TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

Performance Enhancement of RSA Using Runge-Kutta Technique

V. Joseph Raj[1], R. Felista Sugirtha Lizy [2]

[1]Associate Professor and Head, Department of Computer Science Kamaraj College, Thoothukudi – 628 003, TamilNadu, India

[2]Assistant Professor, Department of Information Technology Pope's College, Sawyerpuram – 628 251, TamilNadu, India

[1]v.jose08@gmail.com, [2]21felistaa@gmail.com

Article Info
Volume 83
Page Number: 11850 - 11857
Publication Issue:
May-June 2020

Article History
Article Received: *19 November 2019*
Revised: *27January 2020*
Accepted: *24 February 2020*
Publication: *19 May 2020*

Abstract

Security is one of the major problem in Aadhaar card. This work would be valuable to Aadhaar card elaborately in data storage, transmission, communication and safeguarding data security. Cryptography techniques are used to prescribe secrecy. Cryptography is the most remarkable issue in network security. The benefit of this algorithm for security decreases time for process of text encryption and decryption. RSA is an asymmetric system, where a key pair to be created, a public key and a private key. RSA algorithm is the best algorithm for data security in Smart card, Aadhaar card throughout the world. In this research paper, the performance of RSA Cryptography algorithm is improved in terms of speed and security by combining RSA and Runge-Kutta (RK) Method. The main benefits of RK methods are that they are easy to apply and the error value is low. The RK-RSA algorithm is proposed by improving its performance in terms of Avalanche Effect, Speed, Throughput and Power Consumption. The improved performance of RK-RSA algorithm and experimental results are reported. The mathematical justification supporting the RK-RSA algorithm is also detailed.

Keywords; *Avalanche Effect, Cryptography, RSA, Runge-Kutta, Throughput.*

I. INTRODUCTION

An Aadhaar card is a unique identification number (UID) which has been issued by a central government agency operating in India called the Unique Identification Authority of India (UIDAI). The government intends on keeping a database containing information about every registered citizen of India. These details can be generated by the Aadhaar card holders which contain various personal details like name, address, date of birth, registered mobile number, registered email address and others. In addition to a person's personal information, it also stores their photograph, fingerprints and iris scans. With this system of information, it becomes very easy to identify an individual by simply cross-referencing their data with the data in the system.

The RSA algorithm is the base of a cryptosystem a suite of cryptographic algorithms [1] that are used for definite security facilities or resolves which empowers public key encryption and is widely used to secure penetrating data, mainly when it is being sent over an insecure network such as the internet.

RSA [2,3] was first publicly described in 1977 by Ron Riverst, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, through the 1973 creation of a public key algorithm by British mathematician Clifford locks was kept classified by the UK's GCHQ until 1997.

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

The Avalanche effect [4] has been used to illustrate that the proposed of RK-RSA algorithm possesses latent circulation characteristics such as security as that of the original RSA [5] algorithm. Thus the proposed RK-RSA algorithm improve the performance over RSA.

II. LITERATURE SURVEY

The source of the encryption knowledge which is used, is proposed by Diffie and Hellman in the paper of "New Direction in Cryptography" in 1976 [6]. R. Rivest, A. Shamir and L. Adleman understand a public key cryptosystem that now called RSA public cryptosystem [7]. The algorithm is considered to be the most perfect and the most mature public-key cryptosystem that is widely used in various fields.

Cryptography has a long history, but in general it is still very strange, because it is only in a small area, such as the military, intelligence, diplomatic and other sensitive sectors [8]. Computer cryptography is the study of computer information encryption, decryption and transform scientific, interdisciplinary mathematics and computer, is an emerging discipline [9].

Cryptographic techniques are used to ensure the confidentiality, integrity and authenticity of electronic data. Confidentiality is to encrypt the data, so that the illegal user cannot read data information. The legitimate user can use the key to read out information. The integrity of data is determining whether the data is illegal tampered, correct and complete information to ensure the legitimate users. Authenticity is the authenticity of the data sources, the authenticity of the identification of the data itself, can ensure that legitimate users are not deceived [9].

Asymmetric encryption algorithm of RSA is different from symmetric encryption algorithm that it needs two keys, a public key, a secret key. The two of them appear in pairs, if the public key is to encrypt data, only the corresponding private key can decrypt and vice versa. Because the encryption and decryption is done using two different keys, this algorithm is called asymmetric encryption algorithm [10].

