Global Scientific JOURNALS

GSJ: Volume 12, Issue 5, May 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

Improved RSA Cryptosystem Using Sequence of Reduced Residue System

Muhammad A. H[1] and Abubakar T. U.[2]

[1]Department of Science, Mathematics Unit, State Collage of Basic and Remedial Studies, Sokoto, Nigeria.

[2]Department of Mathematics, Shehu Shagari College of Education, Sokoto, Nigeria.

Abstract

Cryptography plays a huge role in our technological daily life, and we are highly depending on the science of hiding information in plain sight. There are numerous ways to achieve this, where mathematics plays an important role in cryptography to ensure that information cannot be easily recovered for unauthorized person. One of the most reliable and secure encryption algorithms available today is the RSA algorithm, which provides great encryption and performance using asymmetric cryptography, yet intruders and fraudsters are still having their way. This paper provides a unique RSA cryptosystem which comprises the use of Sequence of Reduced Residue System. The result showed that the improved RSA algorithm is more secured and very difficult to attack than the normal RSA algorithm.

Keywords: Factorization, Cryptanalysis, Encryption, Decryption, attacks and Residue.

1.0 Introduction

Cryptography is the study of secure communications techniques that allow the sender and intended recipient of a message to view its contents, (Hassan, Garko, Sani, Abdullahi and Sahalu, 2023). It is the process of transferring information securely, in a way that no unwanted third party will be able to understand the message. Basically there are four objectives of cryptography: Authentication (the process of proving one's identity), Privacy/confidentiality (ensuring that no one can read the message except the intended receiver), Integrity (assuring the receiver that the received message has not been altered in any way from the original), Non-repudiation (a mechanism to prove that the sender really sent the message), (Zulkarnaini and Muhammad, 2013).

There are two types of cryptosystems based on the number of keys involved. These are Symmetric-key Cryptosystem and Asymmetric-key cryptosystem.

In Symmetric Key Cryptosystem, encryption and decryption algorithm uses the same key for conversion of plain text to cipher text and vice versa.

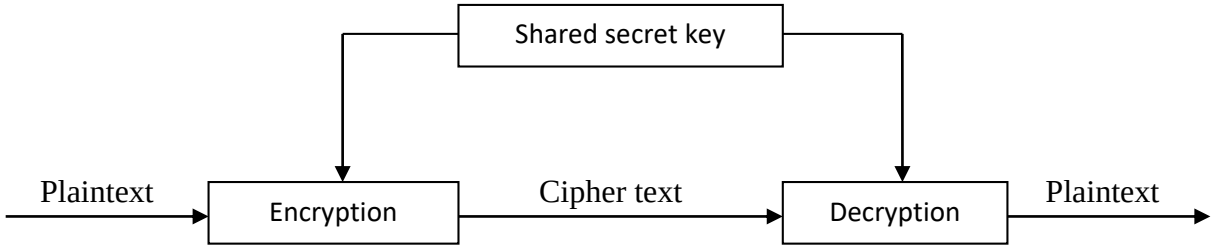

Figure 1: Symmetric key encryption/decryption scheme, (Schneier, 1996).

While, Asymmetric key cryptography, a pair of keys, namely secret-key (or private key) and public-key are used for encryption and decryption process. Whitfield Diffie, Martin Hellman and Ralph Merkle introduced the concept of Asymmetric-key Cryptosystem as cited in (Schneiner, 1996). Although they are different, the pair of keys is linked with mathematical function. The public key is used to encrypt plain text and private key is used to decrypt the cipher text.

