(IJESIR) International Journal of Science and Innovative Research
e-ISSN: 2724-3338
2021, 02(08)
https://novuspublishers.org/ Paper id: 0100069IJESIR

New RSA Scheme For Improved Security

O. Sarjiyus, B.Y Baha and E.J Garba

Department of Computer Science Moddibo Adama University of Technology, Yola, Nigeria

ARTICLE INFO

Received: 05.08.2021
Accepted: 29.08.2021
Final Version: 29. 09.2021

***Corresponding Author:**

O. Sarjiyus
sarjiyus@gmail.com

ABSTRACT

The research, New RSA scheme for improved security is imperative due to the growing number of challenges and threats to data security in a network brought about by the growing number of techniques used by intruders to penetrate and overwhelm the security of data in terms of breaking data confidentially, integrity and authenticity. The study aims at modifying the existing RSA technique which is prone to so many forms of attacks, in order to develop a more expansive and secure scheme by obtaining more robust and efficient secret keys which are a function of the newly derived functionality f generated in place of n, thus making it almost impossible to correctly guess the private key and even factorize n or ø(n). This is achievable since instead of using n to tie the keys (e,n) and(d,n) a number t is obtained between n-p and n and defined on the interval n-p<t<n and used for the encryption and decryption process and overcoming factorization attacks to a very large extend.

Keywords: Decryption, Encryption, Intruders, key, Security Threats.

Introduction

Worldwide, the current trend focuses on the use of cryptographic mechanisms to secure the transmission of sensitive data through conventional channels. Fundamentally, the rationale behind the use of cryptography has to do with the practice of enabling data to be communicated over insecure, conventional channels such that an attacker does not in any way intercept, penetrate and alter the contents of data. In this case the sender encrypts a plaintext (message, *m*) using the public key, *e* and transmits it via the communication channel (Internet). At the receiving end, the recipient uses the private/ secret key, *d* (known only to him) to decrypt the encrypted message back to its original form while at the same time accomplishing such purposes as data secrecy/confidentiality, authenticity and integrity. However, the data transferred through network channels faces some threats all in a bid to uncover the secret information being transmitted. Developing more information technology platforms often results to raising levels of Cyber threats and vulnerabilities of the data in insecure channels [1]. To curb these problems, researchers are developing various techniques to discover unconventional alternatives to improve the security of transmitted data by ensuring data gets to the recipient untempered, unaltered. At present, various enhanced algorithms have been simulated and are known to provide much better security; but such sophisticated algorithms could be very expensive and known to consume much computational resources. As it is known, cryptography is the procedure used to protect sensitive data over a conventional network channel, which may not be necessarily secure being a public channel, in such a way and that the data gets to the recipient unaltered. In modern times, the subject of data confidentiality becomes a very crucial issue in information security. Easy administration of the Internet today and data globally led to the importance of data security even

though, its emergence has created new dangers for users who want their data to remain safe. As it is, hackers are using a diversity of techniques to penetrate and break into information transferred through the channel and steal the information or alter the original data content [2: 3].

Nowadays, cryptography algorithms afford a high level of confidentiality by concealing private data of any individual or group. Many of the ongoing researches aim at finding out the new cryptographic algorithms that are more efficient based on security and complexity [2]. Again, one secret-key cryptography algorithm could be generated and used for both approaches are known as symmetric key cryptography. This technique proves that it has lesser computational efforts but unfortunately has many drawbacks such as key management issues, which can lead to the tendency of the private key becoming compromised [4: 5]. Asymmetric cryptography algorithm uses a public-key to achieve encryption pattern and then use a private key to decrypt the ciphered information. However, asymmetric cryptography implements two different mathematical approaches, like a public key and the other, a private key. Dissimilar symmetric algorithms applied only one key to both the encryption/decryption approach [6: 7]. Moreover, the public key is stored openly and can be used to encrypt data by anyone. On the other hand, the private key is kept secret and implemented by the receiver side to decrypt the received encrypted data.