Exchange the key of the symmetric encryption algorithm [11]: Asymmetric encryption algorithm is slower than symmetric encryption algorithm with t = (p-1)*(q-1). Hence asymmetric encryption algorithm is used mainly for the encryption key of the symmetric encryption algorithm.

III. RSA ALGORITHM

RSA is used by contemporary computers to encrypt and decrypt the messages. It is asymmetric key cryptographic algorithm which is intended for digital signature. The attitude of RSA algorithm is "it is easy to multiply prime numbers but tough to factor them". Hence it takes more time for calculation with huge prime numbers. It is advisable to construct a firm implementation of RSA for Aadhaar cards with crypto coprocessor [12].

The steps of RSA algorithm are as follows:

a) Two prime numbers p and q.
b) $n=p*q$ and $\Phi(n) = (p-1)(q-1)$.
c) Encryption key e, with the goal of gcd(e, $\Phi(n)$)=1. Where $1<e<\Phi(n)$.
d) Find the decryption key d: $d= 1 \bmod \Phi(n)$, where $0 \leq d \leq n$.
e) Public encryption key : PU = {e,n}, which is recognized to each person
f) Retain secret or private the decryption key: PR = {d,n}, which is recognized only to the person.

3.1 Data Encryption

a) The original text or message M, where $0 \leq M \leq n$.
b) Find the public key of receiver, PU={e,n}.
c) Calculate the cipher C: $C = M^e \bmod n$

3.2 Data Decryption

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

a) The cipher text C
b) Uses their private key, PR={d,n}
c) Calculate message M: $M = C^d \bmod n$

3.3 Structure of RSA Algorithm

RSA encryption is a public key encryption well established by RSA Data Security. The RSA algorithm is created on the trouble in factoring very huge numbers. Based on this norm, the RSA encryption algorithm procedures prime factorization as the trap door for encryption. Reasoning an RSA key, consequently, takes a vast volume of time and processing power. RSA is the typical encryption method for essential data, particularly data that's communicated over the Internet. Figure 3.1 shows the structure of the RSA algorithm.

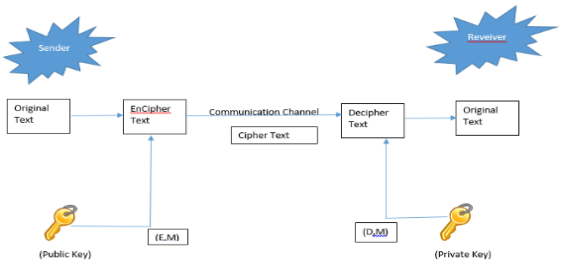

Figure 3.1. Structure of RSA Algorithm

IV. PROPOSED RK-RSA ALGORITHM AND ANALYSIS

The block diagram of the proposed RK-RSA algorithm which is attained by RSA and RK technique is shown in Figure 4.1. The RK-RSA algorithm is detailed below.

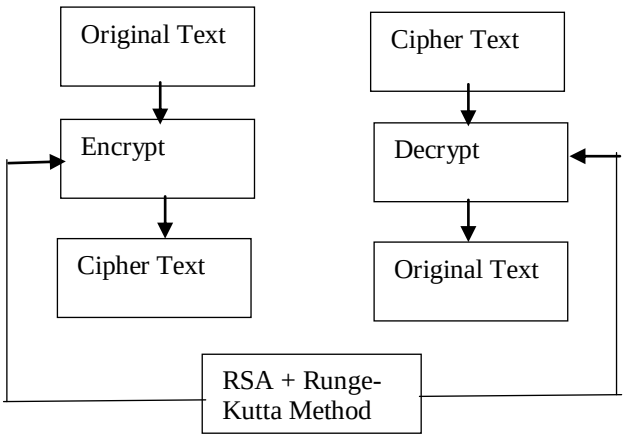

Figure 4.1. Block diagram of RK-RSA Algorithm

4.1 Runge-Kutta Method

The Taylor's series method [13] of explaining differential equation numerically is handicapped by the survival of finding the higher order derivatives.

Euler's method is less competent in practical problems as it needs calculation of higher order derivatives with *h* as small. But the RK methods do not need the calculations of higher order derivatives [14,15].

