SECURITY OF COMMUNICATION OF DATA USING THE MODIFIED RSA ALGORITHM

[1]Sweta Ranjan, [2]Dr. Sunil Gupta
[1]M. Tech Scholar, [2]Professor
Department of Computer Science and Engineering
Global Institute of Technology, Rajasthan

Abstract*: This is the time of digital communication. In this era we are sending and receving our data on the internet in secret and unsecret form. When we are talking about the secret data it is not secret for all time but we need a such type of mechnasim by which we can secure that data from the attacker. Cryptography is one of the many techniques to secure data on network. It is one of the techniques that can be used to ensure information security and data privacy. It is used to secure data in rest as well as data in transit. There are two types of algorithm according to the key, one is symmetric key algorithm and the second is asymmetric key algorithm. In this paper we are concentrating on the asymmetric key algorithm RSA algorithm. As we know RSA algorithm is used in many areas as digital signature. There are some limitations of traditional RSA algorithm as it is depend on two prime numbers and in some case we can find out the prime factorization of these. So in this paper we are increasing the prime numbers in the RSA algorithm so that we can improve the RSA algorithm.

Keywords: Cipher Text, Decryption, Decryption Time, Encryption, Encryption Time, Plain Text, RSA Algorithm.

1. INTRODUCTION

Cryptography is a technique to make a readable data into unreadable data. Modern cryptography's part of mathematics and technology of computer science.[1],[2],[3]
Goals of Security (Purpose of Cryptography)
There are some specific security requirements within the context of any application-to-application communication, including these goals. [3], [4], [5]
Confidentiality: It specifies that only sender and intended recipient should able to access the contents of
Message .The attack on the availability is called interception. There are two main threats to confidentiality, snooping and traffic analysis. [3], [4], [5]

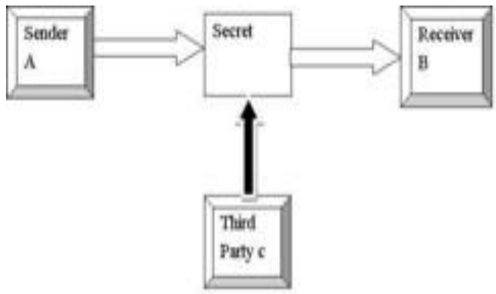

Fig. 1.Loss of Confidentiality [4]

Integrity: When sender sends a message and ensuring that the receiver receives the message as it was, wholly and error free without any changes. Attack on the integrity is called modification. [3], [4], [5]

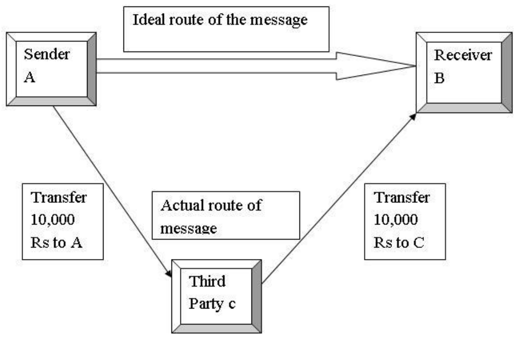

Fig. 2.Loss of Integrity [4]

Availability: Availability is ensuring that those who have the rights to information or material have always got the access to it or resources should be available to authorized parties at all time. The attack on the availability is called interruption [3], [4], [5].

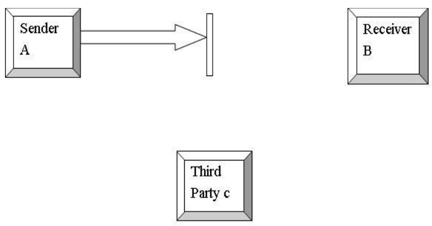

Fig. 3.Attack on Availability [4]

Authentication: It helps establish proof of identities. It ensures that the origin of a document so message is correctly identified. Suppose that third party C sends an electronic message over the internet to receiver B. However, the third-party C had posed as Sender A when C sent this document to user B. How would Receiver B know that the message has come from C.? Who is posing as Sender A.? This type of attack is called as fabrication [3],[4],[5].

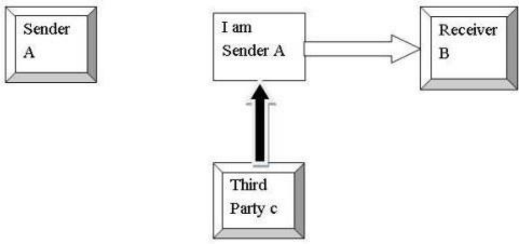

Fig. 4.Absence of Authentication [4]

Non-repudiation: It is a mechanism to prove that sender really sent this message [3], [4], [5].

