Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Password or Pin Encryption and Migration Technique using Catalannumber Sequence and Polygon Triangulation

1. V. Uma Karuna Devi Kakarla 2. CH. Suneetha
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

Article Info
Page Number: 1977-1987
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract: User password or PIN Number has become mandatory in every secret communication, financial and monitory transactions these days. Communicating and strong one-time password or PIN number increases the potential rise of the security. Crypto Council for Innovation (CCI) is developing many PIN security requirements as encrypted symmetric keys in structures called key blocks, which contain protected keys, usage constraints. In these key blocks, there is no expectation that previously established keys can be reused. In the present paper, password or PIN encryption and migration technique is explained using Catalan number sequences. Here the encrypted password or PIN is inserted in a long random text at different positions and the text is communicated to receiver. The positions of the inserted PIN characters are secret between the sender and the receiver.

Key words: Catalan Number C_n, Polygon triangulation T_n, Encryption, Decryption

I. INTRODUCTION

Due to the COVID pandemic many financial transactions are being done online via confirmation of OTP sent to mobile phones which is expected to be well secured. As the password or PIN is very small in size, it can be broken easily in communication mechanism. Crypto currency is a digital or virtual form of currency which uses cryptography for securing the transactions. It is ever expanding, runs on block chain where one exchanges currency with a peer using digital wallet. For the transaction, we need password. Crypto currency units are creating through mining Process. Text based and numerical based password or PIN is a popular authentication mechanism, but it is troublesome in communication aspects. As password or PIN is very small, main problem arises from memorability and reusing issues resulting into vulnerability to dictionary attacks. Moreover, migration of the user Password or PIN from one source to the other is quite difficult in Client/Server systems. Encrypted password or PIN can be stored securely in the directory of server and can be migrated across the internet with protection. Also unauthorized access of user password or PIN from the server can be prevented. The present paper explains password or PIN encryption and migration technique from one source to the other based on Catalan number sequence and polygon triangulation technique. A double encrypted password or PIN is inserted at different positions of a random text, communicated across the public channel. Encrypted mechanism is

secret between legitimate users and servers. The positions where the encrypted password or PIN characters are inserted are the secret keys (Decimal numbers) between the users.

Catalan Numbers:

Catalan numbers were discovered by a Belgian mathematician Eugene Catalan. It is a sequence of natural numbers denoted by C_n.

The formula for number sequence is

$$C_n = \frac{2n!}{(n-1)!n!} = \frac{1}{n+1}\binom{2n}{n} n \geq 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

The following table 1 shows the Catalan numbers for $n \in \{1, 2, ..., 20\}$ calculated with formula 1.

Table 1**:** First 20 values of Catalan numbers

n	C_n	n	C_n
1	1	11	58,786
2	2	12	208,012
3	5	13	742,900
4	14	14	2,674,440
5	42	15	9,694,845
6	132	16	35,357,670
7	429	17	129,644,790
8	1,430	18	477,638,700
9	4,862	19	1,767,263,190
10	16,796	20	6,564,120,420

For example,

If n=20, C_n = 6564120420

Catalan number using Euler`s triangulation problem can also be defined as

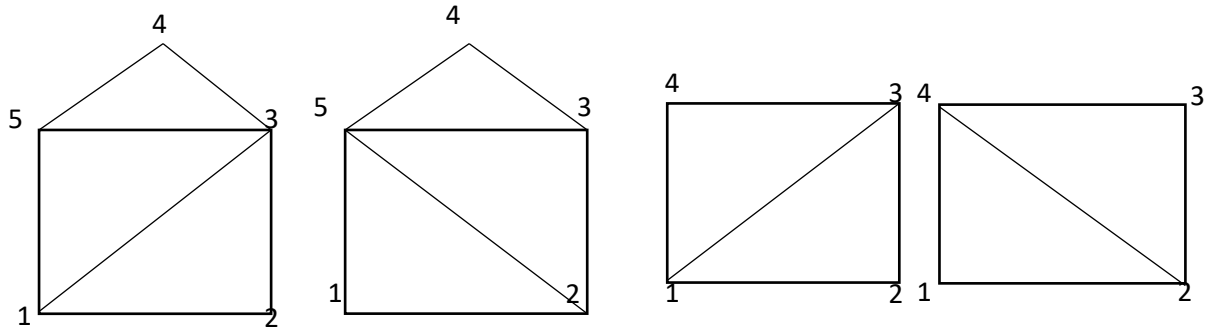
$$C_0 = 1, C_1=1 \quad C_n = \frac{4n-2}{n+1} C_{n-1} \quad n\geq 2 \ldots\ldots\ldots\ldots\ldots (2)$$

