elements in a complete residue system modulo N is denoted as $\phi(N)$ and is called Euler's ϕ Function.*

Theorem 2.2 (Rosen (2011))**.** *If $N = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ is the prime factorization of N, then*

$$\phi(N) = \prod_{i=1}^{s} p_i^{r_i - 1} (p_i - 1)$$

Theorem 2.3 (Fermat–Euler Theorem, Rosen (2011))**.** *Let N and a are coprime positive integers and $\phi(N)$ is Euler's ϕ function. Then for every integer a, $a^{\phi(N)} \equiv 1 \pmod{N}$.*

For most cases in cryptography, the problem is to find the prime factors p and q from $N = pq$. Based on Theorem 2.2 and Theorem 2.3, suppose $N = pq$. Then $\phi(N) = (p-1)(q-1)$ and for every integer a, $a^{(p-1)(q-1)} \equiv 1 \pmod{N}$ such that $\gcd(a, N) = 1$ (Isa et al., 2019).

2.2 RSA Variant with Phony Modulus

This section elaborate the new RSA variants with phony modulus in the form of three important parts, which are key generation, encryption, and decryption. The inputs for the key generation algorithm are the size of k of the security and the output are the phony public key f, phony private key g, and phony modulus X. The key generation algorithm's stages are as follows.

Algorithm 1 Phony-RSA Key Generation

```
Input: Four distinct primes numbers $p, q, r, s$.
Output: Phony public key pair $(X, f)$ and private key $g$.
Choose four distinct primes numbers $p, q, r, s$.
Compute $N = pqrs$ and $\phi(N) = (p-1)(q-1)(r-1)(s-1)$.
Choose $e$ such that $3 \leq e \leq \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
Compute $d$ such that $ed \equiv 1 \pmod{\phi(N)}$.
Compute integer $K$ that satisfies equation $d \equiv 0 \pmod{K}$.
Calculate $f$ and $g$ where $f = eK$ and $g = \frac{d}{K}$ respectively.
Find an integer prime number $X$, that satisfies the equation $ed \equiv 1 \pmod{\phi(X)}$, where $X > N$.
Phony public key pair $(X, f)$ and private key $g$.
```

The inputs for the encryption algorithm are plaintext m, phony public key (X, f) and the output is ciphertext c. The following are the steps of the encryption algorithm.

Algorithm 2 Phony-RSA Encryption

```
Input: Public key pairs $(X, f)$
Output: Ciphertext $c$.
Choose integer $0 < m < X$.
Compute $c \equiv m^f \pmod{X}$.
Return the ciphertext $c$.
```

The inputs for the decryption algorithm are ciphertext c, phony private key g and the output is the message m. The following are the steps of the decryption algorithm.

Algorithm 3 Phony-RSA Decryption

```
Input: Public key $X$, private key $g$ and the ciphertext $c$.
Output: The message $m$.
Compute $m \equiv c^g \pmod{X}$.
Return the message $m$.
```

The following numerical example illustrate the working flow of Phony-RSA cryptosystem algorithm which strictly follows Raghunandan et al. (2019). In the following steps, choose four distinct prime numbers $p = 37, q = 41, r = 47, s = 59$. Compute $N = pqrs$, hence $N = 4206641$. Obtain $\phi(N) = 3841920$ by using Euler's Totient equation where $\phi(N) = (p–1)(q–1)(r–1)(s–1)$. Find a public key exponent e such that $\gcd(e, 3841920) = 1$ where $1 < e < \phi(N)$, thus $e = 2477$. Find private key d such that $2477d \equiv 1 \pmod{3841920}$, hence the value of $d = 1693733$. Compute integer K that satisfies equation $d \equiv 0 \pmod{K}$, thus $K = 163$. Phony public key f obtained by using equation $f = eK$, so $f = 403751$. Phony private key g using equation $g = \frac{d}{k}$, hence the value $g = 10391$. Obtained phony modulus $X = 15200641$ that satisfies equation $ed \equiv 1 \pmod{\phi(X)}$ where $X > N$.

The new parameters so called phony public keys $(X = 15200641, f = 403751)$ is published to the sender and the new phony private key $g = 10391$ must be kept secret. Let $m = 123$ be the message, then the sender encrypt m into a ciphertext using equation $c \equiv m^f \pmod{X}$, hence obtained cipher value is $c = 4004719$. Recipients convert ciphertext into the message back using the equation $m \equiv c^g \pmod{X}$.