Types of Cryptosystem

There are two types of cryptosystem:

Symmetric Key Cryptography: If sender and receiver share the same key for encryption and decryption of message than it is called symmetric key cryptography.[7],[9]

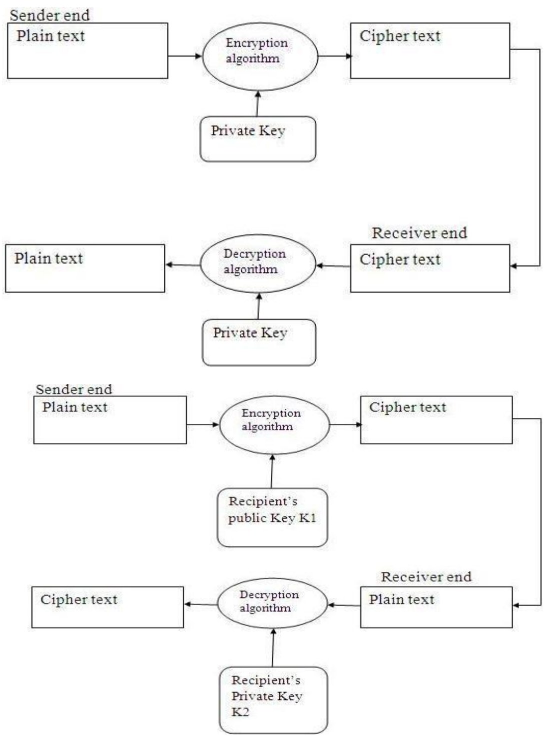

Fig. 5.Private Key Cryptography

Asymmetric Key Cryptography: If sender and receiver share the one key for encryption and another key decryption of message than it is called asymmetric key cryptography. [6], [7], [9]

Fig. 6.Public Key Cryptography RSA Cryptography is the most commonly implemented Asymmetric Key Cryptography.[7],[8],[9],[10]

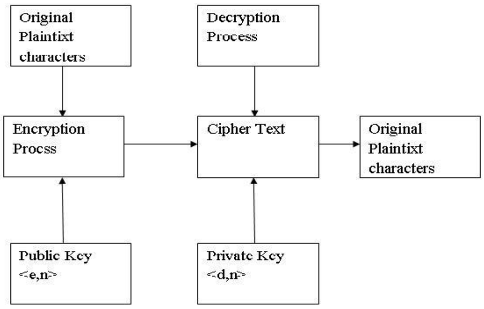

Fig. 7.RSA Model [4]

PROPOSEDALGORITHM

Step1–Take the n prime numbers ($P_1, P_2, P_3, \ldots, P_n$) Instead of two prime numbers that issued in RSA Algorithm.

Step 2 – Calculate the product of these prime Numbers ($N = P_1 x\ P_2 x P_3 x \quad P_n$)

Step3–Now, select the encryption key e, such that it is not a factor of numbers ((P_1-1),(P_2-1),(P_3-1)(P_n-1))

Step 4 – Calculate the decryption key d, such that (d x e) mod ((P_1-1), (P_2-1), (P_3-1) ………. (P_n-1)) = 1