Rivest, Shamir and Adleman (RSA) in 1977 were the first to describe the algorithm that implements the public key [2]. RSA algorithm applied different keys as public/private keys but are related to a large scale of applications. As a result, reliably secured results and better security transfer of data are big prime integer numbers chosen for both the public and private keys [6: 7]. RSA applied extensively for encryption/decryption problems leading to a protected transmission of the data. RSA technique tends to have more enhanced protection when the value of the key is big enough and it becomes much more difficult to figure out its common factors. An asymmetric key means that it works on two different keys as public key and a private key. The public key should be accessible to everyone within the communication sphere but the private key is not and it is kept privately to the authorized and intended recipient only. The objective of RSA is founded on the fact that it should be hard to factorize a key because a large prime integer is chosen. This research therefore, is targeted at modifying the existing RSA scheme in a bid to develop a more expansive and secure scheme by obtaining more robust secret keys which are a function of the newly derived functionality, t generated in place of n, thus making it seemingly impossible to correctly guess the private key d and even factorize n or ø (n). This is achievable in view of the fact that instead of using n to tie the keys e,d as (e,n) and (d,n), a number t between n-p and n defined on the interval $n-p<t<n$ is used for the encryption and decryption process and so, overcoming factorization attacks to a very large extent.

This paper consists of five sections. Section one introduces the background to the research, section two reviews existing literatures in RSA cryptography, section three describes the existing methods in RSA algorithm and approaches used for the modified RSA algorithm, section four is an illustration of the workings and result of the new RSA scheme, while section five concludes the study.

Literature Review

Cryptography is the science of developing methods that allow information to be sent in a secure form in such a way that the intended recipient is the only person able to retrieve this information. It is the practice of hiding information. Cryptography is considered a branch of both mathematics and computer science in modern times, and is closely associated with computer security and engineering information theory [8]. In applications present in technologically advanced societies, cryptography is

used; examples include ATM card authentication, computer passwords, and electronic commerce, all of which rely on cryptography [**8**]. For the sole purpose of achieving secrecy, cryptography is the method of encoding messages to make them unreadable to unauthorized persons [**9**]. [**10**] Gives an insight into the principles of cryptography and various forms of cryptography. This identifies RSA and discusses its intricacies and its functions. It illustrates the various variants of the RSA algorithm in general and, on the basis of complexity and security, poses different comparisons between them.

It shows that a great deal of RSA work can be performed. In particular, the work discussed in his thesis is about the implementation of RSA on 2048-bits for multi-prime and multi power. As the proper way to protect data in the cloud, he suggested implementing the combination of these two algorithms. Flaws in security, where the keys generated are poor, are the main problem of his work, making the algorithm vulnerable to certain threats and the algorithms implemented separately.

[**11**] Using the Chinese Remainder Theorem, Multi Power RSA with N = Pm * Q is proposed for faster decryption in a more stable way. Compared to other algorithms, the suggested multi power RSACRT with N = Pm * Q was defined as taking less execution time. The suggested algorithm also provides better efficiency at the expense of a slight decrease on the decryption side. Besides all this, it provides the framework with semantic protection that is not provided by Multi Prime RSA. The algorithm was only suggested but not implemented. The main issue with this algorithm is that a hacker can predict the exponent so that the prime numbers used in key generation can be identified. [**12**] Proposed to use the Fermat's little theorem with the RSA algorithm, the little Fermat theorem was used to make it faster during key generation. In key generation, the main problem of the RSA algorithm is that it is very slow and this increases key generation time as large key size numbers are picked. This issue can be solved by applying the theorem of Fermat's little theorem during the process of key generation. In the cloud computing world, this modern approach helps to trust users. It also reduces the annoyance of RSA encryption.

[**13**] suggested a Multi-prime RSA algorithm; the middle layer algorithm was implemented before the data was stored in the cloud environment. If the data is requested by an approved user, then the data is decrypted and delivered to the user. The client sends the question to the server in the client process. The server responds to the client with the corresponding file, depending on the query. The client authorization phase is involved before this process. It checks the name of the client and its password for the authentication process on the server side.

The requests are obtained from the client if it is satisfied and the relevant files are checked in the database. Finally, the corresponding file that will be submitted to the client is retrieved. The algorithm's shortcoming is that it can be targeted with brute force. [**9**] Suggested the development of a hybrid cryptographic algorithm to improve cloud computing data security. The combination of two modern cryptography algorithms, the multi-prime RSA and MD5 algorithms, was used to construct this algorithm. In the proposed algorithm, multi-prime RSA was used for data encryption and the MD5 was used to produce a message digest and simultaneously append a digital signature. Compared to many other current algorithms, the proposed algorithm has been found to be efficient in terms of speed and requires less memory space. Therefore, it has been found that those same risks and attacks that contradict cryptographic algorithms can be resisted. The key problem with their work is that the algorithm used is restricted only to solving Internet data protection issues and cannot be used to solve other types of problems of digital communication. Similarly, in [**14**] they used 'n' prime numbers that provide network protection. In which they tried to get the consistency that makes it easier for cryptography to use 'n' prime numbers well. A very important feature in the RSA cryptosystem is the 'n' prime numbers (plays). The RSA algorithm for 'n' prime numbers was developed and four

prime numbers were also used. No qualitative measurement has been performed in this paper and only shows the involved method.

