



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

An Improved Residue Number System Based RSA Cryptosystem

¹Salifu Abdul-Mumin, ²Kazeem A. Gbolagade

¹Faculty of Mathematical Sciences, Department of Computer Science,
University for Development Studies,
Box 24, Navrongo, Ghana.

²College of Information and Communication Technology,
Computer Science Department, Kwara State University, Malete, Illorin, Nigeria.

Abstract: Sensitive information transmitted between a user and a Web site needs to be encrypted to prevent it from being stolen or modified by unauthorized person. In this paper, a novel encryption system is presented. The proposed system has two levels of ciphering and two level of deciphering. The first level is the traditional Rivest Shamir Adleman (RSA) encryption system and in second level; we utilize Residue Number System where the moduli set is part of the private key for the deciphering process. We deduce that more information will be needed in order to break into the security system in the proposed system than the traditional RSA especially if the message is too short such that $c = m^e > n$. The key space in the proposed system is also more than the traditional RSA as the moduli set is part of the private key. A Performance comparison is presented which is found that encrypting a message, m such that $c = m^e < n$ is not secured in the traditional RSA whiles an intruder will need more information about the private key in order to recover the original message in the proposed scheme regardless of the length of m .

Keywords: Decryption, Encryption, Residue Number System, Revest Shamir Adleman

I. INTRODUCTION

ONE of the means of improving the quality of service in data communication is by means of having a secured medium of communication. The fundamental goal is to secure a communication channel between a transmission system and a receiving system through an insecure channel. Increasing the security system in the communication channel will ensure data integrity, data confidentiality, and data reliability. There is no such thing as perfect security; we need to consider how a system will react to a successful attack. Indeed the most critical part of a security system is not how well it works but how well it fails [1].

Public-key cryptography is instrumental to modern security functions such as authentication and key exchange [2].

Most public-key cryptosystems currently in use, such as Rivest Shamir Adleman (RSA), rely on the intractability of factoring and computing discrete logarithms. However, in 1994, Shor proposed efficient quantum algorithms to solve these problems [3]. Hence, should quantum computing become viable, currently-in-use cryptosystems will be broken. As such, research on efficient post-quantum public-key cryptosystems is most valuable [4].

In some cases also, it is easy to compute modular roots without knowledge of the prime factors. For instance, if m is known to be very small, such that $c = m^e < n$, then m can be recovered from c by taking e^{th} roots over the integers, which is easy [5]. Therefore research on enhancing the RSA cryptosystem will improve the quality of service in data communication. We intend to use residue number system to enhance Textbook RSA by transmitting the cypher text generated from RSA cryptosystem through a residue channel. These will involve two level of encryption scheme; the first level is the RSA encryption scheme and the second level will be similar to private key encryption system without exchanging the private key between the sender and the receiver. In this paper, we found that, encrypting a message, m such $c = m^e > n$ is not secured because taking the e^{th} root of $c = m^e$ will produce m . However, the second stage of encryption in the proposed scheme will transform $c = m^e$ into something and without the knowledge of the moduli set, the original message cannot be recovered. The rest of the paper is organized as follows; Section presents the background of Residue Number System, related works are shown in Section B, Section C gave the concept of RSA encryption, the proposed scheme is given in Section D, a comparison

II. BACKGROUND OF RESIDUE NUMBER SYSTEM

Residue Number System (RNS) is defined by the set S which includes N integers that are pair-wise relatively prime. That is $S = \{m_1, m_2, \dots, m_N\}$, where $\gcd(m_i, m_j) = 1$ for $i, j = 1, \dots, N$ and $i \neq j$ and $\gcd$ means the greatest common divisor.

Every integer X in $[0, M - 1]$ can be uniquely represented with an N -tuple where,

$M = \prod_{i=1}^N m_i$ $X \rightarrow (R_1, R_2, \dots, R_N)$, and

$R_i = |X|_{m_i} = (X \bmod m_i)$; for $i = 1$ to N .

The set S and the number R_i are called the moduli set and the residue of X modulo m_i , respectively. [6] [7][8]

The inherent carry free operations, parallelism and fault-tolerance properties of Residue Number System (RNS) have made it a choice of technology for high precision and high throughput rate Digital Signal Processing (DSP) applications where only repeated multiplications and additions are required [9][10][11]

III. RELATED WORKS

In traditional cryptography, such as was available prior to the 1970s, the encryption and decryption operations are performed with the same key [5]. This is known as the private key cryptography or symmetric encryption scheme. This means that the party encrypting the data and the party decrypting it need to share the same decryption key. Key exchange between the sender and the receiver prior to the first message to be encrypted is an interesting challenge. In order to address this challenge Diffie and Helman [13] proposed some techniques for developing public key cryptosystems. In this system, the encryption key is made public and the decryption key is only known and kept secret to the receiver. This type of encryption system is also known as the asymmetric encryption scheme. RSA which was developed at MIT in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman is an example a public key encryption system.