Step 5 – Calculate cipher text (CP) from plain text (PT) as $CT = PT^e \bmod n$

Step 6 – At the receiver's end, calculate plain text (PT) as $PT = CT^d \bmod n$

FLOWCHART

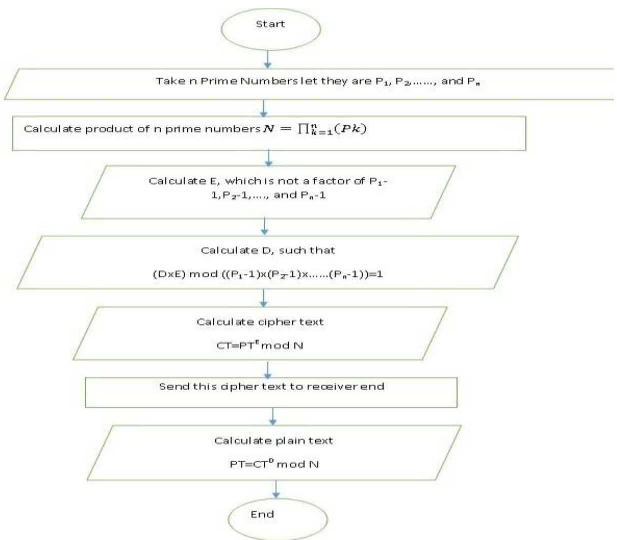

Fig. 8.Flowchart of Proposed Algorithm

PROPOSED ALGORITHM IMPLEMENTATION RESULT

The proposed algorithm is implemented in C and python. We take here 4 types of examples. In these example there is plain text is same for all example that is "India is a Nation." Andthereare2, 3,4 and 5 different prime numbers are used and we calculate the value of N, encryption key value, decryption key value, Encryption time, Decryption time, cipher text and again plain text from cipher text for different combinations. We check variations in encryption and decryption time according to the prime numbers count and check the behavior of time graphs. Here the prime numbers are small for making calculations easy, but we can take large prime numbers in our practical life.

Table- I: List of Prime Numbers Used in this Experiment

	P1	P2	P3	P4	P5
1	23	53	11	37	17
2	29	59	13	41	19
3	31	61	17	43	23
4	37	67	19	47	29
5	41	71	23	53	31
6	43	73	29	59	37
7	47	79	31	61	41
8	53	83	37	67	43
9	59	89	41	71	47
10	61	97	43	73	53

If we are using 2 prime numbers, then P1 and P2 are used.

If we are using 3 prime numbers then P1, P2 and P3areused.

If we are using 4 prime numbers then P1, P2, P3and P4 are used.

If we are using 5 prime numbers then P1, P2, P3, P4 and P5 are used.