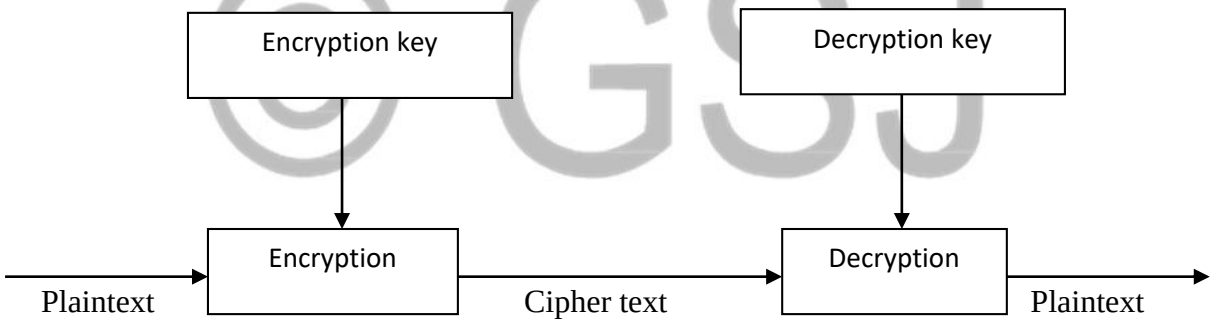

Figure 2: Asymmetric key encryption/decryption scheme, (Schneier, 1996).

The most popular public key cryptosystem in use today is the RSA cryptosystem, introduced by Rivest, Shamir and Adleman in 1977, (Ibrahim, Muhammad, Shehu, Abubakar, Zaid and Bello, 2021). The acronym “RSA” come from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman. It is the first known algorithm using different key for encryption and decryption. RSA is very widely used in electronic commerce protocols, and its security is based on the fact that it is hard to attack as it involves large integer factorization problem and it has been extensively used for many applications in the government as well as commercial domain, which include e-banking,

secure telephone, smart cards, and communications in different types of networks (Dubey, Ratan, Neelam and Saxena, 2014).

The RSA algorithm involves three paces: key generation, encryption and decryption.

1.1 Key Generation in RSA

In RSA two keys are generated; a public key and a private key. The public key is used for encrypting messages which can only be decrypted using the private key.

The keys for RSA are generated in the following steps:

Step I: Choose two distinct large random primes p and q.

Step II: Compute $N = pq$. This N is used as the modulus for both the public and private keys

Step III: Compute $\varphi(N) = (p - 1)(q - 1)$

Step IV: Choose an integer e such that $1 < e < \varphi(N)$ and GCD $(e, \varphi(n)) = 1$

Step V: Compute d to satisfy $ed - k\varphi(n) = 1$

Thus, RSA key generation involves a random selection of two distinct large prime numbers such that their product is represented as $N = pq$ and called an RSA modulus. The Euler Totient function $\varphi(N)$ is computed as $\varphi(N) = (p - 1)(q - 1)$. Additionally, choose an integer $e < \varphi(N)$ such that GCD$(e, \varphi(N)) = 1$ and compute short decryption exponent d such that the relation $ed - k\varphi(n) = 1$ is satisfied. Then, (e, N) are the public keys and (d, p, q) are private keys, (Ibrahim, et al., 2021).

Encryption: The encryption function is computed by choosing a message $M \in \mathbb{Z}_N$ and computing the cipher text $C \equiv M^e (mod\ N)$.

Decryption: The plaintext can be recovered by computing the decryption exponent from equation $M \equiv C^d (mod\ N)$. The primes $p\ and\ q$ in most cases are considered to have same bit-length, (Ariffin, Abubakar, Yunos. and Asbullah, 2018).

1.2 Statement of the Problem

The modern era of this present world is dominated by paperless transaction in business, private and governmental offices by means of e-mail and other media platforms. Due to this, there is a great need of securing data through internet, and the confidentiality and integrity of such important information should be maintained. Hence there is a need to develop a stronger and more secure ciphers that will overcome the shortcomings and weaknesses of the normal RSA. In view of that, the paper is going to carry out on the construction and improving RSA cryptosystem using sequence of Reduced Residue System for a better security.

1.3 Aim and Objectives

This paper is aim to come up with an improved RSA cipher that provides better security in data transmission compared to the normal RSA. This aim can be achieved through the following objectives:

1. To analyze the weaknesses of the normal RSA
2. To come up with improved cryptographic technique by using sequence of Reduced Residue System which will overcome the weakness of the normal RSA.
3. To use the proposed system to encrypt and decrypt a message.
4. To analyze the improved algorithm.

