MODIFIED RSA ALGORITHM BASED ON KEY GENERATION

[1]CARLO A. INTILA, [2]BOBBY GERARDO, [3]RUJI P. MEDINA

Technological Institute of the Philippines Quezon City

Abstract- Asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric ones but lack in time efficiency. RSA Algorithm is a public-key cryptography and is considered as one of the great advances in the field of public key cryptography. Furthermore, in the study of Aggarwal, D. and Maurer U. they show that that e -th roots modulo n with non-negligible probability can be used to factor n. In this regard, factorization attack is the main weakness of the RSA Algorithm based on the 'e' and 'n' which are the public keys used for encryption. With this, the study aims to modify an RSA Algorithm based on key generation of new value of public key e and modulus n to utilized or increased the security against factorization attack and increased the security of encryption and decryption process of the message.

Keywords- RSA Algorithm, Key generation, modulus, public key, private key

I. INTRODUCTION

rotecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. There are asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric ones but lack in time efficiency. It is also difficult to manage such a huge base of key-pairs efficiently and safely. [1]

RSA (Rivest Shamir Adleman) Algorithm is a public-key cryptography [2] and is considered as one of the great advances in the field of public key cryptography. It is suitable for both signing and encryption. Sufficiently long keys and up-to-date implementation of RSA is considered more secure to use. The RSA is more secure from multiple attacks, but the demerits of the RSA are low speed, demand for key deposit, and inappropriate for global system. [3]

In addition to this, the development of internet application needs secured cryptosystem for data communication. Public key cryptosystem is suitable for secured communication. To obtain the user's satisfaction, high speed algorithms with enhanced security has to be developed. The speed and security issues are discussed in study of Amalarethinam G. & Geetha S., to encourage the researchers to propose new algorithms with multiple parameters towards better performance of secured network communication[4].

At present, RSA is the most widely used public key technology today but the use of more simpler connected devices and demand for higher level of security will make continued reliance on RSA more challenging over time. These trends highlight a clear need for an efficient public key cryptosystem that can lower the capacity threshold for small devices to perform strong cryptography and increase a server's capacity to handle the secure communication. [5] In the study of Boneh D. and Venkatesan R. [6] breaking the RSA is equal to factoring. The RSA Algorithm is prone to factorization attacks based on the value 'n' which displayed as a public key. [7] [8] [9] [10]

Furthermore, in the study of Aggarwal, D. and Maurer U.[11], they show that that e -th roots modulo n with non-negligible probability can be used to factor n. In this regard, factorization attack is the main weakness of the RSA Algorithm based on the 'e' and 'n' which are the public keys used for encryption. With this, the study aims to modify an RSA Algorithm based on key generation of new value of public key to utilized or increased the security against factorization attack.

II. REVIEW

In the paper presented by Sahu J. et al. [12], a better version of RSA algorithm with enhanced security. The security feature here is the elimination of n from the original RSA algorithm and addition of a new number f in place of n. The replacement of n i.e. f is used in both private and public keys. The RSA algorithm is prone to mathematical factorization attacks. Since they have eliminated n with f, it is very hard to factorize it and get the original numbers i.e. p and q. This makes the algorithm more secure with a slight increase of time complexity.

Anchored to the paper of Mansour A. et al.[13] proposed a one-to-many asymmetric cryptographic system that uses RSA as a base. This is useful when the sender wants to multicast different encrypted messages to multiple receivers. Existing solutions for multi-asymmetric RSA schemes have limitations. They either require trusting all receivers or need to make some sort of agreements beforehand. The proposed approach leverages Chinese Remainder Theorem (CRT) to address these limitations. They presented their method, it showed that their algorithm is provable mathematically, and explained that the assumptions they make can be considered as safe assumptions. They presented their calculated time complexity and the results of tests they ran compared to that of text book RSA.

Further supported by the paper of Jaju S. &Chowhan S. [14]presented a fair comparison between RSA and Modified RSA algorithm along with time and security by running several encryption and decryption setting to process data of different sizes. The efficiency of these algorithms was considered based on key generation speed and security level. The texts of different sizes were encrypted and decrypted using RSA and modified RSA algorithms. The simulation result proves that in Modified RSA algorithm key generation is faster and it enhances security by two levels. RSA algorithm is faster than Modified RSA in terms of encryption and decryption speed.

