Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 1865–1874
DOI : 10.47974/JDMSC-2363

Evolutionary multi-authentication cryptographic key implications for secure data access control

Sanjeev Kumar Mandal [@]
Ravleen Singh [†]
N. Chandu [§]
Deepak Mehta [‡]
Department of Computer Science & IT
Jain (Deemed-to-be University)
Bangalore 560069
Karnataka
India

Santosh Kumar Henge *
Deepthi Kothapeta [#]
Chanakya Kumar Hinge [$]
Department of Computer Science and Engineering
School of Computer Science and Artificial Intelligence
SR University
Warangal 506371
Telangana
India

Amit Sharma [^]
Department of Computer Application
School of Computer Application
Lovely Professional University
Jalandhar 144402
Punjab
India

[@] *E-mail:* sanjeev.mandal93@gmail.com
[†] *E-mail:* ravleen1234@gmail.com
[§] *E-mail:* chandunagesh2302@gmail.com
[‡] *E-mail:* deepak.mehta@jainuniversity.ac.in
* *E-mail:* hingesanthosh@gmail.com (Corresponding Author)
[#] *E-mail:* deepthivaishu18@gmail.com
[$] *E-mail:* hingechanakya7@gmail.com
[^] *E-mail:* amit.25076@lpu.co.in

Tarak Hussain [+]
Department of Artificial Intelligence & Data Science
Koneru Lakshmaiah Education Foundation
Vaddeswaram 520002
Andhra Pradesh
India

Abstract

Techniques for encryption at rest are essential for protecting data on these platforms against compromise. This research proposing evolutionary rotor machine based multi authentication cryptographic key implications for secure access control for secure data storage and logs. This research explores the operational and historical aspects of RMs, highlighting their use in safe communication during pivotal points in history. This research explores the operational and historical aspects of RMs, highlighting their use in safe communication during pivotal points in history. To strengthen data security in modern environments, a unique multilayer encryption technique is put forth that makes use of rotor machine concepts.

Subject Classification: *Primary 68M25, Secondary 68P25, 68P27.*

Keywords: *Cyber threats (CyTh), Rotor machine (RM), Ciphertext (CT), Cylinder 1/2/3 (C1/C2/C3), Plaintext (PT).*

1. Introduction

In the connected digital world of today, cryptography has developed into a vital defense against cyber attacks and unwanted access [1-3]. Only authorized end-user with decryption keys can right to employ sensitive data thanks to the skill of converting it into unintelligible ciphertext using cryptographic methods [4-6]. This invention greatly improved encryption, increasing its resistance to malevolent actors' interception. Notwithstanding these developments, data security [7] is still difficult, particularly in light of the widespread use of mobile devices and cloud computing [8-10]. The utilization of revolving rotors or cipher disks is the basic idea behind a rotor machine.

There are five sections to this research. Access control mechanism fundamentals, multi-authentication cryptography's important ramifications, and the intricacies of data security and privacy were covered in Section 1. The linked work, which conveys the study's context, is presented in Section 2. The suggested multi-authentication cryptographic

[+] *E-mail:* `tariqsheakh2000@gmail.com`

key implications for evolutionary rotor machine-based secure access control for secure logs and data storage are presented in Section 3. The analysis and results of the experiment are presented in Section 4, and recommendations for added research are presented in Section 5.

2. Related Work

The core of this paper is security. Cryptography is a key component in protecting private data from online attacks and illegal access in our digitally connected society. The core of cryptography is its capacity to apply intricate mathematical processes to transform private information into unintelligible CT [11], guaranteeing that only authorized users possessing decryption keys may access and decode the data [12–15]. In order to adequately address current data security concerns, The purpose of this review of the literature is to look into the operational difficulties and historical significance of rotor machines (RMs) in cryptography [16] [17].