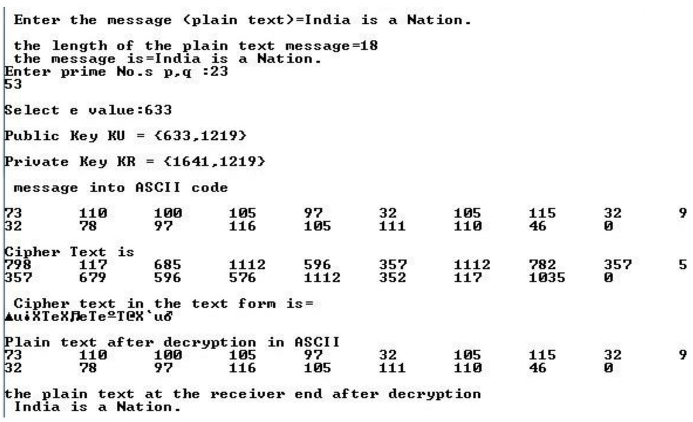

Fig. 9.Example for Two Prime Numbers

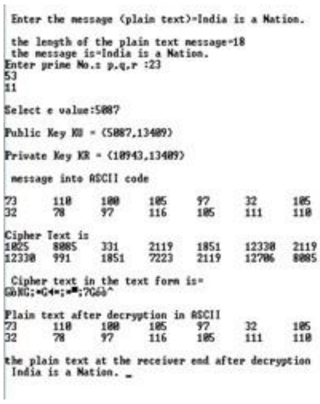

Fig. 10. Example for Three Prime Numbers

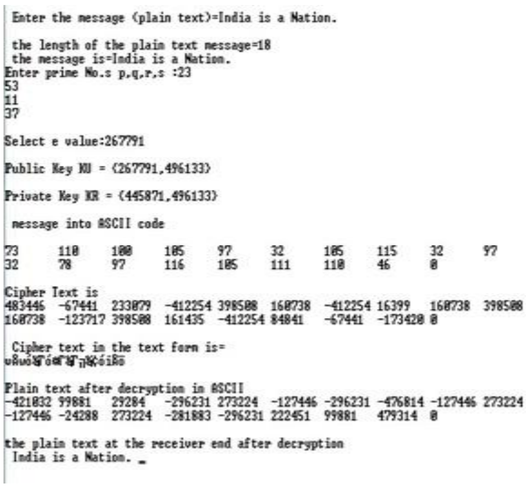

Fig. 11. Example for Four Prime Numbers

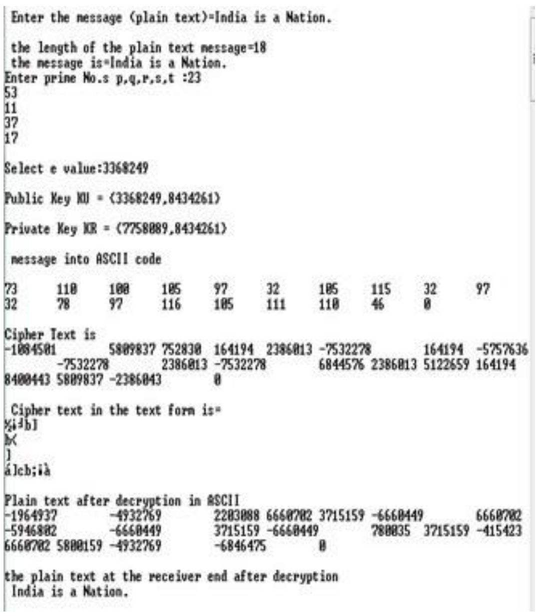

Fig. 12. Example for Five Prime Numbers

PERFORMANCE ANALYSIS OFPROPOSED ALGORITHM

10 sets for 2, 3, 4 and 5 prime numbers have been taken. Tables II, III, IV and V shows the values obtained during the use of two, three, four and five prime numbers.

Table- II: List of Values obtained using Two Prime Numbers

P_1	P_2	n	e	d	encryption time (in sec)	decryption time (in sec)
23	53	1219	633	1641	0.000062900000003197	0.000061999999997844
29	59	1711	429	1677	0.000057400000002872	0.000063700000054400
31	61	1891	799	1399	0.000069099999997491	0.000073200000027710
37	67	2479	779	2315	0.000058899999999085	0.000065299999957160
41	71	2911	277	4013	0.000055599999996048	0.000074499999966467
43	73	3139	319	2095	0.000058299999999178	0.000066600000038025
47	79	3713	511	2935	0.000060699999998803	0.000119300000014880
53	83	4399	1263	2711	0.000069000000003427	0.000068200000011840
59	89	5251	1095	3687	0.000074800000000153	0.000078700000030957
61	97	5917	5563	3187	0.000091199999999958	0.000078500000007585

Table- III: List of Values obtained using Three Prime Numbers

P_1	P_2	P_3	N	e	d	encryption time (in sec)	decryption time (in sec)
23	53	11	13409	5087	10943	0.0000921000000033700	0.0000945000000029950
29	59	13	22243	11957	13469	0.0000849999999985585	0.0000775999999973465
31	61	17	32147	27403	21667	0.0000900999999942087	0.0000864000000007081
37	67	19	47101	8689	25585	0.0000847000000021580	0.0000895000000014079
41	71	23	66953	45811	72091	0.0001067999999975200	0.0001084000000020070
43	73	29	91031	18749	123989	0.0000974000000013575	0.0001036000000027570
47	79	31	115103	52093	61237	0.0001096999999958820	0.0001018999999899960
53	83	37	162763	104861	126005	0.0001141999999987320	0.0001058000000000450
59	89	41	215291	133999	205839	0.0001196999999990570	0.0001091999999971450
61	97	43	254431	4283	186227	0.0000848999999902844	0.0001457999999985300

Table- IV: List of Values obtained using Four Prime Numbers

P_1	P_2	P_3	P_4	N	e	d	encryption time (in sec)	decryption time (in sec)
23	53	11	37	496133	257791	432511	0.0001244000000042430	0.0001199999999954570
29	59	13	41	911963	617993	1126457	0.0001297000000022310	0.0001265999999873200
31	61	17	43	1382321	675587	1271723	0.0001284000000083550	0.0001371999999975060
37	67	19	47	2213747	1403035	1429843	0.0001374999999939060	0.0001302000000009680
41	71	23	53	3548509	1670597	3166733	0.0001431000000025050	0.0001338000000004060
43	73	29	59	5370829	4226941	5490901	0.0002096000000051390	0.0001463999999913310
47	79	31	61	7021283	2868137	7946873	0.0001446999999927810	0.0001470999999924060
53	83	37	67	10905121	1542943	11135071	0.0001385000000198030	0.0001543000000197030
59	89	41	71	15285661	12370703	9366767	0.0001847000000054780	0.0001547999999900190
61	97	43	73	18573463	6919681	23585281	0.0001405000000431760	0.0001477999999792700

