International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Novel Approach for Encryption using Catalan Numbers

V. Uma Karuna Devi Kakarla*[1], Dr. CH. Suneetha[2]

Submitted: 07/05/2023 **Revised**: 17/07/2023 **Accepted**: 08/08/2023

Abstract*:* In today's fast-changing digital world, passwords or PIN numbers are needed for everything from financial transactions to confidential correspondence. This practice protects monitory exchanges, financial processes, and secret communications. Sharing a complex PIN or one-time password has emerged to strengthen this security paradigm and protect critical interactions. The Crypto Council for Innovation (CCI) has developed a complete PIN security architecture to improve security. This method relies on encrypted symmetric keys integrated into complex key block architectures. These structures include cautious key usage limits, strengthening the security system. These key blocks avoid the presumption that previously established keys can be reused, promoting dynamic key management and increased security. At the vanguard of these security advances, this research paper painstakingly explains password and PIN encryption and migration. This unique and stable secure communications system uses Catalan number sequences' mathematical elegance. This novel method presents the recipient of encrypted communication with a lengthy, seemingly random sentence that contains the encrypted password or PIN. This encrypted payload is discretely dispersed throughout the text, making its identification and extraction difficult for malevolent actors. Importantly, both the sender and the recipient are blissfully unaware of the PIN characters' precise positions, adding ambiguity that prevents illegal access. In conclusion, the digital landscape requires strong security to protect financial, secret, and covert transactions. Encrypted symmetric keys in dynamic key block structures, certified by the Crypto Council for Innovation, demonstrate a strong commitment to security. The encryption and migration method, which uses Catalan number sequences to hide passwords and PINs, shows the relentless search of impenetrable security in an increasingly linked world.

Keywords: *Encryption, Polygon triangulation, Decryption Catalan Number, Secure Communication.*

1. Introduction

In order to confirm financial transactions, OTPs are delivered to mobile phones and are intended to be very secure due to the COVID epidemic. The password or PIN can be easily broken in a communication device because of its modest size. Digital or virtual money known as "cryptocurrency" uses cryptography to protect transactions. It is constantly growing and operates on a block chain where peers swap money using digital wallets. We require a password for the transaction. The process of mining produces cryptocurrency units. Although it is a common authentication mechanism, text-based and numerical-based passwords or PINs have communication issues. Due to memorability and reuse difficulties brought on by the very short length of a password or PIN, it is vulnerable to dictionary attacks. In Client/Server systems, it can also be challenging to move a user's PIN or password from one source to another. The server's directory is a secure location where passwords and PINs can be kept and sent over the internet. Additionally, unauthorized access to user passwords or PINs that are saved on the server can be prevented. A Catalan number sequence and a polygon triangulation approach are used in the current study to describe the password or PIN encryption and migration process from one source to another. A random text message received over a public channel occasionally has a doubly encrypted password or PIN attached to it. Only legitimate users and servers can access the encrypted mechanism. The users' shared secret keys (Decimal numbers) are used to place the encrypted password or PIN characters in those specific spots.

[1]*Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India.*
[2]*Associate Professor, Department of Mathematics, GITAM University, Visakhapatnam, India.*
** Corresponding Author Email: ukakarla@gitam.edu*

1.1. Catalan Numbers

C_N stands for the Catalan number, which is a collection of natural numbers.

It is given as

$$C_N = \frac{2n!}{(n-1)!n!} = \frac{1}{n+1}\binom{2n}{n} \quad (1)$$

The table 1 shows first ten Catalan number values.

Table 1: First ten Catalan number values

N	C_N
1	1
2	2
3	5
4	14
5	24

6	132
7	429
8	1430
9	4862
10	1676

For N=18, Catalan number CN = 477638700

Euler's triangulation problem can be used to define Catalan number as

$C_0 = 1, \qquad C_1 = 1C_n = \frac{4n-2}{n+1} C_{n-1} \qquad n>2$ (2)

1.2. Ubiquitous Nature of Catalan Numbers

There are many instances of the Fibonacci, Lucas, and Catalan numbers. Among the many combinatorial uses of Catalan sequences are the parenthesizing issue, binary tree construction, counting the number of Dyck pathways over mountain ranges, abstract algebra, and sports. There are many cryptographic uses for polygon triangulation and Catalan numbers [2, 3, 8]. They have been employed to develop encryption algorithms and key generation methods throughout the history of cryptography.