Likewise, in the paper of Ivy P., Mandiwa P. and Kunar M [15], they used 'n' prime numbers which is provided the security over the networks. In which they endeavoured to get the quality that make easier the cryptography to have a good use of 'n' prime numbers. The 'n' prime numbers acts (plays)a very necessary role in RSA cryptosystem. To develop the RSA algorithm for 'n' prime numbers and also used four prime numbers. In this paper no qualitative measurement were done and only shows its process involved.

Based on the study of Ayele A. and Sreenivasarao, an algorithm is proposed for RSA as a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation. These two public keys are sent separately, that makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security but with less speed.[16]

In the research conducted by Jahan I.,Asif M. and Rozario L.J. is a study of number theory and public key cryptosystems and based on this improving the RSA cryptosystem that is more reliable to brute force attack.RSA cryptosystem produces one public key to encrypt the message. Though it is hard to find out the factors of n and get p and q, two large prime numbers, therefore brute force attack is more difficult in the proposed algorithm as the encryption keys are sent separately, not at once. The proposed RSA is used for system that needs high security but with less speed.[17]

Dhakar, R.S. and Gupta A.K. developed a modified RSA Encryption Algorithm (MREA). The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So MREA improve the security. MREA is secure as compared to RSA as it is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. [18]

To further improve the security of data, the paper of Raj A. et al proposed a new modification to RSA algorithm called Binary RSA Encryption Algorithm. In this approach, encoded message generated using modified RSA algorithm is converted to binary code .So the transmitting code contains only zeroes and ones. Thus decryption is difficult for the intruder .So the BREA provide more security towards the data. The paper is an improved implementation of RSA cryptographic solution providing better security and moderate time and space complexities. [19]

Methods

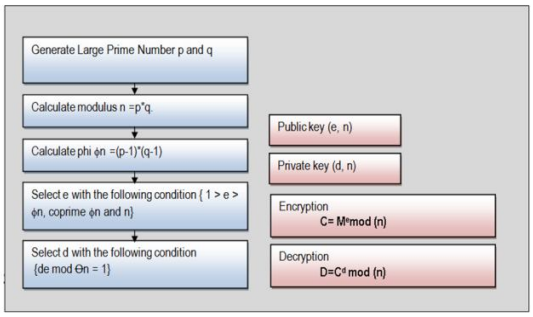


Figure 1.The Original RSA Flow of Encryption

Key Generation

In this step, the both (private and public) keys are generated to be used in Encryption and decryption process.

Generating both keys private and public as shown in below steps:

1. Choose two large prime numbers p and q.
2. Compute modulus number n = p x q.
3. Calculate the Euler function ϕ(n) = (p-1) x (q-1).
4. Select an integer number e randomly as a public key. It should satisfy Greater Common Divisor GCD where (e,ϕ(n)) = 1, 1< e <ϕ(n) and coprime with n, ϕn.
5. Compute the private key d such that de(mod(phi n))=1

Encryption

It is the transformation of data into a form that becomes as difficult as possible to read without the appropriate knowledge (a key). In the RSA algorithm the ciphertext is generated by below equation. The fig. 4 shows the Conceptual Framework of Modified RSA Algorithm based on key generation.

C=Me mod n (1)

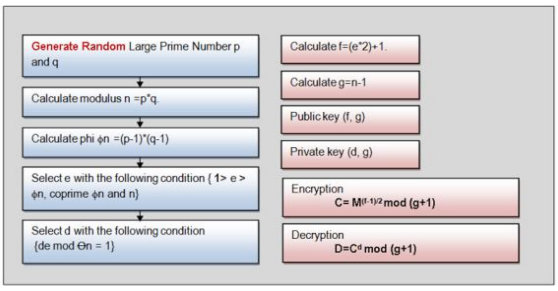


Figure 2. The Modified RSA Algorithm

Figure 2 shows the Modified RSA Algorithm of the study. Initial modification starts with the private key

and followed by decryption formula. The steps below will show the modification process.