Different RNS approaches have been proposed to accelerate the implementation of RSA. For the deciphering, a well-known solution performs the computations over $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ independently and reconstructs the final result via the Chinese Remainder Theorem (CRT) [14].

More recently, other CRT-based solutions have been proposed [15], [16], [17]. They all use a quite similar version of the Montgomery multiplication based on the Residue Number System (RNS) [18] [19], which is well-adapted to fast parallel arithmetic.

IV. RSA ENCRYPTION

RSA public-key cryptosystem was invented at MIT in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. The public key in this cryptosystem consists of the value n , which is called the modulus, and the value e , which is called the public exponent. The private key consists of the modulus n and the value d , which is called the private exponent. [5]

RSA encryption makes use of the following basic facts and conjecture in number theory:

Basic fact 1: **Prime generation is easy:** It's easy to find a random prime number of a given size. [5]

Basic fact 2: **Multiplication is easy:** Given p and q , it's easy to find their product, $n = pq$. [5]

CONJECTURE 1: **Factoring is hard:** Given such an n , it appears to be quite hard to recover the prime factors p and q .

Given these basic facts and conjecture, let n be the product of two randomly large primes. If m and c are integers between 0 and $n-1$, and let e be an odd integer between 3 and $n-1$ such that the $\text{GCD}(e, p-1, q-1) = 1$. [5]

FACT 3. **Modular exponentiation is easy:** Given n , m , and e , it's easy to compute $c = m^e \bmod n$. [5]

FACT 4. **Modular root extraction – the reverse of modular exponentiation – is easy given the prime factors:** Given n , e , c , and the prime factors p and q , it's easy to recover the value m such that $c = m^e \bmod n$. [5]

The value m can be recovered from c by a modular exponentiation operation with another odd integer d between 3 and $n-1$. In particular, for this d , the following holds for all m :

$$m = (m^e)^d \bmod n. [5]$$

CONJECTURE 2. **Modular root extraction is otherwise hard:** Given only n , e , and c , but not the prime factors, it appears to be quite hard to recover the value m . [5]

Below is RSA encryption scheme

We define a public-key encryption scheme as follows:

- GenModulus(1^n) runs GenRSA(1^n) to obtain n ; e , and d . The public key is (n, e) and the private key is (n, d)
- Encpk(m), on input a public key $pk = (N, e)$ and a message $m \in \mathbb{Z}_N$, computes the ciphertext $c := [m^e \bmod N]$.
- Decsk(c), on input a private key $sk = (N, d)$ and a cipher text, $c \in \mathbb{Z}_N$, computes the message $m := [c^d \bmod N]$:

Example

Let $p = 13$, $q = 17$, $e = 5$ (e is an odd public exponent between 3 and $n - 1$ that is relatively prime to $p - 1$ and $q - 1$)

Then $N = pq = 221$, $\phi(N) = (p - 1)(q - 1) = 192$

The relationship between the exponents e and d ensures that encryption and decryption are inverses, so that the decryption operation recovers the original message m . Without the private key (n, d) (or equivalently the prime factors p and q), it's difficult (by CONJECTURE 2) to recover m from c . Consequently, n and e can be made public without compromising security, which is the basic requirement for a public-key cryptosystem. [5]

Which implies $e \cdot d = 1 \bmod \phi(N)$. Therefore $d = 77$

To encrypt the binary message $m = 0111001$ with respect to the key $pk = (N = 221, e = 5)$, taking m as 57 (hence an element of $\mathbb{Z}_n = 221$) in the natural way. Computing $c = 57^5 \bmod 221 = 109$.

To decrypt, we compute $m = 109^{77} \bmod 221 = 57$

In some cases, it is easy to compute modular roots without knowledge of the prime factors. For instance, if m is known to be very small, such that $c = m^e < n$, then m can be recovered from c by taking e th roots over the integers, which is easy. [5]

From the analysis above, RSA is only secured for messages, m such that $c = m^e > n$. There is the need to also add randomness in the RSA cryptosystem by picking the messages and transmitting them at random.

