ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 4437–4447
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.14 Spec. Issue on RDESTM-2020

SECURING GENERALIZED DATA USING RB24 ALGORITHM

K. KARTHIK[1], S. RAJAPRAKASH, THOM MANDAPATHIL, SAHIL SANTHOSH, AND U. M. AKSHAY

ABSTRACT. The amount of data to be communicated through social media like facebook, twitter, instagram, whatsapp, and etc. These social media data used to analyzed the prediction of future any products. This prediction data has security less, So, D.J. Bernstein introduced the Salsa method for security purpose. But this method contribute only speed of encryption only. In this paper, a novel method is RB24 method. This method has three stages. In the first stage, to create secret key and multiply the key. In the second stage, to swap the prime numbers and non negative integer in given matrix. In the third stage, to swap the M pair numbers. Finally, the proposed method RB24 provide very good security when compared with Salsa method.

1. INTRODUCTION

Today's earth data is increased through social media like whatsapp, instagram, facebook, twitter, and etc. Because data is very important in people life in current situations. This data used to predict the future of any products. This prediction data has security less so, D.J Bernstein introduced Salsa method. This method contributes only speed of encryption not gives the important of security. Salsa20 has 20 rounds and each round has independent round [1]. Salsa20/4 algorithm is compare the diffusion speed and level [2].SRB18 algorithm is multiply the secret key and swap the diagonal elements to first row [3]. SRB21

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68P25.

Key words and phrases. Encryption, Salsa, Security, RB24, Prime number.

algorithm swaps the prime number and secret key [4]. RB20 algorithm is used to swap the perfect numbers [5]. CBB22 algorithm is used to convert the matrix data to quadratic form [6]. CBB21 phase 2 methods is used to swap a co-prime numbers [7]. RB21 algorithm is used to multiply the secret key and swap the perfect numbers [8]. To overcome this drawbacks introduced a novel method RB24 (Rajaprakash and Bagathbasha) method.

2. IMPLEMENTATION OF RB24 ENCRYPTION METHOD

The proposed method RB24 is N x N matrix order. RB24 encryption process is shown in Table 1 and RB24 decryption process is shown in Table 2. The proposed RB24 method is developed from modifying the RB20.

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}$$

where A is analyzed facebook data matrix [9].

Step 1: EA = A * S => S=1/2

$$EA = \begin{bmatrix} 1/2 & 1 & 3/2 & 2 \\ 5/2 & 3 & 7/2 & 4 \\ 9/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where EA is Encryption matrix A.

Step 2: E^n *** M**
EB = 16 => EB=2^2 * 4 =>E=2, n=2, M=4
EB=2^1 * 8=> E=2, n=1, M=8
EB=3^0 * 16=> E=3, n=0, M=16
Pair of numbers (2,4), (2,8), and (3,16)

TABLE 1. RB24 Encryption Method

STEPS	RB24 ENCRYPTION
1	Extracting the data from Twitter.
2	Analyzed facebook data are stored in the matrix A.
3	EA = A * S where EA is encryption matrix A, A is analyzed matrix and S is a Secret key.
4	EB = E^n * M where EB is encryption matrix B, E is a prime number, n>=0, and M is non negative integer.
5	Identify the possible number of prime numbers multiply by the M for order of matrix.
6	To swap an E and M in a matrix B.
7	To identify the number of possible pair of M.
8	EC = P_M * M where EC is encryption matrix C, P is framed pair, and M is non negative integer.
9	To multiply the M in the pairs for only odd pairs.
10	The order of 3, is omit the 1st number from 2nd pair onwards.
11	The order of 4 is to form a pair and check already exits, if exits omit the pair.
12	The pairs must be swapped pair values from left to right from matrix EC.

The 1^{st} pair (2, 4) swapped in the matrix EB, represented start from 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 and 16th cell number is 16-1.

$$FPN = \begin{bmatrix} 1/2 & 1 & 5/2 & 2 \\ 3/2 & 3 & 7/2 & 4 \\ 9/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where FPN is first pair number.

TABLE 2. RB24 Decryption Method

STEPS	RB24 DECRYPTION
1	Getting the data from encrypted data as a matrix EC.
2	DA = D^n * M where DA is decryption matrix A, D is a prime number, n>=0, and M is non negative integer.
3	Identify the number possible pairs of M.
4	DB = P_M * M where DB is decryption matrix B, P is framed pair, and M is non negative integer.
5	To multiply the M in the pairs for only odd pairs.
6	The order of 3, is omit the 1st number from 2nd pair onwards.
7	The order of 4 is to form a pair and check already exits, if exits omit the pair.
8	The pairs must be swapped pair values from right to left from matrix DB.
9	Identify the possible number of prime numbers multiply by the M for order of matrix.
10	To swap a D and M from right to left pair in the matrix DB.
11	Divided by the secret key DC= DA / S, where DC is decryption matrix C and S is secret key.