Modified RSA Algorithm Based on Key Generation

In the study of Aggarwal, D. and Maurer U. (2016), they show that that e -th roots modulo n with non-negligible probability can be used to factor n. With this, the proposed study was to modify the e and n value for more secure RSA Algorithm.

1. Generate Random Large Prime Number p and q.
2. Calculate modulus n =p*q.
3. Calculate phi ϕn =(p-1)*(q-1)
4. Select e with the following condition { p > e >ϕn, coprimeϕn and n}
5. Calculate f=(e*2)+1.
6. Select d with the following condition {de mod n = 1}
7. Calculate g=n-1
8. Send Public key (f, g)
   The f and g will serve as a new public key which will hide the original e and n value.
9. Send Private key (d, g)
   The public key that was send will be fixed using the modified equation for encryption.
10. Encryption
    C = $M^{(f-1)/2}$ mod (g+1)
11. Decrytion
    D =C^d mod (g+1)

SAMPLE

1. Generate Random Large Prime Number p and q. p=5 q=11
2. Calculate modulus n =p*q. n=5*11=55
3. Calculate phi ϕn =(p-1)*(q-1) ϕn=(5-1)*(11-1)=4*10=40
4. Select e with the following condition { p > e >ϕn, coprimeϕn and n} e=13
5. Calculate f=(e*2)+1. f = (13*2)-1 = 26+1=27
6. Select d with the following condition {de mod n = 1} d=37
7. Calculate g=n-1 =55-1 = 54
8. Send Public key (f, g) Public Key = (25,54)
9. Send Private key (d, g) Private Key = (37,54)
10. Encryption
    M=4
    C = $M^{(f-1)/2}$ mod (g+1)
    =$4^{(27-1)/2}$ mod 54+1
    =4^{13} mod 55
    =67,108,864 mod 55
    =9
11. Decryption
    D =C^d mod (g+1)
    =9^{37} mod (54+1)
    = 9^{37} mod 55
    = 2.028e+35 mod 55
    =4

The Original RSA Algorithm and Modified RSA Algorithm will be developed in Java Programming Language. A modified key generation of RSA Algorithm will be implemented to improve its security. The method to modify the equation of private key will be utilized which must also concern with the process of encryption and decryption process will be involved. The method to test the two algorithms is to differ the result of RSA factorization calculator. Also, the two algorithms will be tested in the same hardware and software specifications. Figure 5.0 shows the method of the study.

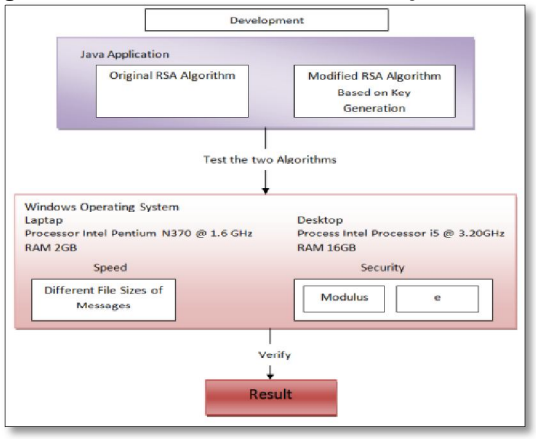


Figure 5.0 The Method of the Study

RESULT

RSA and Modified RSA Algorithm are implemented in java. These algorithms are tested by different file size and calculate the encryption and decryption times. With the design of both algorithms, the test was conducted using RSA Factorization by ECM Enterprise Content Management and result of the private key generation was based on formula of different related studies conducted.