Exactitude is the best in the RK methods [16] and the error value is low. It is the most perfect of numerical approximation techniques. RK methods belong to a family of one-step method. In one step method the global error is the same order as local error. In one-step methods, the information from only one preceding point is considered, that is to evaluate the value $y_i$it needs the conditions at the previous point y_{i-1} only. They are all founded on the general form of the extrapolation equation

$$y_{i+1} = y_i + slop\ x\ interval\ size$$

$$= y_i + mh$$

where *m* represents the slope at numerous points in the interval *h*.

RK methods are self-starting and easy to program for digital computers [17]. Second order RK methods are obtained using two slopes in the RK methods [18,19]. The method has one arbitrary parameter whose value is suitably chosen. The following method is one such choice

$$y_{i+1} = yi + \frac{1}{2}(k_1 + k_2)$$

where $k_1 = hf(x_i,y_i)$ and

$$k_2 = hf(x_i+h, y_i+k_1)$$

4.2 RK-RSA

The *F* function [20,21,22] is improved in such a way that the competence of RK-RSA is greater than that of the RSA algorithm in terms of speed and security.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

dydx=0.5(y*(1-(y/100)))*

This modified *F* function supports to encrypt and decrypt the given texts of the entire file. These operations take the place in 3 steps thereby reducing the time for every decryption.

V. EXPERIMENTAL RESULTS

The experimentation was completed with the input file size changing from 226 bytes to 289 bytes. Each file size is intended for the average of the ten values (ten times). A Laptop with Intel(R) Celeron(R) CPU3865U@1.80GHz 1.80GHZ is used in which the performance data are added. The performance metrics were the encryption time, decryption time, execution speed, encryption throughput, decryption throughput and avalanche effect. The RK-RSA algorithm is applied using MATLAB.

The experimental results of several performance metrices for the RK-RSA algorithm are detailed below.

5.1 Encryption Time

Encryption time is the time taken to convert plaintext message to cipher text. Figure 5.3 shows the average encryption time for different input size for the encryption time. In the bar chart, the average encryption time for RK-RSA algorithm when compared to the RSA algorithm takes the tiniest time. The results are detailed as shown in Table 5.1.

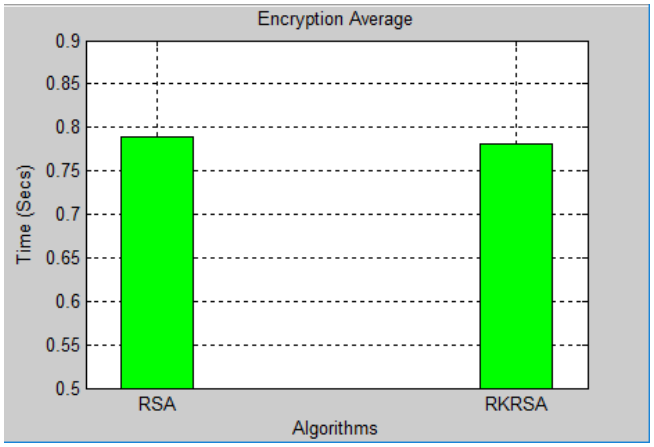

Figure 5.1. Comparison of Average Encryption Time

Table 5.1. Comparative Encryption Times (in Secs)

Input Size in Bytes	RSA	RK_RSA
226	0.602258	0.613445
252	0.744034	0.712629
253	0.723753	0.712525
263	0.782120	0.773362
268	0.791476	0.790323
270	0.805340	0.799510
279	0.866912	0.871408
280	0.834226	0.847019
282	0.862093	0.837777
289	0.871534	0.858908
Average Time (Secs)	0.7883746	0.7816906

5.2 Decryption Time

Decryption time is defined as, the time taken for generating plain text from the cipher text. Figure 5.2 shows the average decryption time for different input size for the encryption time. Clearly, the amount of decryption time taken by RK-RSA algorithm is the least compared to the RSA algorithm from the bar chart. The results are shown in Table 5.2.