3 RESULTS AND DISCUSSION

This section demonstrates how to cryptanalysis the Phony-RSA cryptosystem proposed by Raghunandan et al. (2019). In addition, with a numerical example, this section provides a practical cryptanalysis technique to the Phony-RSA cryptosystem.

3.1 Cryptanalysis of the Phony-RSA cryptosystem

Raghunandan et al. (2019) presented the Phony-RSA cryptosystem, which is a modified RSA cryptosystem. This section will explain why, when the phony modulus X is taken into account, the Phony-RSA cryptosystem becomes insecure and easily decrypted. Proposition 3.1 presents the cryptanalysis of the Phony-RSA cryptosystem by manipulating Theorem 2.2 and Theorem 2.3 as follows.

Proposition 3.1. *Let (X, f) and (X, g) be denoted as phony public key and phony private key counterparts of the Phony-RSA modulus, respectively. For any message m such that $0 < m < X$ and for g' such that $fg' \equiv 1 \pmod{\phi(X)}$, then $m \equiv c^{g'} \pmod{X}$.*

Proof. Assume that (X, f) and (X, g) are phony public key and phony private key counterparts of the Phony-RSA modulus, respectively. Since X is a prime number, therefore, from Theorem 2.2 shows that $\phi(X)$ can be easily obtained by computing $\phi(X) = X - 1$. Next, there exists an integer g' such that $g' \equiv f^{-1} \pmod{\phi(X)}$ satisfying $fg' \equiv 1 \pmod{\phi(X)}$. Thus, the congruence relation can be written as $fg' = 1 + \phi(X)t$ for some integer t. Since the integer m is restricted in the interval $(0, X)$ and X is a prime number, hence $\gcd(m, X) = 1$ holds. Thus, by Theorem 2.3, the message m of the Phony-RSA ciphertext can be recovered using

$$c^{g'} \equiv m^{fg'} \equiv m^{1+\phi(X)t} \equiv m^1 m^{\phi(X)t} \equiv m \pmod{X}.$$

□

Hence given only the parameter of X, f and its ciphertext c, the above result shows that any message m such that $0 < m < X$, can be easily obtained by using the phony private-key g' from Proposition 3.1. As a result, the Phony-RSA cryptosystem is insecure. The following algorithm can be used to cryptanalysis the Phony-RSA cryptosystem.

Algorithm 4 Cryptanalysis of Phony-RSA cryptosystem based on Proposition 3.1.

```
Input: A public key pairs $(X, f, c)$
Output: The message $m$.
1: Compute $\phi(X) = X–1$.
2: Compute $g' \equiv f^{-1} \pmod{\phi(X)}$.
3: Compute $m \equiv c^{g'} \pmod{X}$.
4: Return the message $m$.
```

It should be noted that the stages in the cryptanalysis the Algorithm 4 can decrypt the Phony-RSA cryptosystem in linear time to obtain the message m, which can be solved using only the public key (X, f) and its corresponding ciphertext c values. As a result, the security level of the Phony-RSA cryptosystem is deemed insecure. The successful attacks on the toy instances described in Section 2 utilising Proposition 3.1 will be discussed in the following subsections.

3.2 Simulated Attacks

Two successful cryptanalyses of the Phony-RSA cryptosystem are reported in this section. The following is a toy example that was directly duplicated from Raghunandan et al. (2019) and yielded the following parameters.

Phony Public keys	$X = 3361, f = 517$
Phony Private keys	$N = 1155, e = 47, d = 143, g = 13, K = 11$
Message	$m = 123$
Ciphertext	$c = 504$

Table 1: Parameters of relevance as shown in Raghunandan et al. (2019)

Successful Attack 1: Now, the following steps will illustrate the attack using Algorithm 4 to obtain m easily without the need to obtain all the private keys e, d, K, nor the need to obtain all the prime factors of modulus N. Since

(X, f) are the phony public keys, assume that the values of phony public key are $(3361, 517)$. Following that, calculate $\phi(X) = X - 1 = 3360$. Given that $f = 517$ is publicly accessible, determining the secret value $g' = 13$ is straightforward. $g' \equiv f^{-1} \pmod{\phi(X)}$. Finally, determine the intended message m by computing $c^{g'} \equiv 504^{13} \equiv 123 \pmod{3361}$.

