ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1149–1155
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.40 Spec. Issue on RDESTM-2020

DESIGN OF NEW SECURITY SYSTEM USING RB21 ALGORITHM

S. RAJAPRAKASH[1], K. KARTHIK, A. MOHAN, S. SARKAR, AND J. MATHEW

ABSTRACT. The security of Salsa family has introduced by Daniel Bernstein for encryption speed purpose only. In this paper, the proposed algorithm has two processes. The first process is secret key multiplication in the matrix. The second process is to find a perfect numbers with the help of prime numbers. The proposed method calculate the time and compared with both AES and Salsa. The proposed method has very good security while compare to both AES and Salsa algorithm.

1. INTRODUCTION

Today's the security is very important to all the purposes in the world. For example, data need more security because personal data transaction, credit and debit card data transactions, machine learning algorithm prediction data and Facebook analyzed data.This author studied about Salsa20, and it is used convenient rounds and every round has independent round [1]. They discussed about Salsa20/4 and proposed chaotic Salsa. These algorithms used to compare the diffusion level and speed [2]. This author discussed about ChaCha8 and Salsa20/9. These attacks are mainly used to reducing of complexity of the previous attack [3]. Author studied the Salsa20 family attack model. From this family best attack model is Salsa20/12 and Salsa20/8 [4]. Author proposed the novel algorithm is Probabilistic Neutral Bits. Salsa20 design is proposed by author, this design is quicker than AES [5]. SRB21 methodology are proposed by

[1] *corresponding author*

Key words and phrases. Encryption, Polarity, Salsa, Security, RB20, Twitter, Tweets, Facebook.

Somasundaram Rajaprakash Bagahbasha21. The proposed algorithm has interchanging the prime number secret key and secret key [6]. To overcome these issues, to proposed new algorithm Rajaprakash Bagathbasha21 (RB21) in this current work.

2. Methodology: RB21 Encryption and decryption algorithm

The proposed methodology RB21 with the matrix of order N by N. The proposed algorithm has shown in Table 2 and Table 3.

Table 1. PERFECT NUMBERS

STEPS	e value	K value	PN
1	2	2	6
2	2	3	28
1	2	5	496
1	2	7	8128

3. Implementation of RB21 Encryption Algorithm

This section explained the RB21encryption algorithm below

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix},$$

where A is analyzed twitter or facebook data matrix [7].

By applying equation "(1)" and ek=5

$$A = \begin{bmatrix} 5 & 10 & 15 \\ 20 & 25 & 30 \\ 35 & 40 & 45 \end{bmatrix}.$$

Finally, PN = 6284968128 as shown in Table 1, it's equalling to

$$3010402045304051040.$$

Pair of perfect numbers (3,0),(1,0),(4,0),(2,0),(4,5), (3,0),(4,0),(5,1),(0,4).

Step 1: The 1st pair of perfect number (3, 0) should be swapped in the given matrix and this matrix represented start from 0, 1, 2, 3, 4, 5, 6, 7, and 8.

$$FPN = \begin{bmatrix} 20 & 10 & 15 \\ 5 & 25 & 30 \\ 35 & 40 & 45 \end{bmatrix},$$

where FPN is first pair of perfect number.

Step 2: The 2nd pair of perfect number (1, 0).

$$SPN = \begin{bmatrix} 10 & 20 & 15 \\ 5 & 25 & 30 \\ 35 & 40 & 45 \end{bmatrix},$$

where SPN is second pair of perfect number.

Step 3: The 3rd pair of perfect number (4, 0).

$$TPN = \begin{bmatrix} 25 & 20 & 15 \\ 5 & 10 & 30 \\ 35 & 40 & 45 \end{bmatrix},$$

where TPN is third pair of perfect number.

Step 4: The 4th pair of perfect number (2, 0).

$$FOPN = \begin{bmatrix} 15 & 20 & 25 \\ 5 & 10 & 30 \\ 35 & 40 & 45 \end{bmatrix},$$

where FOPN is fourth pair of perfect number.

Step 5: The 5th pair of perfect number (4, 5).

$$FIPN = \begin{bmatrix} 15 & 20 & 25 \\ 5 & 30 & 10 \\ 35 & 40 & 45 \end{bmatrix},$$

where FIPN is fifth pair of perfect number.

Step 6: The 6th pair of perfect number (3, 0).

$$SIPN = \begin{bmatrix} 5 & 20 & 25 \\ 15 & 30 & 10 \\ 35 & 40 & 45 \end{bmatrix},$$

where SIPN is sixth pair of perfect number.