Ubiquitous Nature of Catalan Numbers:

Like Fibonacci and Lucas numbers Catalan numbers have ubiquitous nature. Catalan sequences have many applications in Combinatorics in finding the number of lattice paths of mountain ranges (Dyck paths), in formation of binary trees, in parenthesizing problem, in abstract algebra and sports. Polygon triangulation and Catalan numbers have several applications in cryptography [2,3,8]. They are used to design encryption algorithms, Cryptography key generation algorithms in the history of cryptography.

Polygon Triangulation:

In computational geometry, dividing the polygon area into triangles with non-intersecting diagonals is called polygon triangulation. For a complex polygon, the triangulation is just drawing the diagonals between nonadjacent vertices.



It has many applications in curved geometry, in art gallery problem for obtaining 3D object Representations, Computer graphics and in CAD programs etc..Catalan number is a number sequence which is the solution of many combinatorial problems. Polygon Triangulation is a problem used in discovery of Catalan numbers. A Convex n-gon can be decomposed into (n-2) triangles. To associate the Polygon triangulation and Catalan number, the number of triangles with n-angle is denoted by T_n.

$T_n = C_{(n-2)}, n \geq 3$…….(3)

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

For polygon triangulation, first the polygon is decomposed into trapezoids; the Trapezoids are divided into monotone polygons, then the monotone polygons into Triangles. This algorithm is called Seidel's Algorithm. A Polygon with 10 vertices requires 0.9milli seconds, 50 vertices require 3.5milli seconds, 100 vertices 6.7milli seconds of time. So, a polygon with 1kb vertices requires 97.6milli seconds.

II. LITERATURE SURVEY

M. Yildirm, I.Mackie[1] proposed Password security and memorability technique for encouraging the users. In that chapter they divided the entire group of users into two parts

and applied empherical formula. Shay et-al[2] specified that the users are not aware of construction of strong passwords. Florencio, D. et-al[3] studied the average password required accounts for a user in a day. Perrig [4] proposed suitable protocol for security levels as key agreement protocols using binary tree. Mishra, Swetha[5] designed an analysis of password-based authentication in her doctoral thesis. In that thesis she developed password hashing algorithm and analysed exiting password mechanisms. Katha chanda [6] studied security analysis and strength of passwords. In that chapter the author carried out different tests to evaluate the resistance of the password against brute force attacks. D. Sravana Kumar et.al [7] designed password encryption scheme based on elliptic curve cryptography over finite fields. Saracevic et-al [8] proposed Possibilities of applying the triangulation method in the biometric identification process. Amounas et-al [9] designed Novel Encryption Schemes Based on Catalan Numbers. Higgins P.M.[10] explained how different kinds of numbers arose and why they are useful. Horak Pet-al [11] proposed an application of Combinatorics in Cryptography. In that article, they focused on the MaxMinMax problem and present results over finite and infinite fields. Koscielny C et-al [12] proposed Theoretical Foundations and Practical Applications. In that chapter, the author introduced some basic mathematical concepts necessary to understand the design of modern cryptographic algorithms and protocols.

III. PROPOSED SCHEME

The present password or PIN encryption and migration technique is well suited for transmitting one time password (OTP) in Client/Server applications. The mechanism works on Catalan number sequence and Polygon triangulation algorithms.

If two legitimate users want to communicate password or PIN or secret key (small in size) for future communications, before transmission they agree upon to use a natural number ‘n’ which is a secret key for encrypting and migrating encrypted password or PIN, particularly a big composite number having more than a non-trivial factors. Example: 36 have 6 non-trivial factors 2,3,4,6,9,12.

In those factors first four numbers in increasing order are to be considered say n_1, n_2, n_3, n_4. The sender also selects a random text with length greater than or equal to the biggest factor [decimal number] of the agreed upon composite number.

