European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 11, 2020

Securing Social Media Data Using Rjb31 Method

K. L. Shunmuganathan1, Dr. Avinash Sharma2 ,
Arun Dev Sp3, Abhiraj J4, Aadish Kr5, and Saikiran Pasupula6**

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.
1klsnathan@avit.ac.in, 3arundevsp@gmail.com,
4abhiraj.jayaraj31@gmail.com, 5Aadishkr7@gmail.com,
6saikiran.pasupula@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 did not have well security; so we applying the Salsa method. This method easily hack the data from the hackers. RBJ31 method has 4 steps. 1. Applying the secret key and multiply that key; 2. To apply the prime number and calculate the $S^2$and T^2; 3. To calculate the EA1 and EA2; 4. To swap the EA1 and EA2 in matrix EnA. The proposed method gives well security while comparing with Salsa method.
Keywords: RJB31,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 did not have well security; so we applying 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 focuse 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 used to

provide security for data [8]. CBB22 method used to provide security for data [9]. To overcome this problem introduced the novel method RJB31(Rajaprakash Jaichandran and Bagath Basha) 31.

TABLE 1. Applying prime numbers in ES and ET

S	T	S^2	T^2	**Equation(2) and(3)**	**Equation(4) and(5)**
3	1	9	1	8	10
5	1	25	1	24	26
7	3	49	9	40	58
9	3	81	9	72	90

2. METHODS

- RJB31 method are Table 2 and Table 3 are encryption and decryption.

3. ENCRYPTION

- "A is a data analyzed matrix". [10]

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

Se=1/3

"Equation (1)"

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

"Pair-1(8,10)"

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

"Pair-2(24,26)"

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

TABLE 2. RJB31Encryption

STEPS	RJB31 ENCRYPTION
1	"The data analyzed from social data".
2	"The data * will form a matrix".
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

TABLE 3. RBJ31 Decryption

STEPS	RJB31 DECRYPTION
1	Applying the prime numbers DS and DT.
2	Calculate the $DS^2$and DT^2.
3	$DA1 = DS^2 - DT^2$ **(4)**
4	$DB1 = DS^2 + DT^2$ **(5)**
5	Swap A1 and B1
6	DnA = A/Se **(6)** where DnA is decryption matrix A.

"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)"

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

4. DECRYPTION

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

"Pair-1(90,72)"

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

"Pair-2(58,40)"

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

"Pair-3(26,24)"

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

Pair-4(10, 8)"

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

"Equation (6)"

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

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 did not have well security; so we applying the Salsa method. This method easily hack the data from the hackers. RBJ31 method has 4 steps. 1. Applying the secret key and multiply that key; 2. To apply the prime number and calculate the S^2 and T^2; 3. To calculate the EA1 and EA2; 4. To swap the EA1 and EA2 in matrix

EnA. The RJB31 method gives well security while compared with Salsa method.

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