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

Predicting The Data For Security Using Rjb23 Algorithm

R.Jaichandran[1], Dr. Avinash Sharma[2], K.L.Shunmuganathan[3],Rebin Baby[4],ArjunKs[5],and Anil Das[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]klsnathan@avit.ac.in, [4]rebinbab33@gmail.com,
[5]anju56365636@gmail.com, [6]anilkanjikulam@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 current world is information world; without this information can't make due in present stage. This information created more from web- based media; this media information is public information; This public information did not have well security; so we applying the proposed method and it has 3 steps; 1. Using prime numbers in quadratic equations; 2. Prime and non-negative integer number used to swap the numbers; 3. Column operations execution; The new method gives well security when contrast to Salsa method.

Keywords: RJB23, Prime, Salsa, Encryption, Decryption.

1. INTRODUCTION

The current world is information world; without this information can't make due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so to conquer this matter we apply the Salsa strategy. This strategy effectively hack the information from the programmers. 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 give security for data [6]. SRB21 method used to give security for data [7]. CBB21 method used to provide security for data [8].CBB22 method used to provide security for data[9].Introduced the new method RJB23(Rajaprakash Jaichandran and Bagath Basha) 23 for this

problem.

2. METHODS

- RJB23 security method are discuss in Table 1 and Table2.

3. ENCRYPTION

- "EM is a analyzed matrix. [10]"

"Equation (1)"

"p=2,q=3,
r=7""EM=36855654"
"Pairs (3, 6), (8, 5), (5, 6) and (5, 4)."

"Pair-1(3, 6)"

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

"Pair-2(8, 5)"

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

"Pair-3(5, 6)"

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

"Pair-4(5, 4)"

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

"Equation (2): E^n* M"

"EB = 9 is3,3"

"EB=3 is 3, 9"

"Pairs (3,3), (3,9)"

Pair-1(3,3)

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

Pair-2(3,9)

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

"Equation (3)"

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

TABLE 1. RJB23 Secure Encryption

STEPS	RJB23 SECURE ENCRYPTION
i	"The data analyzed from social data".
ii	"The data will form a matrix".
iii	"$EM = (-p \pm \sqrt{(p^2)} - 4qr)/2q$.whereEMisencryptedmatrix"**(1)**
iv	" To form a single row for merged numbers".
v	"To form a pair from left to right from Step 4".
vi	"All pair could be swapped cell values from given matrix".
vii	"EB=E^n * M**(2)** where EB is encryption matrix B."
viii	"Identify the prime values multiply by the M for order of matrix".
ix	"E and M will swap in a matrix EB".
x	"$CA = C_i <-> (C_{i+(s-t)})$ **(3)** where CA is Column encrypted matrix "

TABLE 2. RBJ23 Secure Decryption

STEPS	RJB23 SECURE DECRYPTION
i	"$CA = C_i <-> (C_{i+(s-t)})$ **(4)** where CA is Column decrypted matrix"
ii	"To analyse theprime in the given matrix".
iii	"DM1=D^n * M**(5)** where DM1 is decryption matrix 1."
iv	"$DM2 = (-p \pm \sqrt{(p^2)} - 4qr)/2a$.whereDM2isdecryptedmatrix2"**(6)**
v	"To form a single row for merged numbers".

vi	"To form a pair from right to left from Step 5".
vii	"All pair could be swapped cell values from given matrix".

4. DECRYPTION

"Equation (4)"

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

"Equation (5)": $DM\ 1 = D^{n}$*** M**

"DM1 = 9 is 3, 3"

"DM1= 3 is 9,3"

Pairs (9,3),(3,3)

Pair-1(9,3)

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

Pair-2(3,3)

$$DM1=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

"Equation (6)"

"p=2,q=3, r=7"

"$DM2 = (-3 \pm \sqrt{}(32) - 4 * 2 * 7)/2 * 2$"

"$DM12=(-3 \pm \sqrt{}9 - 56)/4$"

"$DM2 = (-3 \pm \sqrt{}47)/4$"

"$DM2 = (-3 \pm 6.85565)/4$"

"DM2 = 36855654."

"Pair of numbers (4, 5), (6, 5), (5, 8), and (6, 3)."

"Pair-1(4, 5)"

$$DM2=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 105\\ 108 & 110 & 102\end{pmatrix}$$

"Pair-2(6, 5)"

$$DM2=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 108\\ 105 & 110 & 102\end{pmatrix}$$

"Pair-3(5, 8)"

$$DM2=\begin{pmatrix}102 & 103 & 104\\ 106 & 105 & 102\\ 105 & 110 & 108\end{pmatrix}$$

“Pair-4(6, 3)"

$$DM2=\begin{pmatrix}102 & 103 & 104\\ 105 & 105 & 102\\ 106 & 110 & 108\end{pmatrix}$$

5. CONCLUSION

The current world is information world; without this information can’t make due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so we apply the RJB23 method and it has 3 steps; 1. Using prime numbers in quadratic equations; 2. Prime numbers and non-negative integer number used to swap the numbers; 3. Column operations execution; The RJB23 method gives well security when comparing to 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