ENCRYPTION:

1. For the four decimal numbers (factors) of the consented composite number corresponding Catalan number C_n and polygon triangulation T_n are calculated using the above mentioned formulae (1),(4).

2. The password or PIN is generally small in size consisting of a numerals say M_1, M_2, M_3, M_4. These four numerals are coded to ASCII equivalent binary values.

3. Let the Catalan number sequences for n_1, n_2, n_3, n_4 be Cn_1, Cn_2, Cn_3, Cn_4. These Catalan number sequences Cn_1, Cn_2, Cn_3, Cn_4 are adjusted to mod 256, corresponding ASCII binary equivalents are written.

4. The polygon triangulation number Tn_1, Tn_2, Tn_3, Tn_4 of the numbers n_1, n_2, n_3, n_4 are adjusted to mod 7.

$Cn_i \pmod{256} = ACn_i$ (Adjusted Cn), for i=1,2,3,4

$Tn_i \pmod 8 = ATn_i$ (Adjusted Tn), for i=1,2,3,4

5. The ASCII binary of the first numeral M_1 in the password or PIN is right rotated byATn_1 times.

For instance M_1 = 11011011 and ATn_1 = 4 then M_1 is right rotated four times.

Table 2: Right rotation operation by 4 times

1	1	0	1	1	0	1	1
1	1	1	0	1	1	0	1
1	1	1	1	0	1	1	0
0	1	1	1	1	0	1	1
1	0	1	1	1	1	0	1

$[M_1, RR(k)]$ M_1R ⟵

6. Logical XOR operation is applied between the resulting binary numbers of step 5and ASCII 8-bit binary equivalent ACn_1.

If ACn_1= 55 then ASCII binary of ACn_1= 55 is 00110111 and M_1R =10111101(obtained from step 5)

Logical XOR is applied between M_1R and ACn_1.(10111101) and (00110111)

$M_1R \oplus ACn_1$:

M_1R: 10111101

$\oplus$

ACn_1: 00110111

$M_1R \oplus ACn_1$= 10001010 = M_1C

$M_iR \oplus ACn_i = M_iC$, for i = 1,2,3,4

The ASCII symbol for this binary number is considered as first encrypted character M_1C.

7. Similar encryption procedure of steps 5,6 are applied on the other numerals of the password or PIN M_2, M_3 and M_4 to get the encrypted password or PIN M_2C, M_3C and M_4C.

8. The sender of the message selects randomly large text having all types of characters as text, numerals, and special characters with a minimum size equal to greatest factor for the considered key (composite number). These encrypted characters inserted at the positions n_1, n_2, n_3 and n_4 of the selected random text and communicated to the receiver as cipher text. The positions n_1, n_2, n_3 and $n_4$are mutual understanding between the sender and receiver or the positions where the encrypted password or PIN characters are inserted may be communicated by the sender in a separate communication. For security concerns the composite number 'n' may be changed from time to time.

Minimum Size of the Random text $\geq$ Max (n_1, n_2, n_3, n_4).

Decryption: Since it is a symmetric cipher the reverse process of encryption is decryption. The receiver after getting the large random text first picks up the encrypted password or PIN characters from their positions (known to both the legitimate entities). Reverse Logical XOR operation is applied on each character as in step 6

$$M_iC \oplus ACn_i = M_iR, \text{ for } i = 1,2,3,4$$

Then the resulting binary stream is left rotated k times to get operation is applied on the resulting binary stream to get the M1. Corresponding ASCII character is the original password character.

$[M_1R, LR(k)]$ M_1 ←

IV. EFFECTIVE UTILITY OF THE ALGORITHM IN CLIENT/SERVER SYSTEM

The present password encryption and insertion technique is well suited in client / server systems for transmitting one time password (OTP) to the client's transactions; also for drawing cash from ATM machines. Composite numbers having minimum four factors are stored in the central server. As the central server is powerful and provides the information to workstations, enormous number of composite numbers having at least four factors can be stored in it.