1.3. Polygon Triangulation

The phrase "polygon triangulation" in computational geometry describes the division of a polygon into triangles with non-intersecting diagonals. Drawing the diagonals between nonadjacent vertices is all that is required to triangulate a complex polygon.

There are many uses for it in curved geometry, as well as difficulties with 3D object representations in art galleries, computer graphics, and CAD systems, to name a few. Many combinatorial puzzles can be solved using the Catalan number, a sequence of numbers. Catalan numbers are found using the problem of polygon triangulation. You can divide a convex polygon into (n-2) triangles. The quantity TN of triangles with n-angles is used to connect the polygon triangulation to the Catalan number.

$T_N = C_{N-2} \qquad \text{for} \qquad n>2$ (3)

$T_N = \frac{1}{n-2}\binom{2n-4}{n-2} = \frac{(2n-4)!}{(n-2!(n-2)!}$ (4)

In order to triangulate a polygon, it must first be divided into trapezoids, which are then divided into monotone polygons, and triangles, which are then formed from the monotone polygons. Known as Seidel's Algorithm, this formula. One millisecond is needed to create a polygon with 10 vertices, three milliseconds for one with 50 vertices, and six milliseconds for one with 100 vertices. A polygon with 1 gb of vertices must therefore be rendered in 97.6 milliseconds.

2. Literature Survey

Mackie and colleagues [1] proposed a novel approach to enhance password security and improve user memorability. Their technique aimed to incentivize users to create stronger passwords. In their study, the user cohort was divided into two distinct groups within the chapter. To devise their strategy, Mackie et al. employed an empirical formula, leveraging empirical data to formulate their approach for bolstering password practices.

Shay et al. [2] underscored that users possess a restricted understanding when it comes to crafting resilient passwords, pointing out that the intricacies of creating strong password combinations remain largely unfamiliar to them.

In their comprehensive study, Florencio et al. [3] delved into the habitual usage patterns of users concerning the number of accounts that necessitate password access within a given day.

Perrig and colleagues [4] put forth a well-considered and suitable method aimed at enhancing key agreement protocols that rely on binary tree structures to establish varying levels of security.

In her doctoral dissertation, Swetha Mishra and her collaborators [5] meticulously outlined a comprehensive research endeavor focused on password-based authentication. The crux of her thesis revolved around the conceptualization and development of an innovative password hashing technique. Additionally, she conducted an extensive review and analysis of prevailing password systems to provide a thorough understanding of the existing landscape in the realm of authentication mechanisms.

Within the scholarly work authored by Katha Chanda and her co-researchers [6], an in-depth exploration into the realms of security analysis and password robustness was undertaken. This chapter served as a platform for the meticulous execution of multiple empirical experiments, each meticulously designed to scrutinize the resilience of passwords when subjected to the formidable challenges posed by brute force attacks. The investigation was driven by a rigorous desire to understand the intricate dynamics that underlie the strength and vulnerability of passwords in the face of determined assailants.

D. Sravana Kumar and his collaborators embarked on an ambitious research endeavor, as detailed in their scholarly contribution [7], wherein they formulated an innovative cryptographic framework. This framework harnessed the power of elliptic curve cryptography within the domain of finite fields, serving as the foundational architecture for a novel approach to password encryption. Their comprehensive work sought to bridge the realms of

advanced mathematics and practical cybersecurity applications, paving the way for enhanced security measures in the encryption of passwords.

In a thought-provoking and forward-looking study, Saracevic and his team of researchers [8] introduced a multifaceted exploration into the integration of the triangulation approach within the intricate domain of biometric identification. With a meticulous and comprehensive approach, their work outlined diverse potential applications where triangulation could be harnessed to enhance the accuracy, reliability, and efficiency of biometric identification processes. By delving into this innovative avenue, the researchers sought to not only advance the theoretical underpinnings of biometric authentication but also to forge new paths for practical implementation that could yield significant strides in the realm of identity verification and security.