2.0 Literature Review

A lot of scholars have done various works in the field of RSA cryptosystem to improve data security. The first attack on small decryption exponent was reported by Wiener in 1990. He showed that RSA is unsecured if the small decryption exponent $d < \frac{1}{3}N^{1/4}$. Since then, many attacks on short decryption exponents emerged, which improved the bound (Wiener, 1990 as reported by (Ariffin, et al., 2018). (Ibrahim, et al., 2021), applied Wiener's technique in RSA and developed three new attacks, in which they showed an improved secret decryption exponent bound which is considered to be better than that of Wiener's bound. (Prakash, Saeed, Rajan, Mohammad and

Ahmed, 2023), in their paper title "A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm". Their algorithm scheme is a combination of the well-known Rivest Shamir Adleman (RSA) algorithm and a simple symmetric key (SSK) algorithm. Their proposed hybrid cryptographic algorithm provides more security and privacy. (Hassan, et al., 2023), work on improving the security of data using a combination of Hill cipher and a Transposition cipher (Gp), (Rajput, Naik and Mane, 2014), improved cryptographic Technique using double encryption and discusses an approaches in improving transposition cipher systems.

2.1 RSA Encryption/Decryption Process

To encrypt a plain text in RSA cryptosystem, let us assign a numerical value to each letter of the alphabet as shown in table 2 below:

Table 2: Relation Between Alphabets and Their Numerical Values

A	B	C	D	E	F	G	H	I	J
000	001	002	003	004	005	006	007	008	009

K	L	M	N	O	P	Q	R	S	T
010	011	012	013	014	015	016	017	018	019

U	V	W	X	Y	Z
020	021	022	023	024	025

Using RSA to encrypt and decrypt the statements "GOOD RESULT"

Key Generation

Let $p = 23$ and $q = 17$

- Compute $N = pq = 391$

- Compute $\varphi(N) = (p-1)(q-1) = 22 \times 16 = 352$
- Select e: $\text{GCD}(e,\ \varphi(N)) = 1$, let $e\ = 7$

To have: $352 = 7 \cdot 50 + 2$

$7 = 2 \cdot 3 + 1$

$2 = 1 \cdot 2 + 0$

Thus, $\text{GCD}(7,\ 352) = 1$

- Determine d: $d \times e\ \equiv\ 1\ (mod\ \varphi(N))$

That is to have d such that: $ed - k\varphi(N) = 1 \Longrightarrow 7d - 352k = 1$

Solving the above Euclidean algorithm for GCD backward:

$1 = 7 - 2 \cdot 3$

$= 7 - (352 - 7 \cdot 50) \cdot 3$

$= 7 \cdot 151 - 352 \cdot 3$

Comparing the above with $ed - k\varphi(N) = 1$, we have $d = 151$

Public key $e_k = (7,\ 391)$

Private key $\text{d}_\text{k} = (151,\ 352)$

Encryption process

To encrypt we use $C\ \equiv\ M^e (mod\ N)$.

$\boldsymbol{M} \longrightarrow \mathbb{Z}_N$	**Encryption**
G ⟶ 006	$6^7\ \ mod\ 391 = 371$
O ⟶ 014	$14^7\ \ mod\ 391 = 0295$
O ⟶ 014	$14^7\ \ mod\ 391 = 0295$
D ⟶ 003	$3^7\ \ mod\ 391 = 0232$
R ⟶ 017	$17^7\ \ mod\ 391 = 0204$
E ⟶ 004	$4^7\ \ mod\ 391 = 0353$

S ⟶ 018 $18^7 \ mod\ 391 = 0052$

U ⟶ 020 $20^7 \ mod\ 391 = 0113$

L ⟶ 011 $11^7 \ mod\ 391 = 1950$

T ⟶ 019 $19^7 \ mod\ 391 = 2161$

The cipher text is: 037102950295023202040353005201131950216 1

Decryption process

To decrypt we use $M \equiv C^d (mod\ N)$

$0371^{151} \ mod\ 391 = 0006$ → G

$0295^{151} \ mod\ 391 = 0014$ → O

$0295^{151} \ mod\ 391 = 0014$ → O

$0232^{151} \ mod\ 391 = 0003$ → D

$0204^{151} \ mod\ 391 = 0017$ → R

$0353^{151} \ mod\ 391 = 0004$ → E

$0052^{151} \ mod\ 391 = 0018$ → S

$0113^{151} \ mod\ 391 = 0020$ → U

$1950^{151} \ mod\ 391 = 0011$ → L

$2161^{151} \ mod\ 391 = 0019$ → T

Hence, the plaintext is 'GOOD RESULT' after replacing the numerical value back to letters.