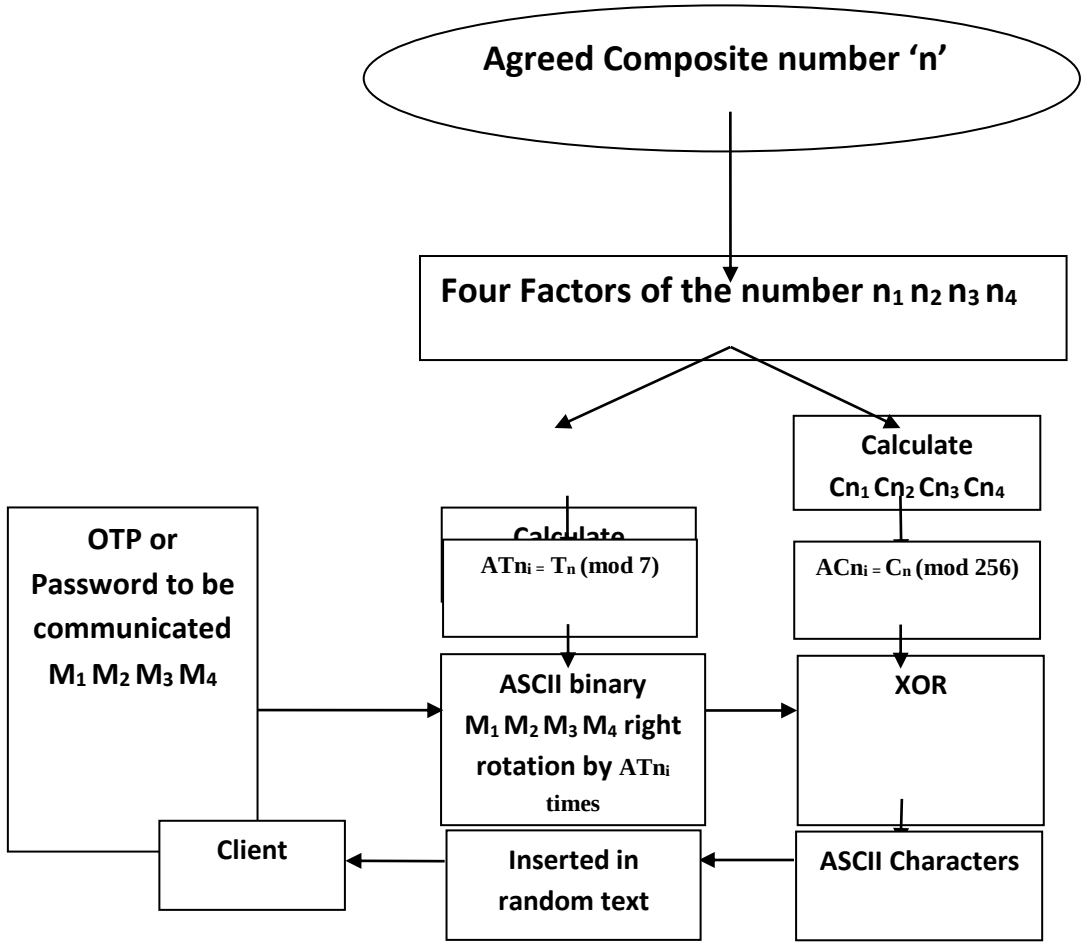
At the initial stage the client has to install the server application and has to register for the activation of client's application server. At that time of activation, central server stores the clients credentials and allots the client random composite numbers to choose one number among them with at least four non trivial factors for future transactions with the bank. When the client wants to make a transaction with the bank, requests the central server for OTP from his/her application server. Central server verifies the client's credentials, generates OTP (four digits), encrypts by using the allotted composite number to the client at the time of registration. The encrypted OTP is inserted in a random text at the positions of n_1,n_2, n_3 andn_4 respectively. Client's application server recognizes the position of encrypted OTP character

(numerals), decrypts it and gives the OTP for the transaction. The decryption process is done at the server application.