V. PROPOSED SYSTEM

Here, RNS is used to enhanced Textbook RSA by transmitting the cyphertext generated from RSA cryptosystem through a residue channel. In this system the private key is enhanced by adding the moduli set to the pk. This will increase the length of the private key and without the knowledge of the moduli set, regardless of the length of the message to be transmitted; m cannot be recovered from c . An important aspect of RNS encoder/decoder is that it can achieve more security than the binary encoder/decoder. In the RNS encoder/decoder, besides the private key, the moduli set $\{P_1, P_2, \dots, P_m\}$ is also part of the secrete keys. The unauthorized listener needs more information to decrypt the system. Thus the RNS encoder/decoder increases the degree of security [21].

Below is the architecture of the proposed cryptosystem:

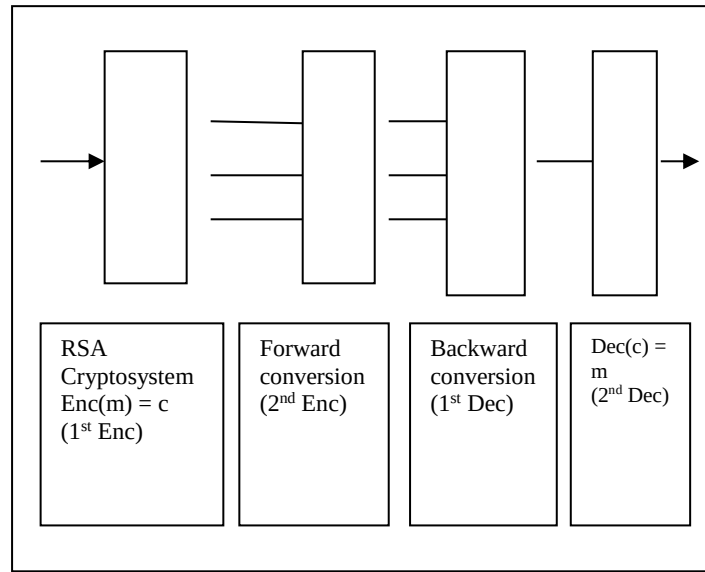


Fig 1: Illustration of the Proposed Cryptosystem

Proposed Algorithm:

- GenModulus(1^n) runs GenRSA(1^n) to obtain n ; e , d and $\{m_1, m_2, m_3\}$. The public key is (n, e) and the private key is $((n, d), (m_1, m_2, m_3))$
- $(\text{Encpk}(m))_1$, on input a public key $pk = (N, e)$ and a message $m \in \mathbb{Z}_N$, computes the ciphertext $c_1 := [m^e \bmod N]$.
- $(\text{Encsk}_1(c_1))_2 = [r_1, r_2, r_3]$ where $r_1 = c_1 \bmod m_1$, $r_2 = c_1 \bmod m_2$ and $r_3 = c_1 \bmod m_3$. $[r_1, r_2, r_3] = c_2$
- $(\text{Decsk}_1(c_2))_1$, on input a private key $sk_1 = (m_1, m_2, m_3)$ and a cipher text, $c_2 \in M$ where M is the dynamic range, using Mixed radix conversion to compute c_1 .
- $(\text{Decsk}_2(c))_2$, on input a private key $sk_2 = (N, d)$ and a cipher text, $c_1 \in \mathbb{Z}_N$, computes the message $m := [c_1^d \bmod N]$

Example

Let $p = 13$, $q = 17$, $e = 5$ (e is an odd public exponent between 3 and $n - 1$ that is relatively prime to $p - 1$ and $q - 1$)

Then $N = pq = 221$, $\phi(N) = (p - 1)(q - 1) = 192$

Let $\{m_1, m_2, m_3\} = \{5, 7, 9\}$

$e \cdot d = 1 \bmod \phi(N)$. Therefore $d = 77$

To encrypt the binary message $m = 0111001$ with respect to the key $pk_1 = (N = 221, e = 5)$, interpreting m as 57 (hence an element of $\mathbb{Z}_n = 221$) in the natural way. Computing $c_1 = 57^5 \bmod 221 = 109$.