In a pioneering study that showcased remarkable ingenuity, Amounas and his collaborators [9] ventured into the uncharted territory of cryptography, devising innovative encryption techniques rooted in the mathematical elegance of Catalan numbers. Through an intricate and comprehensive exploration, their research culminated in the creation of a series of encryption methods that harnessed the unique properties of Catalan numbers. These methods, with their foundation firmly rooted in mathematical theory, sought to usher in a new era of cryptographic practices, potentially revolutionizing the landscape of data protection and security by marrying the intricate world of numbers with the imperatives of modern-day information safeguarding.

In an intellectually stimulating and expansive scholarly inquiry, Higgins P.M. and a team of fellow researchers [10] embarked on a captivating journey to delve into the intricate origins and multifaceted applications of a diverse array of numerical constructs. Their meticulous investigation traversed the annals of mathematical history, unraveling the enigmatic origins of various types of numbers, while simultaneously shedding light on the remarkable spectrum of contexts in which these numerical entities find utility. Through an intricate tapestry of research, analysis, and synthesis, their work not only enriched our understanding of the fundamental nature of numbers but also illuminated the profound impact these numerical entities wield across an extensive spectrum of disciplines and endeavors.

In a scholarly expedition characterized by its depth and intellectual acumen, Horak and his esteemed colleagues [11] embarked on a trailblazing odyssey, advocating for the strategic integration of combinatorial techniques within the realm of cryptography. Within the pages of their meticulously crafted paper, the researchers channeled their energies toward a specific focal point - the intricate and intriguing MaxMinMax problem. This captivating exploration extended its reach across the intricate tapestry of both finite and infinite fields, as they unveiled a trove of results that stood as testament to the power and versatility of their combinatorial approach. Through the discerning lens of their analysis, the paper not only resonated as a significant contribution to the cryptography domain but also resonated as a beacon guiding researchers toward innovative ways of approaching complex mathematical challenges within the sphere of data security and protection.

In a scholarly endeavor that emanated depth and intellectual rigor, Koscielny and the collective expertise of their co-authors [12] unfurled a visionary proposal, laying the cornerstone for what they termed "Applied Research and Theoretical Foundations." This chapter, a testament to their scholarly acumen, embarked on an expansive voyage through the intricate landscape of fundamental mathematical underpinnings. Delving into the very bedrock of modern cryptographic advancements, the authors meticulously explored a myriad of indispensable mathematical concepts. These concepts, intricately woven into the fabric of cryptographic evolution, assumed a pivotal role in elucidating the mechanisms underpinning the development of cutting-edge cryptographic algorithms and protocols. Through their painstaking examination, the chapter not only crystallized the essence of these mathematical tenets but also charted a compelling path toward comprehending the intricate dance between theory and practice in the dynamic realm of data security and encryption.

3. Proposed Scheme

One-time password (OTP) transmission in Client/Server applications is a perfect fit for the current password or PIN encryption and migration technique. The method takes use of the Catalan number system and polygonal triangulation processes.

Two authorized users must first concur to use a natural number, n, as a secret key in order to encrypt and migrate an encrypted password or PIN. A large number with multiple non-trivial factors is preferred for this value. If they are sending a tiny secret code, PIN, or password that will be used in subsequent communications, then this is the situation. Take the non-trivial factors of 36, for instance, which total six. 2,3,4,6,9,12.

n1, n2, n3, and n4 should be considered for those components. Additionally, the sender chooses at random a text whose length is greater than or equal to the largest factor [decimal number] of the mutually agreed-upon composite number.