Table- V: List of Values obtained using Five Prime Numbers

P_1	P_2	P_3	P_4	P_5	N	e	d	encryption time (in sec)	decryption time (in sec)
23	53	11	37	17	8434261	3368249	7758089	0.0001458000000056360	0.0001405000000005430
29	59	13	41	19	17327297	5298563	12062507	0.0001500000000049800	0.0001534000000020800
31	61	17	43	23	31793383	21087041	18400961	0.0001553999999828190	0.0001479999999958180
37	67	19	47	29	64198663	36667549	28792117	0.0001725999999848680	0.0001637999999957170
41	71	23	53	31	1.1E+08	51873697	87112033	0.0001759999998967030	0.0001730000000179640
43	73	29	59	37	1.99E+08	1.49E+08	227267713	0.0001886000000013150	0.0001746000000366620
47	79	31	61	41	2.88E+08	64729411	184227691	0.0001738000000841570	0.0001877999998214360
53	83	37	67	43	4.69E+08	3.05E+08	394023173	0.0001965999999811170	0.0001861999999164250
59	89	41	71	47	7.18E+08	2.64E+08	513683237	0.0002696999999898250	0.0002264999993712990
61	97	43	73	53	9.84E+08	1.03E+08	465483839	0.0003010999989783160	0.0001972999998542950

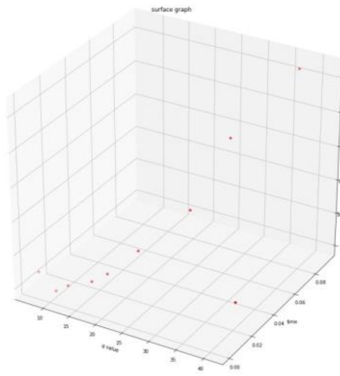

Fig13. Surface graph for 3 prime numbers

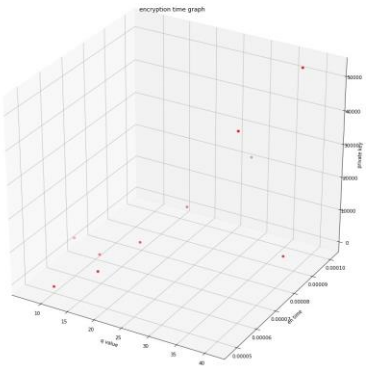

Fig 14. Encryption time for 3 prime numbers

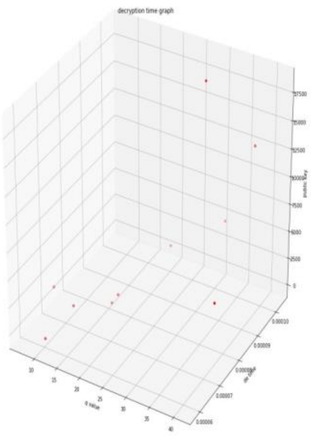

Fig 15. Decryption time for 3 prime numbers

4 prime

Enter the Message (Plain Text): India is a nation.

The Length of Plain Text Message: 18

The Message is: India is a nation.

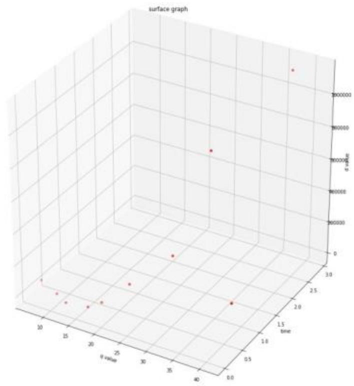

Fig 16. Surface graph for 4 prime numbers

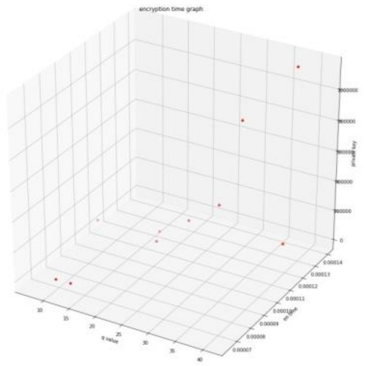

Fig 17. Encryption time for 4 prime numbers

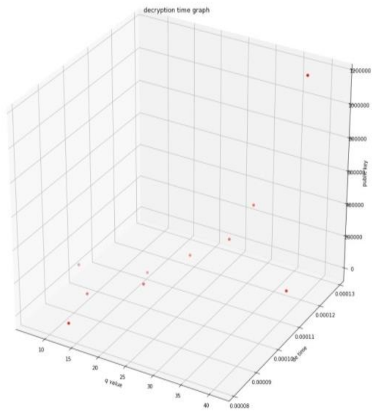

Fig 18. Decryption time for 4 prime numbers

5 prime

Enter the Message (Plain Text): India is a nation.