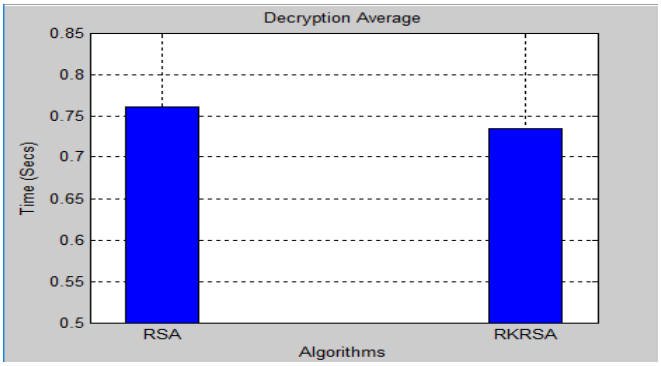

Figure 5.2. Comparison of Average Decryption Time

Table 5.2. Comparative Decryption Times (in Secs)

Input Size in Bytes	RSA	RK_RSA
226	0.560304	0.564343
252	0.693223	0.694658
253	0.782367	0.672388
263	0.775782	0.717334
268	0.764340	0.731002

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

270	0.769396	0.752547
279	0.834860	0.811948
280	0.809466	0.803145
282	0.794328	0.785748
289	0.824921	0.815846
Average Time (Secs)	0.7608987	0.7348959

5.3 Execution Time

The Execution time is defined as the time taken for generating a cipher text from plain text and plain text from the cipher text. Figure 5.3 shows the average execution time for different input size for the execution time. It is clear from the bar chart, the execution time for RK-RSA algorithm is the smallest as compared to the RSA algorithm. The results are detailed as shown in the Table 5.3.

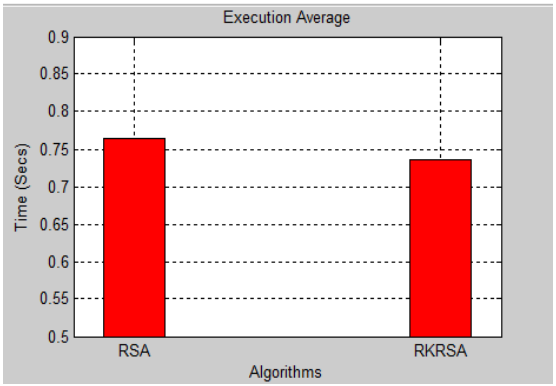

Figure 5.3. Comparison of Execution Time

Table 5.3. Comparative Execution Times (in Secs)

Input Size in Bytes	RSA	RK_RSA
226	0.573907	0.565474
252	0.694055	0.695677
253	0.783417	0.673372
263	0.776696	0.718339
268	0.765315	0.731968
270	0.772589	0.753626
279	0.836048	0.812941
280	0.810452	0.804144
282	0.795308	0.786582
289	0.826452	0.817084
Average Time (Secs)	0.7634239	0.7359207

5.4 Encryption Throughput

Figure 5.4 shows the comparison of Encryption Throughput of RSA and RK-RSA algorithm with different input files. It is clearly seen from the bar chart, RK-RSA algorithm has the highest encryption Throughput as compared to the RSA algorithm. The results are detailed as given in the Table 5.4.

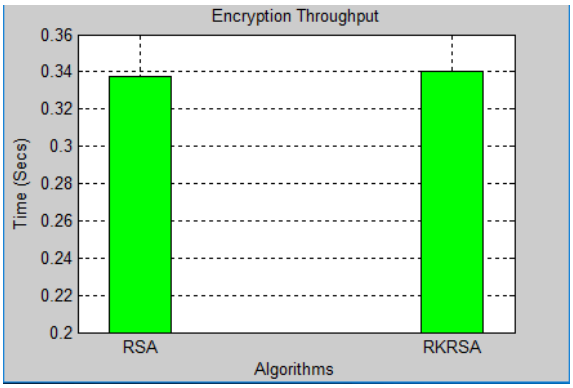

Figure 5.4. Comparison of Encryption Throughput

5.5 Decryption Throughput

Figure 5.5 shows the comparison of Decryption Throughput of RSA and RK-RSA algorithm with different input data files. The bar chart clearly shows that the RK-RSA algorithm has the highest decryption Throughput as compared to the RSA algorithm. The results are detailed as given in the Table 5.4.