Step 7: The 7th pair of perfect number (4, 0).

$$SEPN = \begin{bmatrix} 30 & 20 & 25 \\ 15 & 5 & 10 \\ 35 & 40 & 45 \end{bmatrix},$$

where SEPN is seventh pair of perfect number.

Step 8: The 8th pair of perfect number (5, 1).

$$EPN = \begin{bmatrix} 30 & 10 & 25 \\ 15 & 5 & 20 \\ 35 & 40 & 45 \end{bmatrix},$$

where EPN is eight pair of perfect number.

Step 9: The 9th pair of perfect number (0, 4).

$$NPN = \begin{bmatrix} 5 & 10 & 25 \\ 15 & 30 & 20 \\ 35 & 40 & 45 \end{bmatrix},$$

where NPN is nine pair of perfect number.

Finally, the original matrix could be encrypted successfully.

4. Implementation of RB21 Decryption Algorithm

By applying equations (3) Finally, PN = 6284968128, it equalling to

$$30104020453040510 40$$

as shown in Table 1. Pair of perfect numbers (4,0), (1,5), (0,4), (0,3), (5,4), (0,2), (0,4), (0,1), (0,3) should be swapped in the encrypted matrix and this matrix represented start from 0, 1, 2, 3, 4, 5, 6, 7, and 8.

$$DPN = \begin{bmatrix} 5 & 10 & 15 \\ 20 & 25 & 30 \\ 35 & 40 & 45 \end{bmatrix},$$

where DPN is decrypted data matrix.

By applying equations (4) and dk=5

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

TABLE 2. RB21 Encryption Algorithm

STEPS	RB21 ENCRYPTION ALGORITHM
1	To multiply the secret key in the matrix A. **A = ek.A Equation (1)** where A is matrix, ek is encryption key.
2	Identifying the prime numbers in the Matrix A.
3	$PN = (e^{k-1})(e^k) - 1$ **Equation (2)** where PN is perfect number, e is integer number, e>=2, and k is prime number from given Matrix A.
4	Number of perfect number are derived from step 3.
5	To merge all the perfect numbers into a single row.
6	To form a pair of numbers from left to right from Step 5.
7	Each and every pair should swapped cell values from given matrix.

TABLE 3. RB21 Decryption Algorithm

STEPS	RB21 DECRYPTION ALGORITHM
1	Identifying the prime numbers in the Matrix A.
2	$PN = (d^{k-1})(d^k) - 1$ **Equation (3)** where PN is perfect number, e is integer number, d>=2, and k is prime number from given Matrix A.
3	Number of perfect number are derived from step 2.
4	To merge all the perfect numbers into a single row.
5	To form a pair of numbers from right to left from Step 4.
6	Each and every pair should swapped cell values from given matrix.
7	To divide the secret key in the matrix A. **A = A/dk Equation (1)** where A is matrix, dk is decryption key.

5. Conclusion

Today's the security is very important to all the purposes in the world. For example, data need more security because personal data transaction, credit and debit card data transactions, machine learning algorithm prediction data.

(1) N round in RB21, 16 round in AES, and quarter round in Salsa;
(2) Time is high both RB21 and AES, and time is less in Salsa;
(3) Security is more high in RB21, Security is good in AES, and Security is less in Salsa;
(4) Prime number used in RB21 and no prime numbers used both AES and Salsa.

The proposed method provides high security because of prime perfecr numbers with secret key data while compared to both existing algorithms. In future, to add more operations for data security.

References

[1] Z. Shao, L. Ding: *Related-Cipher Attack on Salsa20*, Proc. Fou. Inter. Conf. on Comp. and Inf. Sci., **1** (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] P. Yadav, I. Gupta, S. K. Murthy: *Study and Analysis of eSTREAM Cipher Salsa And ChaCha*, Proc. Sec. IEEE Int. Con. on Eng. and Tec., 2016.

[4] L. Ding: *Improved Related-Cipher Attack on Salsa20 Stream Cipher*, IEEE Acc., **7** (2019), 30197–30202.

[5] D. J. Bernstein: *The Salsa20 Family of Stream Ciphers*, N. St. Ci. Des.: The eST. Fin., Lec. Not. in Com. Sc., M. Robshaw and O. Billet, eds., Berlin: Springer, 2008.

[6] 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.

[7] 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) (2015), 310–324.

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: rsaiilamaran@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail 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
E-mail address: ajithmohan845@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: sarkarshubham178@gmail.com

Department of Computer Science and Engineering
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation
Chennai, Tamil Nadu, India
E-mail address: jeswinmts9947@gmail.com