Based on the analysis of [**15**], an algorithm is suggested for RSA as a method for implementing a public-key cryptosystem (RSA) using two public keys and some mathematical relationships, and Sreenivasarao. These two public keys are sent separately, which makes it difficult for the intruder to get a great deal of information about the key and to decrypt the message. For systems that require high protection but with less speed, the proposed RSA is used. In the thesis undertaken by [16] an analysis of number theory and public key cryptosystems is based on this enhancement of the more stable RSA cryptosystem for brute force attack. The RSA cryptosystem generates one public key to encrypt the document. While it is difficult to figure out the n factors and get p and q, two big prime numbers, in the suggested algorithm, brute force attack is therefore more difficult as the encryption keys are sent separately, not at once. For systems that require high protection but with less speed, the proposed RSA is used [**16**].

Existing RSA Algorithm

Generally, the RSA algorithm is an asymmetric key crypto- system which is a function of the supposition that it is hardly possible to find component prime factors making up the large integer value, n of modulus. The security strength of RSA scheme is also based on the fact that the encryption function is one way and so, it is mathematically infeasible for an attacker to decrypt a ciphered text. But in practice, in the conventional RSA technique there is a correspondence between and a relationship between the public key and the private key which is based on the principle that the public and private to the sender to encode data and to the receiver to decode the encoded messages respectively. With this, there is a likelihood that an intruder discovers this relationship and successfully derives the secret key.

RSA techniques operate mainly on three (3) phases;

- Phase 1 involves the key generation process where the public key e, and the private key d are generated.
- Phase 2 involves using the public key e generated to encrypt data.
- Phase 3: this is the decryption stage where the encrypted data is received by the recipient and decrypted using the private key, d.

More elaborately;

Phase 1(key generation)

i. Select two very large prime integers, P and q
ii. Compute the value of the modulus, n such that: n= pxq (the length of the modulus is termed the key length expressed in bits)
iii. Compute the Euler's function, also called the totient function ø(n), such that: ø(n) =(p-1)x(q-1).
iv. Determine the public key value, e satisfying the condition;
    a. gcd (e, ø(n))=1 where: 1<e< ø(n)
v. Hence, public key, e is a function of e, n; that is(e,n)
vi. The private key, d is obtained from the relation
    {d*e mod n=1}; Hence private key d is defined in terms of d and n, that is: (d,n)

Phase 2 (encryption phase).

Given the message, m which is to be encrypted by public key, e from the sender; the encryption phase C is defined as:

$C= M^e \bmod (n)$

Phase 3(decryption phase)

As the encrypted data gets to the recipient, the private key, *d* is used to decrypt the message as;

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

So as to obtain the original message, *m.*

Drawbacks of the existing RSA scheme

i. Often times, the intruders tend to encrypt a message using the public key, e and then by trial and error, if the encrypted message matches it, the secret message becomes known.

ii. The public key, *e* is usually transmitted alongside the modulus, *n*, (*e,n*) thereby making room for vulnerability since attackers can subject n to factorization attack by trial and error to get the component factors of *n* and factoring *n* means getting the totient function ø(n) with the possibility of easily getting the private key functionality, *d*.

Approach for the modified RSA scheme

The modification of the existing RSA scheme seeks to introduce two additional security levels in order to remove n from the key (replacing it with new value, *t*) and do away with the possibility of tracing the component values of n; i.e. *p* and *q* by factorization.

This occurs during the key generation phase in which n becomes substituted by a new functionality, t which is inherently used for the encryption and decryption process. The new RSA scheme is also made up three (3) phases- key generation phase were the modification occurs, the data encryption phase and the data decryption phase.

Basically, for the new RSA scheme we are applying a mathematical transformation over *n* to get a replacement for it which clearly makes it hard for the intruder to find the component factors of the modulus ø. By this arrangement, the security modified RSA scheme is raised to second layer security level which improves the security of the new RSA scheme to a greater extent.

The modification process of the RSA scheme is illustrated below:

Phase 1; key generation

i. Select two very large prime integers p and q

ii. Compute the value of the modulus, n such that: n= p*q

iii. Compute the Euler's function ø (n) defined by: ø (n) = (p-1)*(q-1).

iv. Derive public key, e from the condition;

a) $\sqrt{n}<e<n$.

b) gcd (k, ø(n)) =1. k and ø(n) are co prime.

v. Get t to replace n.