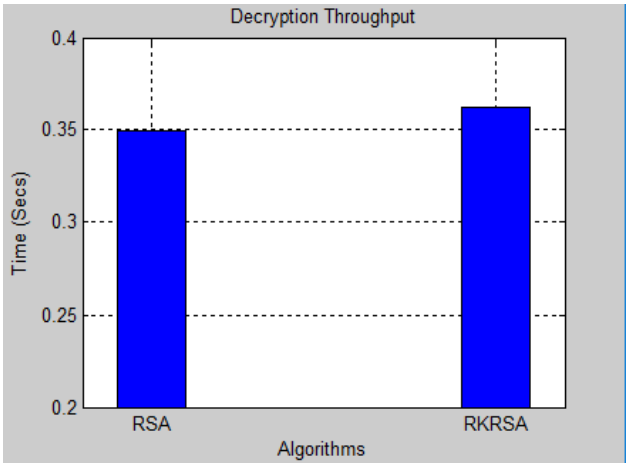

Figure 5.5. Comparison of Decryption Throughput

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

Table 5.4. Comparison of RSA and RK-RSA Algorithm

Input Size in Bytes	RSA			RK_RSA		
	ET	DT	EXT	ET	DT	EXT
226	0.602258	0.560304	0.573907	0.613445	0.564343	0.565474
252	0.744034	0.693223	0.694055	0.712629	0.694658	0.695677
253	0.723753	0.782367	0.783417	0.712525	0.672388	0.673372
263	0.782120	0.775782	0.776696	0.773362	0.717334	0.718339
268	0.791476	0.764340	0.765315	0.790323	0.731002	0.731968
270	0.805340	0.769396	0.772589	0.799510	0.752547	0.753626
279	0.866912	0.834860	0.836048	0.871408	0.811948	0.812941
280	0.834226	0.809466	0.810452	0.847019	0.803145	0.804144
282	0.862093	0.794328	0.795308	0.837777	0.785748	0.786582
289	0.871534	0.824921	0.826452	0.858908	0.815846	0.817084
Average	0.7883746	0.7608987	0.7634239	0.7816906	0.7348959	0.7359207
Throughput (KB/Secs)	0.337656743	0.349849461	0.348692253	0.340543944	0.362228174	0.361723756

5.6 Execution Throughput

Figure 5.6 shows the comparison of Execution Throughput of RSA and RK-RSA algorithm with different input data files. The RK-RSA algorithm has the highest execution Throughput when compared to the RSA algorithm. The results are detailed as given in Table 5.4.

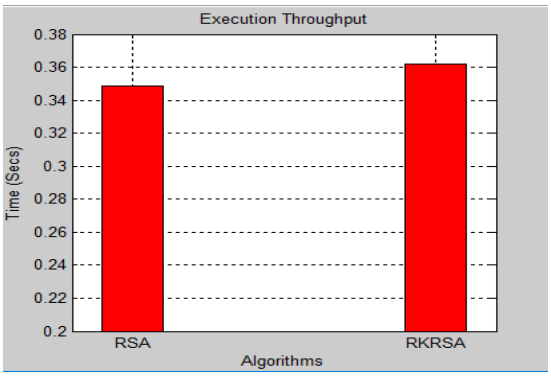

Figure 5.6. Comparison of Execution Throughput

5.7 Power Consumption

From the above findings it is clearly proved that the power consumption will be the least for RK-RSA algorithm which has the highest Execution Throughput when compared to the RSA algorithm.

5.8 Avalanche Effect

When a modification in one bit of the original text or one bit of the key schedule techniques is changed there occurs changes in many bits of the cipher text and that is called Avalanche effect. Thus higher the Avalanche value, higher will be the security.

Figure 5.7 shows the evaluation of Avalanche effect of RSA and RK-RSA algorithm with different input data files. The bar chart clearly shows that the RSA algorithm has the lowest Avalanche effect when compared to the RK-RSA algorithm. The results are detailed in Table 5.5.

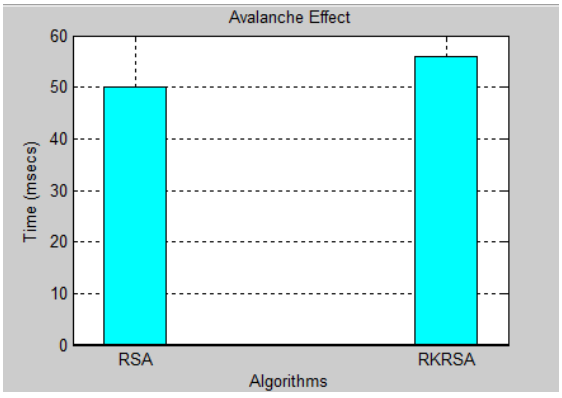

Figure 5.7. Comparison of Avalanche effect

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

Table 5.5. Comparison of Avalanche Effect

Encryption Technique	Avalanche Effect
RSA	50
RK_RSA	56

VI. CONCLUSION

RK-RSA has the better performance compared to the RSA algorithm. Firstly, it consumes less time compared to the RSA algorithm. Secondly, the Throughput is higher than the existing RSA algorithm. Thirdly, high security metrics which are the result of high Avalanche value. Further hybrid techniques with RSA can be developed in future.