2.2 Cryptanalysis of RSA Cryptosystem

There are several ways of attacking RSA mathematically, among which are:

i. Factoring the modulus N into its two prime factors, this enables calculation of $\varphi(N) = (p - 1)(q - 1)$, which in turn enables determination of $d = e^{-1} \ (mod\ \varphi(N))$.

ii. Determine φ(N) directly, without first determining p and q, hence enables determination of $d = e^{-1} (mod\ \varphi(N))$.

iii. Determine d directly, without first determining $\varphi(N)$.

For instance, using trial division factoring method that an integer N is coprime if it has a divisor $\leq \sqrt{N}$, we have:

$$\sqrt{N} = \sqrt{391} = 19.774$$

This implies there exist a prime number $p \leq 19$ that can divide 391.

Prime numbers to be tested with are: $19, 17, 13, 11, 7, 5, 3, 2$

$$19 \nmid 391, \qquad 17|391$$

That is $\frac{391}{17} = 23 \quad \Rightarrow N = 23 \times 17$, thus, $p = 23,\ q = 17$

Hence, $\varphi(N) = 22 \times 16 = 352$

Using $d = e^{-1}\left(mod\ \varphi(N)\right)$, with $e = 7$, we have $d = \frac{1}{7}\ (mod\ 352)$

$\Rightarrow$ there exist $k \epsilon \mathbb{Z}$ such that $7d - 352k = 1$

Computing the GCD of $(7, 352)$:

$$352 = 7 \cdot 50 + 2$$

$$7 = 2 \cdot 3 + 1$$

$$2 = 1 \cdot 2 + 0$$

Thus, $\text{GCD}(7,\ 352) = 1$

Solving the above Euclidean algorithm for GCD backward:

$$1 = 7 - 2 \cdot 3$$

$$= 7 - (352 - 7 \cdot 50) \cdot 3$$

$$= 7 \cdot 151 - 352 \cdot 3$$

Comparing the above with $7d - 352 = 1$, we have $d = 151$

Hence, the decryption exponent has been recovered.

3.0 Methodology

This section will present definitions and some important theorems to be employed in this paper.

Least Residue

If $m > 0$ and r is the remainder when the division algorithm is used to divide n by m, then r is called the least residue of $n\ modulo\ m$, (Rosen, 2011).

Theorem 1

If t and n are integers such that $t \equiv n(mod\ m)$ and $0 \leq t < m$, then t is the least residue of $n\ modulo\ m$.

Example:

The least residue $(mod\ 7)$ to which *25* is congruent is 4

Since $25 = 7 \cdot 3 + 4\ \ i.e. 25 - 4 = 7 \cdot 3$

hence, $25 \equiv 4\ (mod\ 7)$ and $0 < 4 < 7$

$\therefore$ the least residue is 4.

Residue Classes

A residue class $(mod\ m)$ is a set of $m - integers$ which are congruent to each other $(mod\ m)$ and any member of the set can be chosen to represent it. Thus, each residue class contains exactly one of the integers in the set of possible remainders, that is, $\{0, 1, 2, \dots, m - 1\}$

Examples: For a congruent relation under $(mod\ 4)$ there is 4-classes of residue; i.e. $\mathbb{Z}_4 = \{0,1,2,3\}$. Thus, the four classes are $0 + 4k,\ 1 + 4k,\ 2 + 4k,\ 3 + 4k$, where k is any integer.

i) The set $\{-12, -8, -4, 0, 4, 8, \dots\}$ has a common least residue of 0 under $(mod\ 4)$, $\because\ -12 = 4(-3) + 0, -8 = 4(-2) + 0$ etc.

ii) The set $\{-19, -15, -11, -7, -3, 1, 5, 9, \dots\}$ has a common least residue of 1 under $(mod\ 4)$, $\because\ 4|(-11 - 1), 4|(9 - 1)$, etc.