Given q<p then put t such that

a) (n-p)<t<n

b) gcd (k, ø(n)) =1

vi. Compute d from the relation;

d*e mod(t) =1

And so,

Public key is (e, t)

Private Key is (d, t)

Phase 2; Encryption Phase

Sender then encrypts plaintext (message), M using public key, (e,t) as;

$C=M^e \bmod (t)$

Phase 3; Decryption Phase

Recipient receives and decrypts the encrypted message with private key, (d,t) as;

$M=\sqrt{(C^d \bmod (t))}$.

Using the conventional RSA scheme, the keys, *e* and *d* are tied to the large integer number, *n* (the modulus) which is made up of two prime components, *p* and *q* with the public key known to both parties. It is easily possible for an intruder to compute the private key, *d* if the intruder can correctly guess the component factors making up *n* (by brute force attack). In a bid to eliminate the possibility of a brute force attack the RSA algorithm to modified to eliminate the n distribution in the public and private keys and instead replace the n distribution with a new value *t* within the range $(n-q)<t<n$ while still satisfying same conditions stipulated for n.

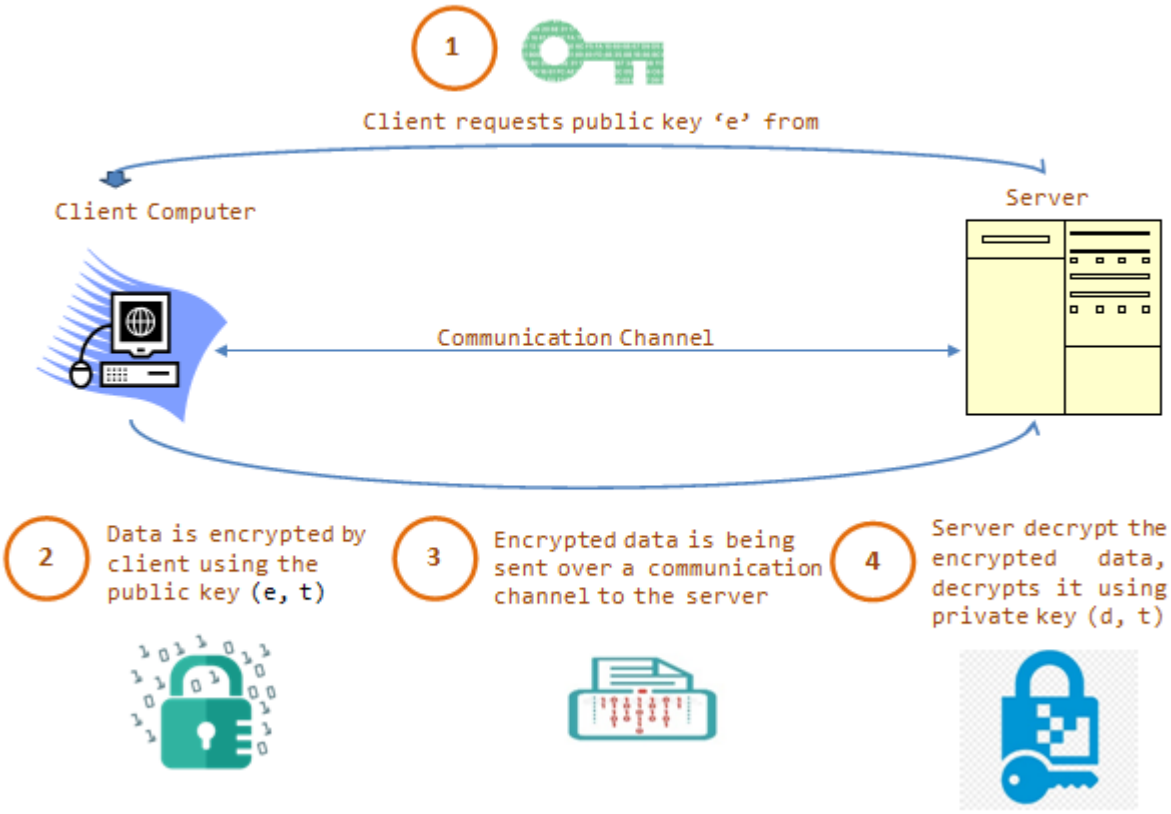

Figure 1: Proposed diagram for System

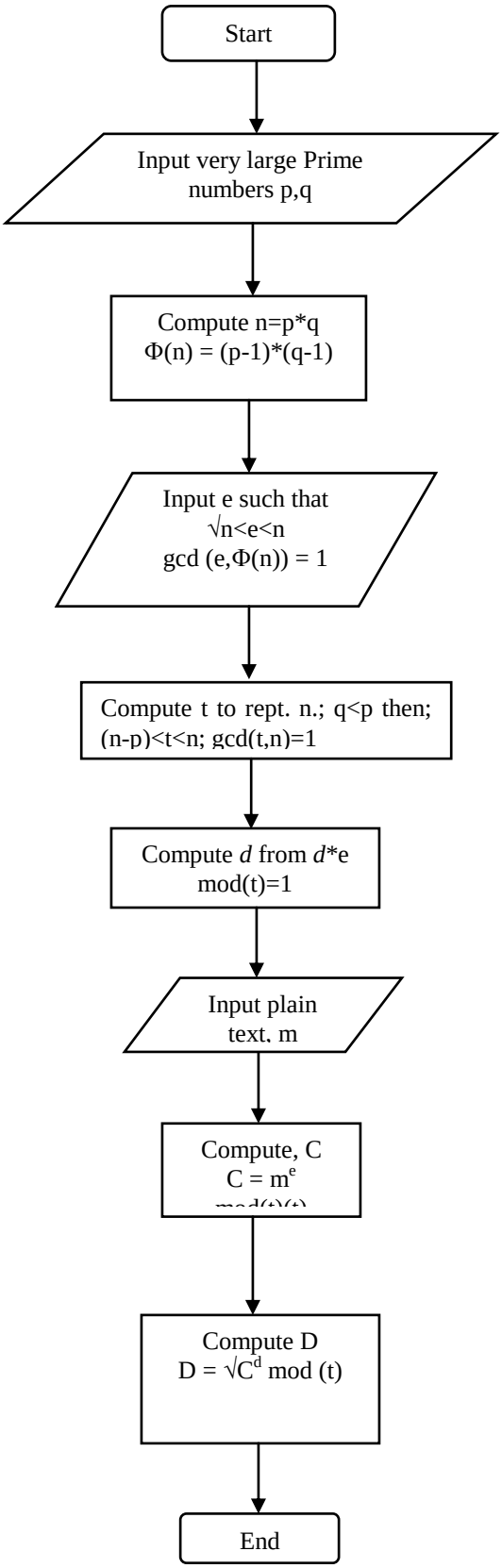

Figure: 2 Flowchart for the system

Illustration

i. p=7,q=11

ii. compute modulus, n

n= p*q

n=7*11

n=77

iii. Compute the Euler's totient function ø(n);

ø(n)=(p-1)*(q-1)

ø(n)=6x10

ø(n)=60

iv. Determine the public key, e;

$\sqrt{n}$<e<n

e must be coprime to n