Result for factorization of n and e.
Factorization

Factorizatio(n)						
p	q	n	n-1	Factorization (n-1)	phi (n-1)	Actual phin n
11	307	3377	3376	2^4 x 211	6572	3060
47	79	3713	3712	2^7 x 29	760	3588
167	907	151469	151468	2^2 x 19 x 1993	71712	150396
257	853	219221	219220	2^2 x 5 x 97 x 113	869224	218112
269	617	165973	165972	2^2 x 3 x 13831	55320	165088
337	719	242303	242302	2 x 121151	121150	241248
349	487	169963	169962	2 x 3 x 13 x 2179	2179	169128
367	947	347549	347548	2^2 x 17 x 19 x 269	154369	346236
463	997	461611	461610	2 x 3^2 x 5 x 23 x 223	117216	460152
659	397	261623	261622	2 x 130811	130810	260568
709	181	128329	128328	2^3 x 3 x 5347	42768	127440
2089	2731	5705059	5705058	2 x 3 x 23 x 41341	1818960	5700240
3221	3877	12487817	12487816	2 x 11 x 141907	5676240	12480720
3217	4363	14035771	14035770	2 x 3^2 x 5 x 7 x 22279	3208032	14028192
3221	3077	9911017	9911016	2^3 x 3^2 x 137653	3303648	9904720

Table 1.0 Result of the Original RSA and Modified RSA Based on n or modulus using RSA Factorization Calculator

The table above was the result in using the RSA factorization calculator by (ECM) Enterprise Content Management to shows the difference between Original RSA and Modified RSA. ECM is the

technology used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. [20]

The RSA Factorization Calculator by ECM was presented by Kostopoulos G. as one of the factorization algorithms in the computer theory[21].

The table shows actual p and q values, n, n-1, factorization of (n-1), phi (n-1) and the actual phi n. The n is the modulus of the original RSA while n-1 is the modulus of modified RSA. Also, the table shows the result of the factorization result between n and n-1 and the result between the actual phi n and phi (n-1).

Test Result of Public Key 'e'

Prime Number		e(Original RSA)	d(Original RSA)	e(Modified RSA)	d(Modified RSA)
p	q				
11	307	1493	2357	2987	503
17	181	1429	2749	2859	-1
47	79	1789	3229	3579	-1
167	907	75193	105277	150387	-1
257	853	108877	111493	217755	-1
269	617	82493	85781	164987	94803
337	719	120557	145829	241115	-1
349	487	84551	162623	169103	115007
367	947	173087	284807	346175	-1
463	997	230059	338347	460119	-1
659	397	130279	234511	260559	-1
709	181	63527	112583	127055	-1
2089	2731	2849933	3764597	5699867	1161443
3221	3877	6240257	9390833	12480515	-1
3217	4363	7013899	12924451	14027799	-1
3221	3077	4952231	8023591	9904463	8748527

Table 2.0 Test Result of the Original RSA and Modified RSA Based on e or Public Key.

The table above shows the result of the Original RSA and Modified RSA Algorithm based on e or public key. The formula 'de mod ϕn' was based on the study of Sharma S. et al.[22] Dhakar R.S. & Gupta A.K. [23] Ivy P. &Mandiwa P. [15] & Kumar M. [24], and Nagar S. &Alshamma S. [25].

RESULT FOR PERFORMANCE

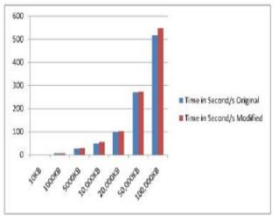
The following tables and graphs show the result of performance of the original and the modified RSA Algorithm. The two algorithms are developed using Java Programming Language.

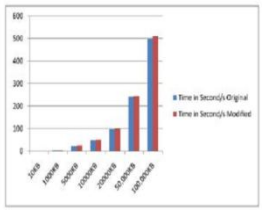
Table 4.0, Table 5.0, Graph 1.0, and Graph 2.0 show the encryption and decryption time using a Laptop with specification of Intel Pentium CPUN370 1.6GHz , 2GB RAM, and 64 bit Windows 10 Operating System.

Encryption		
	Time in Second/s	
Size(KB)	Original	Modified
10KB	2	2
1000KB	7	7
5000KB	28	30
10,000KB	52	56
20,000KB	102	105
50,000KB	271	273
100,000KB	518	549

Decryption		
	Time in Second/s	
Size(KB)	Original	Modified
10KB	1	1
1000KB	5	5
5000KB	25	26
10000KB	50	51
20000KB	97	101
50,000KB	243	245
100,000KB	501	513

Table 4.0 Encryption Time for Device1
Table 5.0 Decryption Time for Device1





Graph 1.0 Encryption Time for Device1
Graph 2.0 Decryption Time for Device1

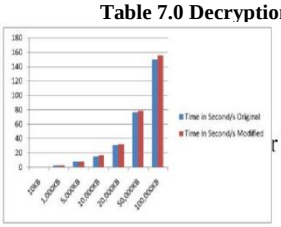
The table 4.0 and 5.0 show the execution time of different file sizes of messages of Original RSA Algorithm and Modified RSA Algorithm for device 1. The Graph 1.0 and Graph 2.0 show the comparison of execution time between Original RSA Algorithm and Modified Algorithm for device 1.