Table. 3 CLIENT/SERVER SYSTEM

Customer	Client Application Server	Central server
Application Request →		Credentials fed to central server and allocated some random composite numbers for applicant to select secret key.
Selects a random number ←		(Secret key)
(secret key) →	(Secret key) →	
	OTP Generation	
starts transaction with OTP →	Requests OTP →	Encrypts OTP, inserted in large random text and communicate to client server.
←	OTP decryption and send to client ←	

FLOW CHART



Example

Consider Composite numbers $n_1 = 3$, $n_2 = 9$, $n_3 = 16$, $n_4 = 22$

Take Password $(M_1\ M_2\ M_3\ M_4) = (1\ 4\ 2\ 6)$

Consider the random Text: GITAM INSTITUTE OF SCIENCES

Table 4. Generation of Catalan number C_n and Polygon triangulation number $T_n$for

n_i For i=1,2,3,4	**C_n**	**T_n**	**$ACn_i = C_n \pmod{256}$**	**$ATn_i = T_n \pmod 7$**
$n_1 = 3$	5	1	5	1
$n_2 = 9$	4862	429	254	2
$n_3 = 16$	35357670	2674440	230	6
$n_4 = 22$	91482563640	6564120420	56	4

considered composite numbers

Table 5. Generation of the encrypted passwordfor considered key (composite number)

M_i for i=1,2,3,4	**8- bit binary equivalent of M_i**	**ATn_i**	**RORATE RIGHT (RR) M_i by ATn_i times $M_iR=[M_i, R(ATn_i)]$**	**8- bit binary equivalent of ACn_i**	**$M_iR \oplus ACn_i$**	**Equivalent Symbol**
$M_1 = 1$	00000001	1	10000000	00000101	10000101	**…**
$M_2 = 4$	00000100	2	00000001	11111110	11111111	ÿ
$M_3 = 2$	00000010	6	00000100	11100110	11100010	â
$M_4 = 6$	00000110	4	01100000	00111000	01011000	X

Minimum Size of the Random text = Max (n_1, n_2, n_3, n_4) = Max(3, 9, 16, 22) = 22

Consider the random Text: GITAM INSTITUTE OF SCIENCES

The encrypted characters (**…,** ÿ, â, X) inserted at the positions n_1, n_2, n_3 and n_4(3, 9, 16, 22) of the minimum size of the random text.

Encrypted Text: GI…AM INÿT**ITUTE** âOF **SC**XEN**CES**

Table 6. Generation of Encrypted Text

Random Text	**GITAM INSTITUTE OF SCIENCES**
Encrypted Text	**GI…AM IN**ÿT**ITUTE** âOF **SC**XEN**CES**

V. Security Analysis and Conclusions

In password or PIN communication mechanisms, main security issues arise since the password or PIN is very small merely number or text characters or special characters. Due to the small size no big deal, it can be cracked very easily and can be tampered. To avoid tracking and stealing of PIN by shoulder surfing when a customer withdraws money from ATM machines, to stop misuse and unnecessary involvement of third party in transactions an indirect PIN entry method safe and more secure. Covert form of password or PIN provides integrity and confidentiality of the sending information. In the present designed password or PIN the password is double encrypted and inserted at different positions of random text and transmitted through insecure channel. The encryption technique and the location of encrypted characters are understanding between the parties. Only one secret key a composite number 'n' is sharing which can be varied time to time to avoid key compromise. The original password or PIN characters are encrypted using Catalan number sequence and polygon triangulation sequence. Since the adversary is unaware of the password or PIN positions man-in-middle attack is highly impossible here to implement. In any case the positions are compromised, the characters are disguised. So, the algorithm developed here is free from all the security issues.

VI. 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. Narmadha R., Latchoumi T.P., Jayanthiladevi A., Yookesh T.L., Mary S.P.: “A Fuzzy-Based Framework for an Agriculture Recommender System Using Membership Function”, In Applied Soft Computing: Techniques and Applications, pp. 207-223, CRC Press, 2022.
14. Vijay Vasanth Aroulanandam, Thamarai Pugazhendhi Latchoumi, Karnan Balamurugan, Tiruchengode Lakshmanasamy Yookesh.: “Improving the Energy Efficiency in Mobile Ad-Hoc Network Using Learning-Based Routing”, Revue d' Intelligence Artificielle, Vol 34(3), pp. 337-343, 2020.
15. Jena, G., Panda, S. S., Rajesh, B. V., & Jena, S.. "Image Super Resolution Using Wavelet Transformation and Swarm Optimization Algorithm." International Conference on Intelligent Human Systems Integration. Springer, Cham, pp. 444-449, 2018.