Reduced Residue System

A list of $\phi(m)$ incongruent integers (where $\phi(m)$ is an Euler number which correspond to the number of integers that are relatively prime to m) such that each member belongs exactly to the

residue class $(mod\ m)$ which are relatively prime to m. Thus, a set S constitutes of reduced residue system modulo m if it satisfies the following conditions:

i) $n(S) = \phi(m)$

ii) $a_i \not\equiv a_j (mod\ m)$

iii) $(a_i, m) = 1$, (Rosen, 2011).

Example: the set $S = \{-1, 7, 13, 11, 14, 19\}$ constitute of reduced residue system $\phi(m)$; since

i) $n(S) = \phi(9) = 6$ $ii)\ a_i \not\equiv a_j (mod\ m)$ $iii)\ (a_i, 9) = 1$

That is $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\mathbb{Z}_{\varphi(9)} = \{1, 2, 4, 5, 7, 8\}$

Thus, $\{-1, 7, 13, 11, 14, 19\} = \{19, 11, 13, 14, 7, -1\} \equiv \{1, 2, 4, 5, 7, 8\}\ (mod\ 9)$

Reduced Residue Theorem

If $r_1,\ r_2, \dots,\ r_{\varphi(n)}$ is a reduced residue system modulo n, and if a is a positive integer with $(a, n) = 1$, then the set $ar_1,\ ar_2, \dots,\ ar_{\varphi(n)}$ is also a reduced residue system modulo n.

Proof

To show that each integer ar_j is relatively prime to n, we assume that $(ar_j, n) > 1$. Then, there is a prime divisor p of (ar_j, n) . Hence, either pIa or pIr_j. Thus, we have either pIa and pIn, or pIr_j and pIn. However, we cannot have both pIr_j and $p\ I\ n$, because r_j is a member of a reduced residue system $modulo\ n$, and both p I $a\ and\ p$ I n

4.0 Proposed Algorithm

Normal RSA does not provide a very high level of security; however, by modifying it using Sequence of Reduced Residue System we will obtain a strong cipher.

4.1 Improved Algorithm:

I. Choose: a positive integer n

II. **Compute** $\mathbb{Z}_{\varphi(n)}$ such $\varphi(n) \geq 26$

III. **Select** $R = \{r_0, r_1, \ldots, r_{25}\}$ such that $r_i \in \mathbb{Z}_{\varphi(n)}$

IV. Express alphabets $A, B, \ldots, Y, Z$ in numerical form r_i such that $r_i \in R$

V. Replace Plaintext P in numerical form in which $P \subset R$

Input: an RSA prime modulus $N = pq$ with $q < p < 2q$, and public key (e, N)

Output: The private key (N, d).

1. Choose two random and distinct n - bit strong primes (p, q).

2. **for each** pair of the form (p, q) **do**

3. **Compute** $N = pq$

4. **Compute** $\varphi(N) = (p-1)(q-1)$

5. **Select** e: $\mathrm{GCD}(e, \varphi(N)) = 1$

6. **Determine** d: $d \times e \equiv 1\ (mod\ \varphi(N))$

7. **Publish** public key $e_k = (e,\ N)$

8. **Store** private key $\mathrm{d_k} = (d,\ \varphi(N))$

9. **Encrypt** message: $C \equiv {r_i}^e (mod\ N)$

10. **Decrypt** message: $r_i \equiv C^d (mod\ N)$

11. Replace r_i message to plaintext

12. **End**

4.2 Encryption and Decryption with the Improved Algorithm

Suppose we want to encrypt the message 'GOOD RESULT'

Let $n = 58$

$\mathbb{Z}_{\varphi(58)} = \{0,1,\ldots,57\}$ with $R_i \in \mathbb{Z}_{\varphi(58)},\ 0 < R_i < 57$

Relation Between Alphabets and their Numerical Values Based on the Sequence

A	B	C	D	E	F	G	H	I	J
003	005	007	009	011	013	015	017	019	021
K	L	M	N	O	P	Q	R	S	T

023	025	027	031	033	035	037	039	041	043
U	V	W	X	Y	Z				
045	047	049	051	053	055				

Table 2

Encryption process using the improved Algorithm

To encrypt we use $C \equiv r_i{}^e (mod\ N)$.