Three encryption steps—fusion, substitution, and permutation—are proposed by the author, in which different combinations are considered [18]. To strengthen data security and prevent data hacking, the author recommended using multilayer linear feedback shift register (LFSR) cryptographic technology [19–21]. By combining symmetric and asymmetric key cryptography methods, the author proposed a multi-tiered system that would offer excellent availability, integrity, confidentiality, authentication, and scalability [22–26]. The author proposed a wrapper feature selection of the K-Nearest Neighbor classifier with binary Runge–Kutta optimization for information-guided communication to identify system intrusions [27][28].

3. Methodology

Important functionality to guard against purposeful and unintentional data compromise and change is provided by cryptographic techniques. Certain cryptographic techniques maintain communication secrecy by encrypting the message before sending it and decrypting it after it's received. Data content integrity and source authentication are provided by additional cryptographic techniques like digital signatures and message authentication codes [41]. Using the rotor machine methodology, a multilayer encryption method is developed in this study. Two levels of encryption, referred to as cylinders 1 and 2, are carried out, as illustrated

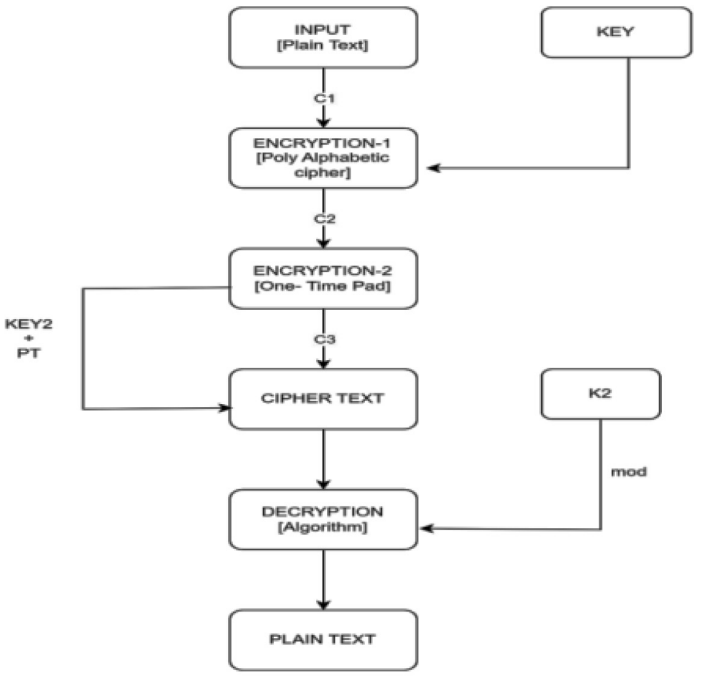

Figure 1

Multi-authentication cryptographic processed method

in Fig. 1. Two levels of encryption have been suggested in the suggested method: Key 2 (K2) is the new key created by applying a chosen key to a poly alphabetic cipher in the first encryption step. In the second encryption step, the new key is an equivalent fixed length of plain text.

4. Result and Discussion

The experimental scenarios framed with dual encryption based key mechanism which helps to security analyzers and systems to analyze malwares, cyber attacks and threads based on synchronized vulnerabilities using simulated port, protocols, cyber threats (CyTh), RM based cylinder 1/2/3 (C1/C2/C3). This experimented with the plain text of HELLO by including the key of CHAND.

4.1 *Encryption Process 1*

The first encryption method processed based two base level steps: As indicated in Figures 2 and 3, assign numerical values to each of the three

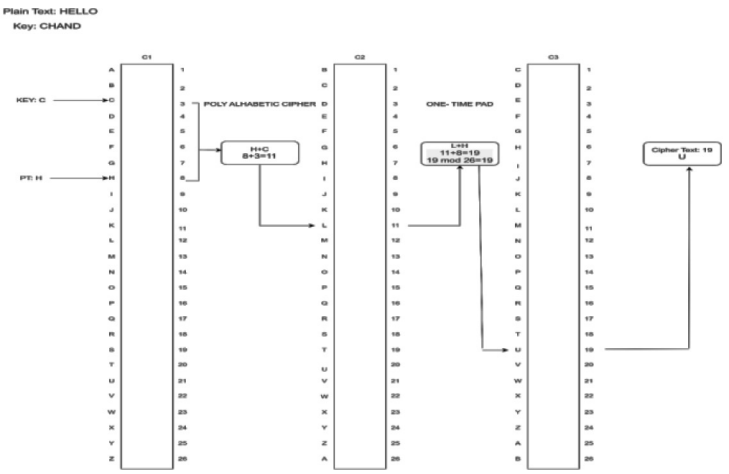

Figure 2

Evolutionary rotor machine based multi-authentication cryptographic key implications

cylinders' alphabetic letters. Then, use the poly alphabetic cipher to obtain the new key [K2].