3.1. Encryption

1. Decimal digits N_1, N_2, N_3, and N_4 are four composite numbers.
2. Create a series of Catalan numbers, such as CN_1, CN_2, CN_3, CN_4, and Polygon Triangulation numbers, such as TN_1, TN_2, TN_3, TN_4, for the cons N_1, N_2, N_3, and N_4.
3. Adjust a series of Catalan numbers CN_1, CN_2, CN_3, CN_4 to mod 256 by using the formula
   i. Adjusted CN $ACN_i = CN_i \pmod{256}$ for i=1,2,3,4
4. Adjust a sequence of Polygon Triangulation numbers TN_1, TN_2, TN_3, TN_4 to mod 7
5. by using the formula
   i. Adjusted TN $ATN_i = TN_i \pmod 7$ for i=1,2,3,4
6. Choose four decimal digit Password say P_1, P_2, P_3 and P_4.
7. Convert each decimal numeral P_i in the Password into its equivalent 8-bit ASCII binary and then rotate right by ATN_i times to get P_iR.
8. Apply Logical Exclusive-OR operation on P_iR and ACN_i to get binary coded encrypted password cipher character BC_i.
   i. $BC_i = P_iR \oplus ACN_i$ for i= 1, 2, 3, 4.
9. Generate encrypted Password character by converting each BC_i into its equivalent symbol.
10. Consider a random text whose size must be greater than equal to the maximum value of considered Composite numbers (>=Max(N_1, N_2, N_3,N_4)).
11. Insert the encrypted Password characters in the random text at positions specified by N_1, N_2, N_3, N_4.

3.2. Decryption Operation

Decryption is the reverse operation of encryption because it is a symmetric cipher. The user at destination selects the encrypted characters of password characters from their places (which are known to both the authenticated parties) after receiving the huge random text. On each character, the reverse logical XOR operation is used.

$$P_iR=P_iC \oplus ACN_i \text{ for } i = 1,2,3,4$$

After that, apply rotate left operation on generated 8-bit binary to obtain the P_i. First character of a password is its corresponding ASCII character.

$$\mathbf{[P_1R, LR(k)] \longleftarrow P_1}$$

4. Performance Study of the Algorithm

One-time passwords (OTPs) are effectively sent to client transactions and used to withdraw cash from ATMs using the present manner of password encryption and insertion in client/server systems. The central server stores composite numbers with at least four components. The power and capability of the central server to provide information to workstations allow for the storage of a large number of composite numbers with at least four components.

The client must initially register for the activation of their application server and install the server application. At the moment of activation, the central server saves the login information of the clients and distributes random composite numbers, allowing the clients to select one of them with at least four non-trivial components for subsequent bank transactions. Every time a client wants to conduct a transaction with the bank, they ask that the application server send an OTP request to the central server. A central server authenticates the client's identity, creates a four-digit OTP, and encrypts the data using the composite number given to the client during registration. At locations N1, N2, N3, and N4, the encrypted OTP is added. The client's application server finds the location of the numerical characters in the encrypted OTP, decrypts them, and then provides the OTP for the transaction. The server application is where the decryption operation is carried out.

4.1. Example

Consider four Composite numbers (N1, N2, N3, N4) = (12, 15, 18, 24)

Four digit Password (P1 P2 P3 P4) = (1 9 6 8)

Generation of sequence of Catalan numbers CNi and Polygon Triangulation number TN_i.

N_i, for i = 1 to 4	N_1 = 12	N_2 = 15	N_3 = 18	N_4 = 24
CN_i	208012	9694845	477638700	1289904147324
TN_i	16796	742900	35357670	91482563640
$ACN_i = CN_i \pmod{256}$	140	125	44	124
$ATN_i = TN_i \pmod 7$	3	4	5	6

Generation of Encrypted Password.

P_i, for i = 1 to 4	P_1 = 1	P_2 = 9	P_3 = 6	P_4 = 8
8-bit Binequ of P_i	00000001	00001001	00000110	00001000

ATN_i	3	4	5	6
$P_iR=[M_i, RR(ATn_i)]$	00100000	10010000	00110000	00100000
8-bit Binequ of ACN_i	10001100	01111101	00101100	01111100
$P_iR \oplus ACN_i$	10101100	11101101	00011100	01011100
Symbol	¼	Ý	FS	\

Size of Random text size >= Max(N_1, N_2, N_3, N_4) =Max(12, 15, 18, 24) = 24

Random Text = SAI PRANEETH AND RONITH ARE BROTHERS

Encrypted password characters (**¼,Ý, FS,** \ )

Insert Encrypted characters in random text at positions (12, 15, 18, 24).