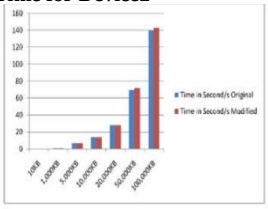
Table 6.0, Table 7.0, Graph 3.0, and Graph 4.0 show the encryption and decryption time with a Desktop with specification of Intel Pentium i5-4570 3.20GHz, 16GB RAM, and64 bit Windows 10 Operating System.

Decryption		
	Time in Second/s	
Size(KB)	Original	Modified
10KB	0	0
1,000KB	1	1
5,000KB	7	7
10,000KB	14	14
20,000KB	28	28
50,000KB	70	72
100,000KB	140	143

Encryption		
	Time in Second/s	
Size(KB)	Original	Modified
10KB	0	0
1,000KB	2	2
5,000KB	8	8
10,000KB	15	16
20,000KB	30	32
50,000KB	76	79
100,000KB	150	156

Table 6.0 Encryption Time for Device2
Table 7.0 Decryption Time for Device2





Graph 3.0 Encryption Time for Device2
Graph 4.0 Decryption Time for Device2

The table 5.0 and 6.0 show the execution time of different file sizes of messages of Original RSA Algorithm and Modified RSA Algorithm for device 2. The Graph 3.0 and Graph 4.0 show the comparison of execution time between Original RSA Algorithm and Modified Algorithm for device 2.

Findings

The following are the results and findings of this study:

1. In the result of table 1.0, the result shows based on RSA Factorization Calculator that the Modified RSA was more complex than the Original RSA Algorithm.

2. In the result of table 2.0, the result shows that the Modified RSA Algorithm produce different value of private key 'd' which was used for decryption process.

3. In the result of performance, the Modified RSA Algorithm slightly increased in

encryption and decryption process than the Original RSA Algorithm.

4. The modification of RSA Algorithm based on the public key ‘e’ and modulus ‘n’ produced complex result for decryption and factorization than the original RSA Algorithm.

CONCLUSIONS

Comparison of algorithms requires substantial criteria to show the result in more transparent way to effectively display result and analysis.

In the study of Aggarwal, D. and Maurer U.[11], they show that the e -th roots modulo ‘n’ with non-negligible probability can be used to factor n. Thus, this study presented the modification of RSA Algorithm based on key generation of ‘e’ and ‘n’.

This study presented a more secure RSA Algorithm based on key generated ‘e’ and ‘n’. Different value was generated and used for ‘e’ and ‘n’ which is visible to public and in result, different value or information will be generated using the original RSA equations. Based on the findings, the Modified RSA Algorithm has slightly increased in terms of speed but offers better security which is more important in information transfer.

Finally, this study shows that the modification of both ‘e’ and ‘n’ will increase the complexity of the security of RSA Algorithm.

RECOMMENDATIONS

Cryptographic technique is widely used for information security. RSA is such a technique for data confidentiality. To further improve the security of data, this paper proposes a further modification to RSA algorithm.

The implementation of this study Modified RSA based on key generation was implemented using small prime numbers. The next step of this work is to adopt this approach to large prime numbers. Also, the application of this modification will be implemented in an online messaging and will be tested its security with different online sniffing tools.

Another recommendation in modifying public key ‘e’ and modulo ‘n’ is to provide better equations in transformation for better security.