4.1.1 Cylinders-3 (3C) based Numeric Value Allocation

As illustrated in Figure 3, assign numerical values to each of the three cylinders' alphabetic letters. First cylinders begin and finish with A–Z, 1–26; second cylinders begin and finish with B–A, 1–26; and third cylinders begin and finish with C–B, 1–26.

4.1.2 Allocation of Poly Alphabetic Cipher based Auto Mutated Key

To obtain the new key [K2], using the Poly alphabetic cipher.

Plain Text:	H	E	L	L	O
Key:	C	H	A	N	D

Formula: E + H = 5 + 8 = 13 = N; L + A = 12 + 1 = 13 = N; H + C = 8 + 3 = 11 = L
Key 2 [K2]: LNNAT; L + N = 12 + 14 = 26 = A; O + D = 15 + 4 = 19 = T

4.2 *Encryption Process 2*

The first encryption method processed based three base level steps: Apply the K2 + PT by using the modules function to obtain the cipher text; assign the alphabetic letters to the numerical values according to the

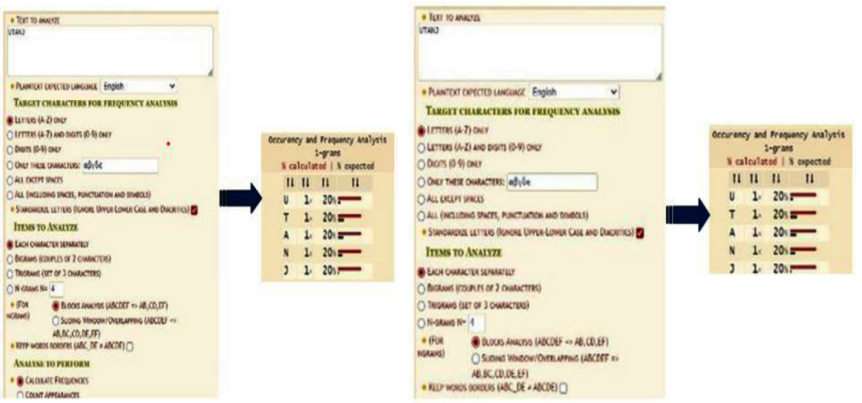

Figure 3

Security encryption based key computations and Security encryption based key frequency values

Cylinder 3 construction; and use the One-Time Pad process to obtain the cipher text. To obtain the encrypted text, the ONE-TIME PAD synced.

4.2.1 Integration of Second Secure Key and PT procedure

The generated CT wills furtherer added with the K2 + PT to obtain the ciphertext by using the modules function. K2: Key 2; PT: Plain Text; CT: Cipher Text.

Formula: N + E = 13 + 5 = 18 mod 26 = 18; N + L = 13 + 12 = 25 mod 26 = 25; A + L = 26 + 12 = 38 mod; L + H = 11 + 8 = 19 mod 26 = 19; T + O = 19 + 15 = 34 mod 26 = 8; 12 = 12

4.2.2 Allocation of Cylinder 3 (C3) alphabetic letters to the numeric principles

The alphabetic script is assigned to the numeric principles as per the Cylinder 3 formations. Therefore, final cipher text formed as CT: UTANJ

19	18	25	12	8
U	T	A	N	J

4.3 *Decryption Process*

CT:	U	T	A	N	J
K2:	L	N	N	A	T

Formula: J – T = 8 - 19 = -11+26 = 15 mod 26 = 15 = O; U – L = 19 - 11 = 8 mod 26 = 8 = H; T – N = 18 - 13 = 5 mod 26 = 5 = E; A – N = 25 - 13 = 12 mod 26 = 12 = L; N – A = 12 - 26 = -14 + 26 = 12 mod 26 = 12 = L