REFERENCES

[1] U.S. National Bureau of Standards, "Data encryption standard", U.S. Fed. Inform. Processing Standards Pub., FIPS PUB 46, January 1977, pp. 2-27.

[2] Dilbag Singh and Ajit Singh, "A Secure Private Key Encryption Technique for Data Securiy in Model Cryptosystem", BIJIT Journal, ISSN 0973-5658, Vol. 2, BIJIT 2010, pp. 251-254, 270.

[3] Nehha Mishra, Shahid Siddiqui and Jitwst P. Tripathi, "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues", BIJIT Journal, ISSN 0973-5658, Vol. 7, BIJIT 2015, pp.810-814.

[4] A. Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn.

[5] Atul Kahte, "Cryptography and Network Security", Tata McGraw Hill, 2007.

[6] Kahata, A., "Cryptography and Network Security", Tsinghua University Press, 2005, Beijing, China.

[7] Chen, Z., "The encryption algorithm and security of RSA", J.Hengyang Normal Univ., 2012, 12:69-69

[8] Wei, X., Z.Li and Y.Zhu "On the RSA algorithm and application", J. Honghe Univ., 2011, 4 :31-32

[9] Shi, Z., "Computer Network Security Tutorial", Tsinghua University Press, 2007, Beijing, China

[10] Cai, C. and Y. Lu, "Asymmetric encryption JAVA and VC Computer Knowledge", Technol., 2011, 18:4306-4307

[11] Chen, C and Z. Zhu, "Application of RSA algorithm and implementation details", Computer Eng. Sci., 2006, 9:13-14

[12] William Stallings, "Cryptography and Network Security", Fifth Edition, Pearson Education, 2011, pp. 119-120.

[13] M.K.Jain, S.R.K. Iyengar, and R.K.Jain, "Numerical Methods for Scientific and Engineering Computation", Fifth Edition, New Age International Publishers, 2007, pp. 438-445.

[14] L.F. Shampine and H.A.Watts, "Comparing Error Estimators for Runge-Kutta Methods", Mathematics of Computation, Vol. 25, Number 115, July 1971, pp.445-455.

[15] S.S.Sastry, "Introductory Methods of Numerical Analysis", Fourth Edition, 2009, pp. 304-306.

[16] E. Balagurusamy, "Numerical Methods", Tata McGraw-Hill Education Private Limited, pp. 436-437.

[17] S.R.K.Iyengar and R.K.Jain, "Numerical Methods", First Edition, New Age International Publishers, 2009, pp. 200-203.

[18] Ashok Kumar and T. E.Unny, "Application of Runge-Kutta method for the solution of non-linear partial differential equations", Applied Mathematical Modelling, Elsevier, Vol.1, Issue4, March1977, pp. 199-204.

Published by: The Mattingley Publishing Co., Inc.

May – June 2020
ISSN: 0193-4120 Page No. 11850 - 11857

[19] J.C. Butcher, "A History of Runge-Kutta Methods", Elsevier, Applied Numerical Mathematics, Vol. 20, 1996, pp. 247-260.

[20] V. Josephraj and B.Shamina Ross, "Enhancement of Blowfish Encryption in Terms of Security Using Mixed Strategy Technique", IIOAB Journal, ISSN 0976-3104, Vol.7, Special Issue-Emerging Technology in Networking and Security 2016, pp. 69-76.

[21] V. Josephraj and B.Shamina Ross, "A Hybrid Blowfish Encryption Algorithm Using Nash Equilibrium with Cautious Attackers", International Journal of Control Theory and Applicattions, ISSN 0974-5572, 2016, pp.4761-4769.

[22] V. Josephraj and B.Shamina Ross, "Security Evaluation of Blowfish and Its Modified Version Using GT's One Shot Category of Nash Equilibrium", International Journal of Control Theory and Applications, ISSN 0974-5572, 2016, pp.4771-4777.

Published by: The Mattingley Publishing Co., Inc.