$\sqrt{77}$<e<77

8.9<e<55

e=8.9

v. Compute t;

If p>q

(n-p)<t<n

t must be co-prime to n

But if p<q

(n-q)<t<n

t must be co-prime to n;

But to find d (the private key)

d*e mod t=1

In this illustration;

q>p

so that 77-11<t <55

66<t<77

Put t= 67

d*e Mod 67=1

d*q mod 67=1

Hence using extended Euclidean algorithm, d=15

Step 6:

Sending the public key e and private key d entails;

Public key= (t, e) = (67, 9)

And private key= (t, d) = (67, 15)

Step 7:

Sending or encrypted message with m=4;

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

$C= 4^9 \bmod (67)$

C= 262144 mod (67)

C= 40

Step 8:

The encrypted message is decrypted as;

$D= \sqrt{} (c^d \bmod (t))$

$D= \sqrt{}(40^{15} \bmod (67))$

D=4

To clearly show the working of the new RSA scheme, an illustration was used in this research to show all the steps involved from key generation phase, encryption phase to decryption. The peculiarity of the new RSA scheme is that after obtaining the modulus *n* and Eulier'sTotient function ø(n), we used the relation $\sqrt{n}<e<n$ to determine the value of *e*, using $(n-q)<t<n$ to determine the value of *t* and *t* being co-prime to *n* and in turn using $d*e \bmod(t)=1$. To determine the value of the private key *d* in terms of the new *t* transform. Finally, the encryption and decryption processes were carried out in terms of *t* as $C=M^e \bmod(t)$ and $D = \sqrt{C^d} \bmod(t)$ respectively with *t* as the hidden security layer around *n*.

