Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.9854886

USE OF CATALANNUMBER SEQUENCE AND POLYGON TRIANGULATION FOR PASSWORD OR PIN ENCRYPTION AND MIGRATION

V. Uma Karuna Devi Kakarla[1] , Dr. CH. Suneetha[2] , Dr. Naga Madhavi Latha Kakarla[3]

1. Research Scholar, Department of Mathematics, GITAM University, Visakhapatnam, India
ukakarla@gitam.in
2. Associate Professor, Department of Mathematics, GITAM University, Visakhapatnam, India
schivuku@gitam.edu
3. Associate Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India
madhavilathakakarla@sircrrengg.ac.in

Abstract: In today's world, using a user password or PIN number is required for any monitory, financial, and secret communication transactions. The possible increase in security is increased by sharing a strong PIN or one-time password. As encrypted symmetric keys in key block structures with usage limits on protected keys, the Crypto Council for Innovation (CCI) is establishing a number of PIN security standards. These key blocks don't assume that previously established keys can be used again. The encryption and migration method for passwords or PINs is described in the current paper using Catalan number sequences. In this case, the recipient receives a long, random text that contains the encrypted password or PIN inserted at various points throughout. The sender and the receiver are unaware of the placements of the inputted PIN characters.

Key words*:* Encryption, Polygon triangulation, Decryption Catalan Number

I. 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 "crypto currency" 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.

Catalan Numbers:

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

It is given as

$$C_N = \frac{2n!}{(n-1)!n!} = \frac{1}{n+1}\binom{2n}{n} n \geq 0 \quad \text{..... (i)}$$

The table 1 shows first ten Catalan number values.

Table 1**:** First ten Catalan number values

N	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
C_N	**1**	**2**	**5**	**14**	**42**	**132**	**429**	**1430**	**4862**	**16796**

For N=18, Catalan number C_N = 477638700

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

$$C_0 = 1, C_1=1 \quad C_n = \frac{4n-2}{n+1} C_{n-1} \quad n\geq 2 \text{.....} \quad \text{(ii)}$$

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.

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 T_N of triangles with n-angles is used to connect the polygon triangulation to the Catalan number.

$T_N = C_{(N-2)}$, for N > 2…….(iii)

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

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.

LITERATURE SURVEY

- Mackie et-al. [1] suggested a technique for password security and memorability to encourage users. The entire user group was separated into two groups in that chapter, and an empiric formula was used.
- Shay et-al. [2] creation of strong passwords is not well known by users.
- Florencio, D. et al. [3] investigated the typical number of password-required accounts a user accesses in a day.
- Perrig et al. [4] proposed an appropriate approach for key agreement protocols that use binary trees for security levels.
- Mishra, Swetha, et al. [5] her PhD thesis contained a design for a study of password-based authentication. She developed a technique for hashing passwords and reviewed existing password systems in her thesis.
- Katha Chanda et al. [6] looked at security analysis and password strength. In that chapter, the author conducted numerous experiments to evaluate the password's resistance to brute force attacks.
- D. Sravana Kumar et al. [7] created elliptic curve cryptography over a finite fields-based password encryption approach.
- Saracevic et al. [8] proposed applications for the triangulation approach in the biometric identification process.
- Amounas et al. [9] developed novel encryption methods based on Catalan numbers.
- Higgins P.M. et al. [10] explored the origins and uses of several sorts of numbers.
- Horak P et-al. [11] recommended employing combinatorics in cryptography. In that paper, they mainly focused on the MaxMinMax problem and offered results for both finite and infinite fields.
- Koscielny C et-al. [12] proposed Applied Research and Theoretical Foundations. That chapter covered a number of fundamental mathematical concepts that are crucial to understanding the development of modern cryptographic algorithms and protocols.

II. 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.

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

   Adjusted CN $ACN_i = CN_i \pmod{256}$ for i=1,2,3,4

   Adjust a sequence of Polygon Triangulation numbers TN_1, TN_2, TN_3, TN_4 to mod 7 by using the formula

   Adjusted TN $ATN_i = TN_i \pmod{7}$ for i=1,2,3,4

4. Choose four decimal digit Password say P_1, P_2, P_3 and P_4.
5. 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.
6. Apply Logical Exclusive-OR operation on P_iR and ACN_i to get binary coded encrypted password cipher character BC_i.

   $BC_i = P_iR \oplus ACN_i$ for i= 1, 2, 3, 4.

7. Generate encrypted Password character by converting each BC_i into its equivalent symbol.
8. 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)).
9. Insert the encrypted Password characters in the random text at positions specified by N_1, N_2, N_3, N_4.

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.

$[P_1R, LR(k)]$ P_1 ←

III. 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.

Example

Consider four Composite numbers $(N_1, N_2, N_3, N_4) = (12, 15, 18, 24)$

Four digit Password $(P_1\ P_2\ P_3\ P_4) = (1\ 9\ 6\ 8)$

Generation of sequence of Catalan numbers CN_i 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

IV. 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