The final output text generated as the plain text: HELLO. This section described the experimental test case results and its concern discussions with the security strength of CT which used by the decoder mechanism. The test cases are analyzed based encryption based key computations and its frequency analysis which analyzed based on key frequency values. It suggests an alphabetic record of n-grams as statistically as shown in Fig.4. The study indicates that safe access control, secure data storage, and secure logging are significantly impacted by multi authentication cryptography based on evolving RMs.

5. Conclusion

The study suggests that multi authentication cryptography based on evolving RMs has important implications for safe access control, secure data storage, and secure logs. This work explores the operational and historical aspects of RMs, highlighting their function in protected communication throughout pivotal historical moments. In order to strengthen data security in modern settings, a unique multilayer encryption technique is put forth that makes use of rotor machine principles.

References

[1] Subiono, J. Cahyono, D. Adzkiya, and B. Davvaz, "A cryptographic algorithm using wavelet transforms over max-plus algebra," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 3 (2022), doi: 10.1016/j.jksuci.2020.02.004.

[2] Z. Hu, B. Liu, X. Ren, and Y. Tang, "Analysis and Implementation of the Enigma Machine," in Proceedings - 2022 International Conference on Big Data, *Information and Computer Network*, BDICN 2022 (2022). doi: 10.1109/BDICN55575.2022.00093.

[3] S. Kepley, D. Russo, and R. Steinwandt, "Cryptanalysis of a modern rotor machine in a multicast setting," *Cryptologia*, vol. 40, no. 6 (2016), doi: 10.1080/01611194.2015.1115443.

[4] D. Nadarajan and T. PramanandaPerumal, "Elliptic Curve Cryptography Encryption Framework for Ensuring Security in Open Social Networks," *Scand. J. Inf. Syst.*, vol. 35, no. 1 (2023).

[5] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms," *Electron.*, vol. 11, no. 19 (2022), doi: 10.3390/electronics11193156.

[6] V. Esther Jyothi, B. D. C. N. Prasad, and R. K. Mojjada, "Analysis of Cryptography Encryption for Network Security," in IOP Conference Series: Materials Science and Engineering (2020). doi: 10.1088/1757-899X/981/2/022028.

[7] R. Adee and H. Mouratidis, "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography," *Sensors*, vol. 22, no. 3 (2022), doi: 10.3390/s22031109.

[8] M. A. A. Pujari and M. S. S. Shinde, "Data Security using Cryptography and Steganography," *IOSR J. Comput. Eng.*, vol. 18, no. 04 (2016), doi: 10.9790/0661-180405130139.

[9] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *Int. J. Comput. Sci. Mob. Comput.*, vol. 13, no. 1 (2024), doi: 10.47760/ijcsmc.2024.v13i01.007.

[10] C. Mascia, M. Sala, and I. Villa, "A SURVEY ON FUNCTIONAL ENCRYPTION," *Adv. Math. Commun.*, vol. 17, no. 5 (2023), doi: 10.3934/amc.2021049.

[11] X. Chang, A. Yan, and H. Zhang, "Ciphertext-only attack on optical scanning"

[12] Prakash, F., Gupta, S., & Goswami, G. Feature Extraction Using Canonical Correlation Analysis for Improved Recognition of Objects in Hyper Spectral Data. In 2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC), Debre Tabor, Ethiopia (pp. 1-6) (2024). doi: 10.1109/ICOCWC60930.2024.10470883.

[13] Mandal, Sanjeev Kumar, A. R. Deepti, Lalit Kumar, and M. N. Nachappa. "An Improvised Caesar Cipher Technique for Enhancing Data Security." *International Journal of Advanced Research in Engineering and Technology* 11(11), pp. 1304-1313 (2020).