The 2^{nd} pair (2, 8) swapped from FPN matrix.

$$SPN = \begin{bmatrix} 1/2 & 1 & 9/2 & 2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where SPN is second pair number.

The 3^{rd} pair (3, 16) swapped from SPN matrix.

$$TPN = \begin{bmatrix} 1/2 & 1 & 9/2 & 8 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where TPN is third pair number.

EB = TSN
Step 3: To find the possible number of M pairs.
EC = P_M *** M**
P_M = 4 and M=4 => PM = => P_4 = ( ), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2,3), (1,2,4), (1,3,4), (1,2,3,4)
EC = P_4 * M (Only odd pairs) => EC = (4,8), (1,3), (4,16), (2,3), (8,16), (3,4), (4,8,12), (1,2,4), (4,12,16), (1,2,3,4)
The order of 3, omits the 1st number from 2nd pair onwards.
The order of 4, is to form a pair and check already exits, if exits omit the pair.
Pair of numbers are (4,8), (1,3), (4,16), (2,3), (8,16), (3,4), (4,12), (2,4), (12,16), (1,2)
The 1^{st} pair (4, 8) swapped from TPN matrix, represented start from 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 and 16.

$$FMPN = \begin{bmatrix} 1/2 & 1 & 9/2 & 4 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where FMPN is first M pair number.

The 2^{nd} pair (1, 3) swapped from FMPN matrix.

$$SMPN = \begin{bmatrix} 9/2 & 1 & 1/2 & 4 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where SMPN is second M pair number.

The 3^{rd} pair (4, 16) swapped from SMPN matrix.
The 4^{th} pair (2, 3) swapped from TMPN matrix.
The 5^{th} pair (8, 16) swapped from FMPN matrix.
The 6^{th} pair (3, 4) swapped from FiMPN matrix.
The 7^{th} pair (4, 12) swapped from SMPN matrix.
The 8^{th} pair (2, 4) swapped from SiMPN matrix.
The 9^{th} pair (12, 16) swapped from EMPN matrix.

The 10^{th} pair (1, 2) swapped from NMPN matrix.

$$TeMPN = \begin{bmatrix} 6 & 9/2 & 2 & 1/2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 8 \\ 13/2 & 7 & 15/2 & 1 \end{bmatrix}$$

where TeMPN is tenth M pair number.

EC = TeMPN

3. Implementation of RB24 decryption method

$$EC = \begin{bmatrix} 6 & 9/2 & 2 & 1/2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 8 \\ 13/2 & 7 & 15/2 & 1 \end{bmatrix}$$

where EC is encrypted matrix C.

Step 1: DA=D^n * M
DA = 16 => DA=2^2 * 4 =>E=2, n=2, M=4
P_M = 4 and M=4 => P_4 = ( ), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2,3), (1,2,4), (1,3,4), (1,2,3,4)
Step 2: DB = P_M * M (Only odd pairs)
DB = (4,8), (1,3), (4,16), (2,3), (8,16), (3,4), (4,8,12), (1,2,4), (4,12,16), (1,2,3,4)
Pair of numbers are (2,1), (16,12), (4,2), (12,4), (4,3), (16,8), (3,2), (16,4), (3,1), (8,4)
The 1^{st} pair (2, 1) swapped from EC matrix.

$$DB1 = \begin{bmatrix} 9/2 & 6 & 2 & 1/2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 8 \\ 13/2 & 7 & 15/2 & 1 \end{bmatrix}$$

where DB1 is decrypted matrix B1.

The 2^{nd} pair (16, 12) swapped from DB1 matrix.

$$DB2 = \begin{bmatrix} 9/2 & 6 & 2 & 1/2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 1 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DB2 is decrypted matrix B2.

The 3^{rd} pair (4,2) swapped from DB2 matrix.

$$DB3 = \begin{bmatrix} 9/2 & 1/2 & 2 & 6 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 1 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DB3 is decrypted matrix B3.

The 4^th pair (12,4) swapped from DB3 matrix.

$$DB4 = \begin{bmatrix} 9/2 & 1/2 & 2 & 1 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DB4 is decrypted matrix B4.

The 5^{th} pair (4,3) swapped from DB4 matrix.

$$DB5 = \begin{bmatrix} 9/2 & 1/2 & 1 & 2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DB5 is decrypted matrix B5.

The 6^{th} pair (16,8) swapped from DB5 matrix.

$$DB6 = \begin{bmatrix} 9/2 & 1/2 & 1 & 2 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 4 \end{bmatrix}$$

where DB6 is decrypted matrix B6.

