DATA SECURITY USING RJB32 METHOD

R. Jaichandran[1], Dr. Avinash Sharma[2] , Nethaji A[3], Nithish Kumar K.N[4], Guru Vignesh M[5], and Suhail Jalal[6]**

[1,3,4,5,6] Department Of Computer Science And Engineering
Aarupadai Veedu Institute Of Technology
Vinayaka Mission'S Research Foundation
Paiyanoor-603 104, Tamil Nadu, India.
[1]rjaichandran@avit.ac.in, [3]mukesh.ajay99@gmail.com, [4]98nitish@gmail.com
[5]guruvigneshvijay@gmail.com, [6]asifjalal1998@gmail.com

[2]Professor, CSE Department, M.M. Deemed to be University, Mullana, Haryana, India, 133207
asharma@mmumullana.org
Corresponding Author: **Dr. Avinash Sharma[2]****

Abstract. The present world is data world; without this data cannot survive in present stage. This data produced more from social media; this media data is public data; This public data not have good security; so to overcome this issue we apply the Salsa method. This method easily hack the data from the hackers. RBJ32 method has 5 steps. 1. Applying the key and multiply that key; 2. To apply the prime number in the S^2 and T^2; 3. To calculate the EA1 and EA2; 4. To swap the EA1 and EA2 in matrix EnA; 5. Apply the column operations. The proposed method provides good security while comparing with Salsa method.

Key words: RJB32, Prime, Salsa, Encryption, Decryption.

1. INTRODUCTION

The present world is data world; without this data cannot survive in present stage. This data produced more from social media; this media data is public data; This public data not have good security; so to overcome this issue we apply the Salsa method. This method easily hack the data from the hackers. The additional rotations XOR for ChaCha is fault attack [1]. This author is used new hash concept for key guessing and halting condition [2]. Author was introduced the bricklayer attack for analysis of ChaCha [3]. They mainly focus the security for Double A [4]. They made new design for secure fast and flexible algorithm [5]. SRB18 method used to provide security for data [6]. SRB21 method used to provide security for data [7]. CBB21 method

TABLE 1. Applying prime numbers in ES and ET

S	T	S^2	T^2	**Equation(2) and (6)**	**Equation(3) and (7)**
3	1	9	1	8	10
5	1	25	1	24	26

7	3	49	9	40	58
9	3	81	9	72	90

used to provide security for data [8]. CBB22 method used to provide security for data [9]. To overcome this problem introduced the novel method RJB32(Rajaprakash Jaichandran and Bagath Basha) 32.

2. METHODS

- RJB32 method are Table 2 and Table 3 are encryption and decryption.

3. ENCRYPTION

- A is a data analyzed matrix. [10]

$$\text{EnA}=\begin{pmatrix} 102 & 103 & 104 \\ 106 & 105 & 105 \\ 108 & 110 & 102 \end{pmatrix}$$

Se=1/3

Equation (1)"

$$\text{EnA}=\begin{pmatrix} 102/3 & 103/3 & 104/3 \\ 106/3 & 105/3 & 105/3 \\ 108/3 & 110/3 & 102/3 \end{pmatrix}$$

"Pair-1(8,10)"

$$\text{EnA}=\begin{pmatrix} 110/3 & 103/3 & 104/3 \\ 106/3 & 105/3 & 105/3 \\ 108/3 & 102/3 & 102/3 \end{pmatrix}$$

TABLE 2. RJB32 Encryption

STEPS	RJB32 ENCRYPTION
1	Analyzed the prediction data from social media.
2	Convert the prediction data to matrix A.
3	EnA = Se* A **(1)** where EnA is encryption matrix A.
4	Applying the prime numbers ES and ET.
5	Calculate the ES^2 and ET^2.
6	$EA1 = ES^2 - ET^2$ **(2)**
7	$EB1 = ES^2 + ET^2$ **(3)**

8	If EA1 and EB1 value will be above size of the matrix then add and make it single digit values
9	Swap EA1 and EB1 in EnA
10	$CA = C_i <-> (C_{i+(n-m)})$**(4)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers

"Pair-2(24,26)"

$$\text{EnA=}\begin{pmatrix} 110/3 & 103/3 & 104/3 \\ 106/3 & 105/3 & 102/3 \\ 108/3 & 105/3 & 102/3 \end{pmatrix}$$

"Pair-3(40,58)"

$$\text{EnA=}\begin{pmatrix} 110/3 & 103/3 & 104/3 \\ 106/3 & 105/3 & 102/3 \\ 108/3 & 105/3 & 102/3 \end{pmatrix}$$

"Pair-4(72,90)"

$$\text{EnA=}\begin{pmatrix} 110/3 & 103/3 & 104/3 \\ 106/3 & 105/3 & 102/3 \\ 108/3 & 105/3 & 102/3 \end{pmatrix}$$

Equation(4)

$$\text{CA=}\begin{pmatrix} 104/3 & 103/3 & 110/3 \\ 102/3 & 105/3 & 106/3 \\ 102/3 & 105/3 & 108/3 \end{pmatrix}$$

4. DECRYPTION

$$\text{DnA=}\begin{pmatrix} 104/3 & 103/3 & 110/3 \\ 102/3 & 105/3 & 106/3 \\ 102/3 & 105/3 & 108/3 \end{pmatrix}$$

TABLE 3. RBJ32 Decryption

STEPS	RJB32 DECRYPTION
1	$DA = D_i <-> (D_{i+(n-m)})$**(5)** where CA is Column encrypted matrix, C is a columns, i, n and m is column numbers
2	Applying the prime numbers DS and DT.
3	Calculate the DS^2 and DT^2.
4	$DA1 = DS^2 - DT^2$ **(6)**
5	$DB1 = DS^2 + DT^2$ **(7)**
6	Swap A1 and B1