For the second encryption with respect to the key $sk_1 = \{5, 7, 9\}$, computing c_2 as follows: $|109|_5 = 4$, $|109|_7 = 4$, $|109|_9 = 1$. Hence $c_2 = (4, 4, 1)$

For first decryption, using the Chinese Remainder Theorem,

$$|x|_m = |\sum_{j=1}^N \hat{m}_j | \frac{r_j}{\hat{m}_j} |_{m_j} |_m \text{ Where } \hat{m}_j = \frac{M}{m_j}, M = \prod_{j=1}^N m_j \text{ and}$$

$$\gcd(m_j, m_k) = 1 \text{ for } j \neq k$$

$$M = \prod_{i=1}^N m_i = 5 * 7 * 9 = 315$$

$$|\hat{m}_1|_{m_1} = |7 \times 9|_5 = |63|_5 = 3 \text{ then } \left| \frac{1}{\hat{m}_1} \right|_5 = 2$$

$$|\hat{m}_2|_{m_2} = |5 \times 9|_7 = |45|_7 = 3, \left| \frac{1}{\hat{m}_2} \right|_7 = 5$$

$$|\hat{m}_3|_{m_3} = |5 \times 7|_9 = |35|_9 = 8, \left| \frac{1}{\hat{m}_3} \right|_9 = 8$$

$$\begin{aligned} |x|_{315} &= |63|_5 \times |2 \times 4|_7 + |45|_7 \times |5 \times 4|_9 + |35|_9 \times |8 \times 1|_{315} \\ &= |63 \times 3 + 45 \times 6 + 35 \times 8|_{315} \\ &= |739|_{315} = 109 \end{aligned}$$

For second decryption with respect to $sk_2 = (d, N)$, we compute $m = 109^{77} \bmod 221 = 57$ as required.

VI. PERFORMANCE ANALYSIS

The proposed scheme is compared with the classical RSA encryption system. In the RSA encryption, the private key is (N, e) and in the proposed system, the private key is $\{m_1, m_2, m_3\}, N, d\}$. The key length of the proposed system is more than the traditional RSA. Any secure cryptosystem should have a key space which is not vulnerable to exhaustive search. A large key space is necessary but not sufficient. Security relies solely on the secrecy of the private key.

Also RSA is only secured for messages, m such that $c = m^e > n$. whiles in the proposed system, more information about the moduli set will be needed in order to decipher the cypher text regardless of the length of the messages, m . The following illustrates the point;

Let $p = 13, q = 17, e = 5$ (e is an odd public exponent between 3 and $n - 1$ that is relatively prime to $p - 1$ and $q - 1$)

Then $N = pq = 221, \phi(N) = (p - 1)(q - 1) = 192$

Which implies $e.d = 1 \bmod \phi(N)$. Therefore $d = 77$

To encrypt the binary message $m = 10$ with respect to the key $pk = (N = 221, e = 5)$, taking m as 2 (hence an element of $Z_n = 221$) in the natural way. Computing $c = 2^5 \bmod 221 = 32$. We have $c = 32$ which is less than n . So taking e^{th} root of $c = 32$ will recover the original message with ease. That is $\sqrt[5]{32} = 2$.

The proposed system will transform $c_1 = 32$ into $c_2 = (2, 4, 5)$ and only a knowledge of the pk_2 which is the moduli set can recover the original $c_1 = 32$.

TABLE I
RSA RESULTS EVALUATION

Message(m)	m^e	Cipher text (c)	$e\sqrt[c]{c}$	Key-Length
10	1000000	196	70	7-bits
5	500000	98	49.497	7-bits
2	32	32	2	7-bits

In the table above, transmitting 10 and 5 is secured because m^e is greater than $n = 221$. Therefore taking the $e\sqrt[c]{c}$ will not recover the message, m . Transmitting 2 however is not secured because m^e is less than $n = 221$. Taking e^{th} root of $c = 32$ will recover the original message without the knowledge of the prime numbers.

TABLE II
PROPOSED SYSTEM RESULTS EVALUATION WITH (5, 7, 9) MODULI SET

Message(m)	m^e	C_1	C_2	Key-Length
10	1000000	196	(1, 0, 7)	16-bit
5	500000	98	(3, 0, 8)	16-bit
2	32	32	(2, 4, 5)	16-bit

In the table above, transmitting 12, 5 and 2 are secured because the second level of encryption will transform C_1 into C_2 . This will not only cause more confusing to the hacker, but also enable the message 2 to be encrypted. The key-length in the proposed system is enhanced because the moduli set are part of the private component of the classical RSA cryptosystem. The security of a cryptosystem is proportional to the length of the private key.