Conclusion

A model of the new, enhanced RSA scheme has been shown in this research. To improve protection, *n* was transformed to *t*, thus providing the original RSA scheme with additional secret layers of security, so that both e and d were used for encryption and decryption in *t* instead of n. Therefore, it is difficult to use factorization attacks to obtain the component primes of *n* that is, *p, q*. These all aim to improve the security of the new RSA system. Essentially, with the new RSA method, as a stronger, hidden/secret key that is a function of the newly derived function, *t* is created, a more expansive and protective system can be obtained, making it more difficult for intruders to guess the private/secret key *d*, as they attempt to guess *n*, which in principle, has been converted into *t*. This is possible because encryption and decryption processes can be carried out in terms of the new transform value, *t* as $C = M^e \bmod(t)$ and $D = \sqrt{C^d} \bmod(t)$ with *t* serving as the new hidden security layer around *n*. Hence, making the new RSA scheme to have a better, formidable security.

References

1. Obaid, T. A. S. (2020). "Study a Public Key in RSA Algorithm". European Journal of Engineering Research and Science. 5(4), 396-397.

2. Jamgekar R. S., Joshi G.S., (2013), "File Encryption and Decryption Using Secure RSA," *International Journal of Emerging Science and Engineering (IJESE)*. 1(4) ISSN: 2319–6378.
3. Khyoon, A. I. (2005) "Modification on the Algorithm of RSA Cryptography System," *Al-Fatih Journal.* 1(24), 80-89. ISSN: 87521996.
4. Obaid T. A. S. Khami M. and Shehab L. G. (2017), "Hiding Secured key in digital media", *Int. Jo. Eng. Res. A.* www.ijera.com 7(9), 58-63.
5. Nisha S., and Farik M., (2017). "RSA Public Key Cryptography Algorithm – A Review", *International Journal of Scientific & Technology Research*. 6(7). ISSN 2277-8616.
6. Al-Lehiebe A., (2015), "Ciphered Text Hiding in an Image using RSA algorithm", *Journal of College of Education for Women.* 26(3).
7. Cid C. (2019), "Cryptanalysis of RSA: A Survey", *SANS Institute. International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, DOI: 10.1109/ICCUBEA .8463720, Publsher:IEEE.
8. Gupta S. M. D and Ritu G. (2017) "Mobile Cloud Computing: A Scientometric Assessment of Global Publications Output during 2007-16". *Journal of Scientometric Res.* 6(3):186-194.
9. Ismail A. and Rashid H. (2017) "Performance Analysis of Multi-Level Algorithm For Data Storage Security In Cloud Computing". *World Journal of Engineering Research and Technology WJERT* 3(5), 480-487. ISSN 2454-695X
10. Zareen (2011) "*Enhancement on Implementation of Multi-prime and Multi-power RSA Algorithm*" An M.Sc Thesis Submitted to the Department of Computer Science and Engineering Department, Thapar University, Patiala.
11. Padmavathama M. and Sreedevi (2017) "New Variant Digital Signature Schemes based on Jk-RSA Cryptosystem" *International Journal of Artificial Intelligence and Computational Research* 2009 1(2) .95- 100 ISSN.0973-6794 0.559
12. Mohsen B., Sharifah M, Ramlan M., Zurina M. (2014) "Comparison of ECC and RSA Algorithm in Resource Constrained Devices" Department of Computer Science Faculty of Computer Science and Information Technology Universiti Putra Malaysia.
13. Ranganathan N. K. (2014). An Implementation of Multi-Prime RSA Algorithm in Data Cloud using Cloud Sql. In NCDMA – 2014, IJERT Conference Processding, Volume 2, Issue 15.
14. Ivy P. and Mandiwa P. & Kumar M. (2012) "A Modified RSA Cryptosystem Based on 'n' Prime Numbers". *IJECT*. 1(2), 63-66.
15. Ayele A. and Sreenivasarao V. (2013) "A Modified RSA Encryption Technique Based on Multiple public keys". *International Journal of Innovative Research in Computer and Communications Engineering* 1(4), 859-900
16. Jahan I, Asif M. and Rozario L. J. (2015). "Improved RSA cryptosystem based on the study of number theory and public key cryptosystems". *American Journal of Engineering Research (AJER)*. 4(1),143-149. e-ISSN: 2320-0847 p-ISSN: 2320-0936.