[14] A. Varshney, K. Suneetha, and D. K. Yadav, "Analyzing the Performance of Different Compactor Techniques in Data Compression & Source Coding," 2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC), Debre Tabor, Ethiopia, p. 1-6 (2024), doi: 10.1109/ICOCWC60930.2024.10470923

[15] Gulati, Sagar, Bhatia, K., P. K. Yadav, "Reliability Optimization for Distributed Systems through Task Clustering', In Proc. Of 5th International Conference on Advance Computing and Communication Technologies, pp. 176-182 (2015), DOI: 10.1109/ACCT.2015.78 IEEE Xplore.

[16] Friedrich L. Bauer, 14 - Rotor machines and bombes, The History of Information Security, Editor(s): Karl De Leeuw, Jan Bergstra, Elsevier Science B.V., Pages 381-446 (2007), https://doi.org/10.1016/B978-044451608-4/50015-8.

[17] He, Yifeng, Ye, Nan, Zhang, Rui, Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication Security, *Wireless Communications and Mobile Computing*, 2295130, 19 pages (2021). https://doi.org/10.1155/2021/2295130

[18] Abdallah, H.A.; Meshoul, S. A Multilayered Audio Signal Encryption Approach for Secure Voice Communication. Electronics, 12, 2 (2023). https://doi.org/10.3390/electronics12010002

[19] A. A. Raj, A. Beno and R. Jaisakthi, "Security Enhancement of Information using Multilayered Cryptographic Algorithm," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, pp. 348-353 (2020), doi: 10.1109/ICOEI48184.2020.9143052.

[20] Santosh Kumar Henge, Gitanjali Jayaraman, M Sreedevi, R Rajakumar, Mamoon Rashid, Sultan S. Alshamrani, Mrim M. Alnfiai, Ahmed Saeed AlGhamdi. Secure keys data distribution based user-storage-transit server authentication process model using mathematical postquantum cryptography methodology[J]. *Networks and Heterogeneous Media*, 18(3): 1313-1334 (2023). doi: 10.3934/nhm.2023057

[21] Fauziyah, Zhaoshun Wang, Mujahid Tabassum, A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security, Computers, Materials & Continua, Vol. 78, No. 3, pp. 4417-4452 (2024), http://www.techscience.com/cmc/v78n3/55899.

[22] D. Upadhyay, M. Zaman, R. Joshi and S. Sampalli, "An Efficient Key Management and Multi-Layered Security Framework for SCADA Systems," in *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 642-660 (March 2022), doi: 10.1109/TNSM.2021.3104531.

[23] Mahjabeen Tahir, Azizol Abdullah, Nur Izura Udzir, Khairul Azhar Kasmiran, A novel approach for handling missing data to enhance network intrusion detection system, Cyber Security and Applica-

tions, 100063, ISSN 2772-9184 (2024), https://doi.org/10.1016/j.csa.2024.100063.

[24] Pooja Dhiman, Santosh Kumar Henge, Sartaj Singh, Avinash Kaur, Parminder Singh,3, Mustapha Hadabo, Blockchain Merkle-Tree Ethereum Approach in Enterprise Multitenant Cloud Environment, Computers, Materials & Continua, Vol. 74, No. 2, pp. 3297-3313 (2023), http://www.techscience.com/cmc/v74n2/50215.

[25] Xu, W., Li, X., Su, Y. et al. Verifiable privacy-preserving cox regression from multi-key fully homomorphic encryption. Peer-to-Peer Netw. Appl. (2024). https://doi.org/10.1007/s12083-024-01740-9

[26] Santosh Kumar Henge, Pooja Dhiman; Integrating of rule based secure parameters for analysing third-party applications and libraries in cross platform development. AIP Conf. Proc. 8 September 2023; 2800 (1): 020074. https://doi.org/10.1063/5.0167752.

[27] Yuan, L., Tian, X., Yuan, J. et al. Enhancing network security with information-guided-enhanced Runge Kutta feature selection for intrusion detection. *Cluster Comput* (2024). https://doi.org/10.1007/s10586-024-04544-x

[28] Data in Transit, https://www.imperva.com/learn/data-security/data-in-transit/ (Accessed on 4th July 2024).

Received November, 2024