Next, the following is another simulated attack on the numerical example given in Section 2.2. Let all the phony public keys and private keys as follows.

Phony Public keys	$X = 15200641, f = 4037511$
Private keys	$N = 4206641, e = 2477, d = 1693733,$ $g = 10391, K = 163$
Message	$m = 123$
Ciphertext	$c = 4004719$

Table 2: Parameters of relevance as shown in Section 2.2

Successful Attack 2: Now, the following steps will illustrate the attack using Algorithm 4 to obtain m easily without the need to obtain all the private keys e, d, K, nor the need to obtain all the prime factors of modulus N. Let $(X = 15200641, f = 4037511)$ are the phony public keys. Following that, calculate $\phi(X) = 15200640$ and determining the secret value $g' \equiv f^{-1} \equiv 10391 \pmod{\phi(X)}$. Finally, determine the intended message m by computing $c^{g'} \equiv 123 \pmod{15200641}$.

4 CONCLUSION

According to the Proposition 3.1 and Algorithm 4, the cryptanalysis of the Phony-RSA Cryptosystem proposed by Raghunandan et al. (2019) is linear in running time. Using the Phony public key parameter X, f and the ciphertext c, the alternative phony private-key g' can be computed, and thus the message m can be easily obtained. Our simple cryptanalysis exposes the security level RSA variant with phony modulus, resulting in a total break. As a result, brute force is not required to break the RSA variant with a phony modulus cryptosystem. To summarize, the security level of the Phony-RSA Cryptosystem has been determined to be no better than that of the original RSA cryptosystem.

REFERENCES

Al_Barazanchi, I., Shawkat, S. A., Hameed, M. H., and Al-Badri, K. S. L. (2019). Modified RSA-based algorithm: A double secure approach. *Telecommunication Computing Electronics and Control*, 17(6):2818–2825.

Aumasson, J.-P. (2017). *Serious cryptography: a practical introduction to modern encryption*. No Starch Press.

Holden, J. (2018). *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton University Press.

Isa, M., Rahmany, N., Asbullah, M., Sathar, M., and Rasedee, A. (2019). On the Insecurity of Generalized (Rivest-Shamir-Adleman)-Advance and Adaptable Cryptosystem. In *Journal of Physics: Conference Series*, volume 1366, page 012021. IOP Publishing.

Jin, W. T., Kamarulhali, H., and Said, M. R. M. (2013). On the Hastad's Attack to LUC4, 6 Cryptosystem and compared with Other RSA-Type Cryptosystem. *Malaysian Journal of Mathematical Science*, 7:1–17.

Lone, A. H. and Khalique, A. (2016). Generalized RSA using 2k prime numbers with secure key generation. *Security and Communication Networks*, 9(17):4443–4450.

Paar, C. and Pelzl, J. (2009). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Science & Business Media.

Raghunandan, K., Aithal, G., and Shetty, S. (2019). Secure RSA variant system to avoid factorization attack using phony modules and phony public key Exponent. *Int J Innovative Technol Exploring Eng (IJITEE)*, 8(9).

Raghunandan, K., Ganesh, A., Surendra, S., and Bhavya, K. (2020). Key Generation Using Generalized Pell's Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis. *Cybernetics and Information Technologies*, 20(3).

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

Rosen, K. H. (2011). *Elementary Number Theory*. Pearson Education London.

Sarbini, I. N., Jin, W. T., Feng, K. L., Othman, M., Said, M. R. M., and Hung, Y. P. (2018). Garbage-man-in-the-middle (type 2) Attack on the Lucas Based El-Gamal Cryptosystem in the Elliptic Curve Group Over Finite Field. In *Cryptology and Information Security Conference 2018*, page 35.

Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman and Hall/CRC.

Susilo, W., Tonien, J., and Yang, G. (2021). Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA. *Computer Standards & Interfaces*, 74:103470.

Thangavel, M., Varalakshmi, P., Murrali, M., and Nithya, K. (2015). An enhanced and secured rsa key generation scheme (esrkgs). *Journal of information security and applications*, 20:3–10.

Wong, T. J., Said, M. R. M., Othman, M., and Koo, L. F. (2015). On the common modulus attack into the LUC4, 6 cryptosystem. In *AIP Conference Proceedings*, volume 1660, page 090052. AIP Publishing LLC.