Input text: SAI PRANEETH AND RONITH ARE BROTHERS

Encrypted output text: SAI PRANEET¼ A **Ý**D **FS**ONITH\ ARE BROTHERS.

5. Conclusion

As a result of the password or PIN being a relatively tiny amount of text characters, numbers, or special characters, the major security concerns in password or PIN communication mechanisms arise. It can be readily broken and tampered with because to its small size, which isn't a significant concern. An indirect PIN entering method is safer and more secure since it prevents misuse and unwanted third-party involvement in transactions. Shoulder surfing is a common method of tracking and stealing PIN when a consumer withdraws money from ATM machines. Information being sent is kept secure and intact using covert password or PIN forms.The password, or PIN, as it is now constructed, is twice encrypted, placed throughout with random text, and delivered through an insecure channel. On how to encrypt data and where to put encrypted characters, the parties concur. The only shared secret key is a composite number named "N," which prevents key compromise. A Catalan number sequence and a polygon triangulation sequence are used to encrypt the initial few characters of a password or PIN. A man-in-the-middle attack is quite unlikely in this situation because the adversary is unaware of the password or PIN positions. The locations are compromised in all cases, and the characters are hidden. This technology was therefore developed in a secure manner in all respects.

References

[1] Yildirim. M and Mackie. I, “Encouraging users to improve password security and memorability”, International Journal of Information Security (2019), ISSN 1615-5262, https://doi.org/10.1007/s10207-019-00429-y.

[2] Shay et-al, “Encountering Stronger Password Requirements: User Attitudes and Behaviors”, Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA USA.

[3] Florencio, D. et-al, “A large-scale study of web password habits”,International Conference on World Wide Web, WWW 2007, Banff, Alberta, Canada, May 8-12, 2007, DOI:10.1145/1242572.1242661.

[4] Perrig et-al, “Tree-based Group Key Agreement”, ACM Transactions on Information and System Security 7(1), February 2002, DOI:10.1145/984334.984337.

[5] Sweta Mishra, the thesis titled “Design and Analysis of Password-based Authentication Systems” Indraprastha Institute of Information Technology, Delhi, 2017.

[6] Katha Chanda,”Password Security: An Analysis of Password Strengths and Vulnerabilities” International Journal of Computer Network and Information Security, 2016, 7, 23-30 Published Online July 2016 in MECS, DOI: 10.5815/ijcnis.2016.07.04

[7] D. Sravana Kumar, C. H. Suneetha, and P. Sirisha. "New password embedding technique using elliptic curve over finite field",

http://doi.org/10.1007/978-981-13-6001-5_15

[8] Saracevic, Muzafer, Mohamed Elhoseny, AybeyanSelimi, and Zoran Lončeravič. "Possibilities of applying the triangulation method in the biometric identification process."

[9] Amounas F., El-Kinani E.H., Hajar M.: “Novel Encryption Schemes Based on Catalan Numbers”, International Journal of Information and Network Security, vol. 2(4), pp. 339-347, 2013.

[10] Higgins P.M.: “Number Story: From Counting to Cryptography”, Springer Science and Business Media, Berlin, Germany, 2008.

[11] Horak P., Semaev I., Tuza I.Z.: “An application of Combinatorics in Cryptography”, Electronic Notes in Discrete Mathematics, vol. 49, pp. 31-35, 2015.

[12] Koscielny C., Kurkowski M., Srebrny M.: "Modern Cryptography Primer: Theoretical Foundations and Practical Applications", Springer Science and Business Media, Berlin, Germany, 2013.

[13] Mohan, B. R. ., M, D. ., Bhuria, V. ., Gadde, S. S. ., M, K. ., & N, A. P. . (2023). Potable Water Identification with Machine Learning: An Exploration of Water Quality Parameters. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 178–185. https://doi.org/10.17762/ijritcc.v11i3.6333

[14] Carmen Rodriguez, Predictive Analytics for Disease Outbreak Prediction and Prevention , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[15] Beemkumar, N., Gupta, S., Bhardwaj, S., Dhabliya, D., Rai, M., Pandey, J.K., Gupta, A. Activity recognition and IoT-based analysis using time series and CNN (2023) Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, pp. 350-364.