VII. CONCLUSION

In this work, the RSA cryptosystem is further enhanced through a two level encryption scheme. The first level is the traditional RSA encryption and in the second level, we applied RNS where the moduli set are part of the private key for the deciphering process. The performance analysis indicates that small messages for which $m^e > N$ can still be encrypted with the proposed system. The analysis also showed that an adversary would need more

information about the moduli set before he can break into the proposed system. This improves the cryptosystem of the traditional RSA encryption system, and consequently increases the quality of service in the communication system.

REFERENCES

- [1] Salifu Abdul-Mumin. Detection of Man-in-the-Middle attack in Computer Network, i-manager's Journal on Communication Engineering and Systems, Vol. 2 No. 1, pp. 1-8 November 2012 - January 2013
- [2] William L. Freking and Keshab K. Parhi. Modular Multiplication in the Residue Number System with Application to Massively-Parallel Public-Key Cryptography Systems, Conference of [Circuit, Systems and Computers](#), Vol. 2, pp. 1339-1343
- [3] P.W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In IEEE Symp. on Found. of Comp. Sci., pp.124-134, 1994
- [4] Paulo Martins, Leonel Sousay, Programmable RNS Lattice-Based Parallel Cryptographic Decryption, IEEE 26th International Conference on Application-specific Systems, Architectures and Processors (ASAP) pp: 149-153, 2015
- [5] Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem", RSA Laboratories. April 9, 2006
- [6] Arash Hariri, Keivan Navi, Reza Rastegar. A new high dynamic range moduli set with efficient reverse converter, An international Journal of Computers and Mathematics with Applications Vol 55, Issue 4, , pp. 660–668, February 2008
- [7] Kazeem Alagbe Gbolagade. Effective Reverse Conversions in Residue Number Systems Processors, Ph. D Theses submitted to TuDelf ,2010
- [8] Amir Sabbagh Molahosseini and Keivan Navi. New Arithmetic Residue to Binary Converters , International Journal of Computer Sciences and Engineering Systems, Vol.1, No.4, pp. 296-300 October 2007
- [9] N. S. Szabo and R. I. Tanaka, Residue Arithmetic and its Applications to Computer Technology, New York: McGraw Hill, 1967
- [10] M. A. Soderstrand, W. K. Jenkins, G. A. Jullien and F. J. Taylor, *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing* New York: IEEE Press, 1986.
- [11] Bin Cao, Chip-Hong Chang and Thambipillai Srikanthan, Adder Based Residue to Binary Converters for a New Balanced 4-Moduli Set, Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis, vol. 2 pp. 820-825, Sept 2003
- [12] Duc-Minh Pham, A. B. Premkumar, and A. S. Madhukumar, Error Detection and Correction in Communication Channels Using Inverse Gray RSNS Codes, IEEE Transactions on Communications-TCOM ,VOL. 59 no.4 pp.975 - 986 · April 2011
- [13] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, 1976 IEEE Transactions on Information Theory, VOL. 22, NO. 6, NOVEMBER 1976
- [14] J.-J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," IEE Electronics Letters, vol. 18, no. 21, pp. 905-907, Oct. 1982.
- [15] K.C. Posch and R. Posch, "Modulo Reduction in Residue Number Systems," IEEE Trans. Parallel and Distributed Systems, vol. 6, no. 5, pp. 449-454, May 1995
- [16] S. Kawamura, M. Koike, F. Sano, and A. Shimbo, "Cox-Rower Architecture for Fast Parallel Montgomery Multiplication," Advances in Cryptology, Proc. EUROCRYPT 2000, pp. 523-538, May 2000
- [17] H. Nozaki, M. Motoyama, A. Shimbo, and S. Kawamura, "Implementation of RSA Algorithm Based on RNS Montgomery Multiplication," Proc. Cryptographic Hardware and Embedded Systems (CHES 2001), pp. 364-376, Sept. 2001.
- [18] F.J. Taylor, "Residue Arithmetic: A Tutorial with Examples," IEEE Computer Society Press Los Alamitos, CA, USA vol. 17, no. 5, pp. 50-62, May 1984
- [19] Laurent Imbert, and Jean-Claude Bajard, A Full RNS Implementation of RSA, IEEE Transactions on Computers, Vol: 53 No 5, pp: 769 – 774, may 2004
- [20] M. Roshanzadeh, A. Ghaffari and S. Saqaeean, Using Residue Number Systems for Improving QoS and Error Detection & Correction in Wireless Sensor Networks, Communication Software and Networks (ICCSN), IEEE 3rd International Conference, , pp: 1- 5, may 2011