The 7^{th} pair (3,2) swapped from DB6 matrix.

$$DB7 = \begin{bmatrix} 9/2 & 1 & 1/2 & 2 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 4 \end{bmatrix}$$

where DB7 is decrypted matrix B7.

The 8^{th} pair (16,4) swapped from DB7 matrix.

$$DB8 = \begin{bmatrix} 9/2 & 1 & 1/2 & 4 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where DB8 is decrypted matrix B8.

The 9^{th} pair (3,1) swapped from DB8 matrix.

$$DB9 = \begin{bmatrix} 1/2 & 1 & 9/2 & 4 \\ 3/2 & 3 & 7/2 & 8 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where DB9 is decrypted matrix B9.

The 10^{th} pair (8,4) swapped from DB9 matrix.

$$DB10 = \begin{bmatrix} 1/2 & 1 & 9/2 & 8 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 2 \end{bmatrix}$$

where DB10 is decrypted matrix B10.

DB = DB10
DA= D^n * **M**
DA = 16 => DA=2^2 * 4 =>D=2, n=2, M=4
DA=2^1 * 8=> D=2, n=1, M=8
DA=3^0 * 16=> D=3, n=0, M=16

Pair of numbers (16, 3), (8, 2) and (4,2)
The 1^{st}pair (16,3) swapped from DC matrix.

$$DA1 = \begin{bmatrix} 1/2 & 1 & 9/2 & 2 \\ 3/2 & 3 & 7/2 & 4 \\ 5/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DA1 is decrypted matrix A1.

The 2^{nd}pair (8,2) swapped from DA1 matrix.

$$DA2 = \begin{bmatrix} 1/2 & 1 & 5/2 & 2 \\ 3/2 & 3 & 7/2 & 4 \\ 9/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DA2 is decrypted matrix A2.

The 3^{rd}pair (4,2) swapped from DA2 matrix.

$$DA3 = \begin{bmatrix} 1/2 & 1 & 3/2 & 2 \\ 5/2 & 3 & 7/2 & 4 \\ 9/2 & 5 & 11/2 & 6 \\ 13/2 & 7 & 15/2 & 8 \end{bmatrix}$$

where DA3 is decrypted matrix A3.

DA = DA3 **Step 3: DC=DA / S** =>S=1/2

$$DC = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}$$

where DC is decrypted matrix C.
DC = A .

4. Conclusion

Today's earth is very important for security to all the purposes. For example, credit and debit card transactions, bank data, and prediction data.

(1) RB24 has N rounds and Salsa has four rounds.

(2) Encryption and decryption time is high in RB24 but less time in Salsa.
(3) Security is high in RB24 and less security in Slasa.
(4) RB24 used prime numbers and Salsa not used prime numbers. The proposed RB24 method is security is high because of prime number and secret key while compared with Salsa.

In future, more operations will be add for data security.

REFERENCES

[1] Z. SHAO, L. DING: *Related-Cipher Attack on Salsa20*, Proc. Fou. Inter. Conf. on Comp. and Inf. Sci., (2012), 1182–1185.
[2] M. ALMAZROOIE, A. SAMSUDIN, M. M. SINGH: *Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map*, J. of Inf. Pro. Sy., **11**(4) (2015), 310-324.
[3] C. BAGATH BASHA, S. RAJAPRAKASH: *Enhancing The Security Using SRB18 Method of Embedding Computing*, Mir. and Mic, ID103125, 2020.
[4] C. BAGATH BASHA, S. RAJAPRAKASH: *Securing Twitter Data Using Srb21 Phase I Methodology*, Inter. J. of Sci. and Tech. Res., **8**(12) (2019), 1952–1955.
[5] K. KARTHIK, C. BAGATH BASHA, U. BHASWANTH THILAK, T. SAI KIRAN, J. RAJ: *Securing Social Media Analyzed Data Using RB20 Method*, Adv. In Mat. :Sci. Jou., **9**(3) (2020), 1157-1163.
[6] C. BAGATH 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.
[7] C. BAGATH BASHA, S. RAJAPRAKASH: *Applying The CBB21 Phase 2 Method For Securing Twitter Analysed Data*, Adv. In Mat. : Sci. Jou., **9**(3) (2020), 1085-1091.
[8] S. RAJAPRAKASH, K. KARTHIK, A. MOHAN, S. SARKAR, J. MATHEW: *Design of New Security System Using RB21 Algorithm*, Adv. In Mat. Sci. Jou., **9**(3) (2020), 1149-1155.
[9] C. BAGATH BASHA, K. SOMASUNDARAM: *A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data*, Inter. J. of Rec. Tech. and Eng., **8**(1) (2019), 591-599.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA
Email address: karthik@avit.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AARUPADAI VEEDU INSTITUTE OF TECHNOLOGY
VINAYAKA MISSION'S RESEARCH FOUNDATION
CHENNAI, TAMIL NADU, INDIA