$\boldsymbol{M} \longrightarrow \mathbb{Z}_N$	**Encryption**
G $\longrightarrow$ 015	$15^7 \ mod\ 391 = 0195$
O $\longrightarrow$ 033	$33^7 \ mod\ 391 = 0152$
O $\longrightarrow$ 033	$33^7 \ mod\ 391 = 0152$
D $\longrightarrow$ 009	$9^7 \ mod\ 391 = 0257$
R $\longrightarrow$ 039	$39^7 \ mod\ 391 = 0248$
E $\longrightarrow$ 011	$11^7 \ mod\ 391 = 0122$
S $\longrightarrow$ 041	$41^7 \ mod\ 391 = 0029$
U $\longrightarrow$ 045	$45^7 \ mod\ 391 = 0275$
L $\longrightarrow$ 025	$25^7 \ mod\ 391 = 0151$
T $\longrightarrow$ 043	$43^7 \ mod\ 391 = 0274$

New cipher text is: 019501520152025702480122002902750151027 4

Decryption process

To decrypt we use $r_i \equiv C^d (mod\ N)$

$195^{151} \ mod\ 391 = 015$ $\rightarrow$ G

$152^{151} \ mod\ 391 = 033$ $\rightarrow$ O

$152^{151} \ mod\ 391 = 033$ $\rightarrow$ O

$257^{151}\ mod\ 391 = 009 \rightarrow$ D

$248^{151}\ mod\ 391 = 039 \rightarrow$ R

$122^{151}\ mod\ 391 = 011 \rightarrow$ E

$029^{151}\ mod\ 391 = 041 \rightarrow$ S

$275^{151}\ mod\ 391 = 045 \rightarrow$ U

$151^{151}\ mod\ 391 = 025 \rightarrow$ L

$274^{151}\ mod\ 391 = 043 \rightarrow$ T

Hence, the plaintext is 'GOOD RESULT' after replacing the numerical value back to letters

Conclusion

RSA algorithm is a strong algorithm for data security but yet attackers are still having their way as illustrated in the paper. RSA cryptosystems relies on the difficulty of factoring very large numbers and if there is an algorithm that can decompose a large number fast, the RSA algorithm's security would be threatened. In this paper we provide an improved RSA cryptosystem which comprises the use of Sequence of Reduced Residue System. The improved method provides more secured and stronger cipher than the normal RSA. The advantage of the improved system is that; it provides better security because even if some component ciphers are broken or some of the secret keys are leaked the confidentiality of the original data can still be maintained.

References

Ariffin, M., Abubakar, S., Yunos F. and Asbullah, M, (2018). New Cryptanalytic Attack on RSA Modulus N = pq Using Small Prime Difference Method. *Malaysia Journal of Mathematical Sciences* **3**(1).

Dubey, M. K., Ratan, R., Neelam, V. and Saxena, P. K., (2014). Cryptanalytic Attacks and Countermeasures on RSA. In Proceedings of the *Third International Conference on Soft Computing for Problem Solving; Springer: New Delhi, India*, 805–819.

Hassan, A., Garko, A., Sani, S., Abdullahi, U., and Sahalu, S. (2023). Combined Techniques of Hill Cipher and Transposition Cipher. Journal of Mathematics Letters, **1**(1), 57–64

Ibrahim, A. A., Muhammad, A. H, Shehu, S., Abubakar, T. U., Zaid, I. and Bello, U. (2021). Cryptanalysis on RSA Using Decryption Exponent. IOSR Journal of Mathematics (IOSR-JM), **17**(5), 01-08

Prakash, K., Saeed, Q. Y. A., Rajan, J., Mohammad, H. and Ahmed, A. S. M. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics.* **12**(2), 1148-1158. DOI: 10.11591/eei.v12i2.4967

Rajput, Y., Naik, D. and Mane, C. (2014), An improved cryptographic technique to encrypt Text message using double encryption. *International Journal of Computer Applications*. **86**(6), 24-28.

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms and Source Code in C. *John Willey, New York,* 2nd edition.

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms and Source Code in C. *John Willey, New York,* 2nd edition.

Zulkarnaini, M. D. and Mohammad, A. J., (2013). New Computation Technique for Encryption and Decryption Based on RSA and El-Gamal Cryptosystems. *Journal of Theoretical and applied Information Technology*, **47**(1), 74-76.