The Length of Plain Text Message: 18

The Message is: India is a nation.

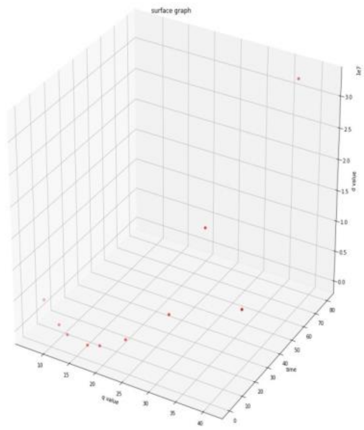

Fig 19. Surface graph for 5 prime numbers

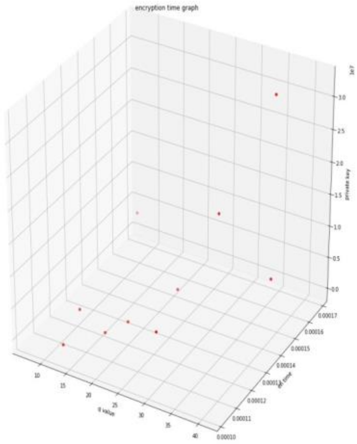

Fig 20. Encryption time for 5 prime numbers

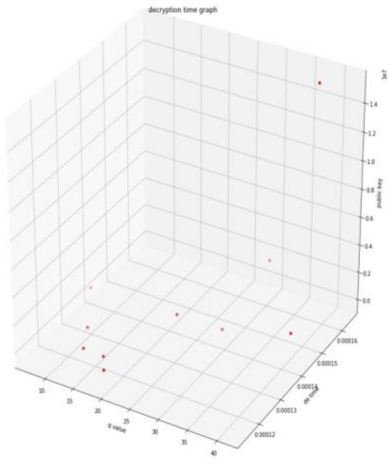

Fig 21. Decryption time for 5 prime numbers

By analysis of these graphs we can say that if we increase the prime number then encryption and decryption time will be increased in terms of e^x.

ADVANTAGES OF PROPOSEDALGORITHM

It is very hard to find out the factors of N. In this case $((P_1-1), (P_2-1), (P_3-1) \ldots\ldots\ldots (P_n-1))$ because when we increase number of prime numbers then its product is also a big number.

The security aspects are not compromised here like confidentiality, availability, integrity, Authentication.

CONCLUSION

At the end by comparing and checking all the parameters of proposed algorithm with existing algorithm, we can say that when we increase the number of prime numbers in RSA algorithm then its security also improves because it's hard to find the factor of N, while there are more than two prime numbers.

Encryption and Decryption time is depends on the value of e(encryption key) and d(decryption key) and here value of e is smaller because we are using more than 2 prime numbers so due to this the value of d is also not so big and by this process the encryption and decryption time is less.

REFERENCES

[1] RSA algorithm using modified sub setsum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011

[2] The large prime numbers based on genetic algorithm, hang Qing, (ICISIE) pp-434-437, IEEE 2011..

[3] An advanced secure (t, n) threshold proxy signature scheme based on RSA crypto system for known signers, Kumar, R, Dept. of Computer Sci. and Eng, pp 293-298, IEEE2010.

[4] An efficient decryption method for RSA cryptosystem, Ren-Junn Hwang, Dept. of Compute. Sci. and Inf. Eng, pp-585-590, IEEE2005.

[5] A new RSA cryptosystem hardware design based on Montgomery's algorithm, Ching Chao Yang, Dept. of Electron. Eng, pp- 908-913, IEEE 1998.

[6] A systolic RSA public key cryptosystem, Po – Song Chen, Dept. of Electron. Eng, pp 408-411, IEEE1996.

[7] "Secure Key Exchange using RSA in Extended Playfair Cipher Technique" Surendra Singh Chauhan, International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014.

[8] Blocking method for RSA cryptosystem without expanding cipher length, NEC Corp, Kanagawa, Japan, pp 773-774, IEEE1989.

[9] A method or obtaining digital signatures and public key cryptosystems, R.Rivest, A.Shamir and L.Adleman "communication of the association for computing machinery " 1978, pp120-126.

[10] "A modified RSA cryptosystem based on 'n' prime numbers", B.Persis UrbanaIvy, Purshotam Mandiwa. Mukesh Kumar, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No.63-66