7	DnA = A/Se **(8)** where DnA is decryption matrix A.

Equation(5)

$$\text{DnA}=\begin{pmatrix}110/3 & 103/3 & 104/3\\ 106/3 & 105/3 & 102/3\\ 108/3 & 105/3 & 102/3\end{pmatrix}$$

"Pair-1(90,72)"

$$\text{DnA}=\begin{pmatrix}110/3 & 103/3 & 104/3\\ 106/3 & 105/3 & 102/3\\ 108/3 & 105/3 & 102/3\end{pmatrix}$$

"Pair-2(58,40)"

$$\text{DnA}=\begin{pmatrix}110/3 & 103/3 & 104/3\\ 106/3 & 105/3 & 102/3\\ 108/3 & 105/3 & 102/3\end{pmatrix}$$

"Pair-3(26,24)"

$$\text{DnA}=\begin{pmatrix}110/3 & 103/3 & 104/3\\ 106/3 & 105/3 & 105/3\\ 108/3 & 102/3 & 102/3\end{pmatrix}$$

Pair-4(10, 8)"

$$\text{DnA}=\begin{pmatrix}102/3 & 103/3 & 104/3\\ 106/3 & 105/3 & 105/3\\ 108/3 & 110/3 & 102/3\end{pmatrix}$$

"Equation (8)"

$$\text{EnA}=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

5. CONCLUSION

The present world is data world; without this data cannot survive in present stage. This data produced more from social media; this media data is public data; This public data not have good security; so to overcome this issue we apply the Salsa method. This method easily hack the data from the hackers. RBJ32 method has 5 steps. 1. Applying the key and multiply that key; 2. To apply the prime number in the S^2 and T^2; 3. To calculate the EA1 and EA2; 4. To swap the EA1 and EA2 in matrix EnA; 5. Apply the column operations. The RJB32 method provide good security while compared with Salsa method. In the future, to add the prime factors operations of the data security.

REFERENCES

[1] P. A. BABU AND J. J. THOMAS: A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20, Wo. on Fa. Di. and To. in Cr. (2017), 33-40.

[2] S. V. D. KUMAR, S. PATRANABIS, J. BREIER, D. MUKHOPADHYAY, S. BHASIN, A. CHATTOPADHYAY, AND A. BAKS: Freestyle, a randomized version of ChaCha for resisting offline brute-force and dictionary attacks, IE. tr. on In. Fo. and Se. (2018).

[3] A. ADOMNICAI, J. J. A. FOURNIER, AND L. MASSON: Bricklayer Attack: A Side- Channel Analysis on the ChaCha Quarter Round, Pr. in Cr. In., Le. No. in Co. Sc., Sp. 65-84.

[4] B. MAZUMDAR, S.K. S. ALI AND O. SINANOGLU: Power Analysis Attacks on ARX: An Application to Salsa20, On-. Te. Sy. IE. (2015), 40-43.

[5] C. WATT, J. RENNER, N. POPESCU, S. CAULIGI, AND D. STEFAN: CT-Wasm: Type- Driven Secure Cryptography for The Web Ecosystem, Pr. ACM Pr. La. PO. (2019), 77:1-77:29.

[6] C. BAGATH BASHA, S. RAJAPRAKASH: Enhancing The Security Using SRB18 Method of Embedding Computing, Mic. and Mic 103125, (2020).

[7] C. B. BASHA, S. RAJAPRAKASH: Securing Twitter Data Using Srb21 Phase I Methodology, Int. Jou. of Sci. and Tec. Res. 8(12) (2019), 1952–1955.

[8] C. B. BASHA, S. RAJAPRAKASH: Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data, Adv. In Mat. : Sci. Jou. 9(3) (2020), 1085-1091.

[9] C. B. BASHA, S. RAJAPRAKASH, V. V. A. HARISH, M. S. KRISHNA, K. PRABHAS: Securing Twitter Analysed Data Using CBB22 Algorithm, Adv. In Mat. : Sci. Jou. 9(3) (2020), 1093-1100.

[10] C. B. BASHA, K. SOMASUNDARAM: A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data, Int. Jou. of Rec. Tec. and Eng. 8(1) (2019), 591-599.

[11] Somasekar, J. & Sharma, A. & Reddy, N. & Reddy, Y.. (2020). IMAGE ANALYSIS FOR AUTOMATIC ENUMERATION OF RBC INFECTED WITH PLASMODIUM PARASITES-IMPLICATIONS FOR MALARIA DIAGNOSIS. Advances in Mathematics: Scientific Journal. 9. 1221-1230. 10.37418/amsj.9.3.48.

[12] A. SHARMA1 AND J. SOMASEKAR "Contrast Image Construction Technique for Medical Imaging" published in Advances in Mathematics: Scientific Journal (Adv. Math., Sci. J.) vol-9-no-6-2020 (pp 3325–3329)

[13] *Rohini Goel, Avinash Sharma, and Rajiv Kapoor,* "Object Recognition Using Deep Learning" published in Journal of Computational and Theoretical Nanoscience Vol. 16, 4044–4052, 2019

[14] Santosh, Mamta & Sharma, Avinash. (2019). A Proposed Framework for Emotion Recognition Using Canberra Distance Classifier. Journal of Computational and Theoretical Nanoscience. 16. 3778-3782. 10.1166/jctn.2019.8250.

[15] Mamta Santosh, Avinash Sharma, "Facial Expression Recognition using Fusion of LBP and HoG Features" published in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019