REFERENCES

[1] Meghana V., Aishwarya B. &, Shobha M.S. “Amalgamation of Cryptographic Techniques for Secured Data Transmission”. IJRCCE Vol. 5. 2007

[2]Rivest R. L. & Shamir A. &Adleman L. “A method for obtaining digital signatures and public-key cryptosystems”. Communications of the ACM, 21(2):120{126. 1978

[3] Sankara Narayanan, C. & Anna Durai, S. “A Critical Study on Encryption Based Compression Technique”. Journal of Computers Volume 11, Number 5. 2016

[4] Amalarethinam G. &Geetha S. “A Survey on Secured Communication with High Speed using Public Key Cryptography”. International Journal of Scientific & Engineering Research, Volume 7, Issue 4. 2016

[5] Arya P. K. et al. “Comparative Study of Asymmetric Key Cryptographic Algorithms”. International Journal of Computer Science & Communication Networks,Vol 5(1),17-21, ISSN:2249-5789. 2015

[6] Boneh D. and Venkatesan R.. “Breaking RSA May Be Easier Than Factoring”. ResearchGate GmbH. 1999

[7] Sahu J. Et al. “An Enhanced Version of RSA to Increase the Security”. Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Volume 7, Issue 4. 2017

[8] Ivy P. &Mandiwa P. & Kumar M. “A Modified RSA Cryptosystem Based on ‘n’ Prime Numbers”. IJECTVolume1 Issue 2 Nov 2012 Page No. 63-66. 2012

[9] Jaju S. &Chowhan S. “A Modified RSA algorithm to enhance security for digital signature”. 2015 International Conference and Workshop on Computing and Communication (IEMCON). 2015

[10] Ayele A. &Sreenivasarao V. “A Modified RSA Encryption Technique Based on Multiple public keys”. 2013

[11] Aggarwal, D. and Maurer U. “Breaking RSA Generically Is Equivalent to Factoring”. IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 62, NO. 11, NOVEMBER 2016

[12] Sahu J. Et al. “An Enhanced Version of RSA to Increase the Security”. Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Volume 7, Issue 4. 2013

[13] Mansour A. et al. “Multi-Asymmetric Cryptographic RSA Scheme”. CISRC '17. 2017

[14] Jaju S. &Chowhan S. “A Modified RSA algorithm to enhance security for digital signature”. 2015 International Conference and Workshop on Computing and Communication (IEMCON). 2015

[15] Ivy P. &Mandiwa P. & Kumar M. “A Modified RSA Cryptosystem Based on ‘n’ Prime Numbers”. IJECTVolume1 Issue 2 Nov 2012 Page No. 63-66. 2012

[16] Ayele A. &Sreenivasarao V. “A Modified RSA Encryption Technique Based on Multiple public keys”. 2013

[17] Jahan I. &Asif M. &Rozario L.J. “Improved RSA cryptosystem based on the study of number theory and public key cryptosystems”. American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-4, Issue-1, pp-143-149. 2015

[18] Dhakar R.S. & Gupta A.K. “Modified RSA Encryption Algorithm (MREA)”. Advanced Computing & Communication Technologies 978-0-7695-4640-7/12 $26.00 © 2012 IEEE

[19] Nagar S. &Alshamma S. “High Speed Implementation of RSA Algorithm with Modified Keys Exchange”. IEEE 6th

International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) 2012

[20] Tyrvainen P. et al. "Characterizing the Evolving Research on Enterprise Content Management". European Journal of Information Systems 15(6), 627-634. 2006

[21] Kostopoulos G. "An Original Numerical Factorization Algorithm". IBIMA Publishing.Journal of Information Assurance & Cyber security. Vol. 2016 (2016), Article ID 775081, 8 pages DOI: 0.5171/2016.775081. 2016

[22] Sharma S.Sharma P. &Dhakar R. S. "RSA Algorithm Using Modified Subset Sum Cryptosystem". ICCCT, IEEE, 457-461. 2011

[23] Dhakar R. & Gupta A. & Sharma P. "Modified RSA Encryption Algorithm". Advanced Computing Communication Technologies (ACCT), 2012, 426-429. 2012

[24] Kumar N. and Chaudhary P. "Implementation of Modified RSA Cryptosystem for Data Encryption and Decryption based on n Prime number and Bit Stuffing". ICTCS © 2016 ACM. ISBN 978-1-4503-3962-9/16/03. 2016

★★★