Journal of Theoretical and Applied Information Technology

30th November 2023. Vol.101. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

VARIABLE LENGTH PACKET CIPHER USING CATALAN SEQUENCE

V. UMA KARUNA DEVI KAKARLA[1] , CH. SUNEETHA[2]

[1]Research Scholar, GITAM University, Department of Mathematics, Visakhapatnam, India

[2]Associate Professor, GITAM University, Department of Mathematics, Visakhapatnam, India

[1]ukakarla@gitam.in, [2]schivuku@gitam.edu

ABSTRACT

In recent times, the world is transforming to digital communication from than physical communication. Secure data transfer has become essential and challenging task all over the world. Cryptography is the science of secure communication of sensitive data via public channel. Encryption algorithms use mathematical techniques to create confusion and non-comprehensible to unintended persons. Applied number theory and cryptography have inextricable attachment. Many tools of elementary and applied number theory have vast applications in cryptography. The present paper aims at designing a variable length packet cipher using Catalan number sequence. Sequence of Catalan numbers forms variable size matrices when arranged in a special pattern. The interesting fact is that all these matrices are symmetric having determinant one. These matrices are used in the present algorithm for encryption and decryption.

Key Words: *Catalan Number Sequence, Encryption, Decryption, Matrices.*

1. INTRODUCTION

The modern Cryptography has significance to research in order to transfer data securely between two or more entities, especially when the data transferred classified as a critical or important data. Even though there are numerous encryption algorithms exist, it is always doubtful. So, it is necessary to introduce a secure and hack proof method to cyber security. The proposed work represents a new algorithm to encrypt and decrypt data securely with the benefits of catalan number sequences, Matrix Diagonal Function to generate variable length packet ciphers. Many cryptographic algorithms mostly based on specialized branch of mathematics, the number theory. Computational number theory especially is the most important field in information security.

A Cryptographic primitive which uses fixed size input is called Fixed Input Length (FIL) primitive. All the conventional packet ciphers like AES, DES operate on a fixed size input. Fixed size packet ciphers are easily vulnerable to linear and differential cryptanalysis, because of fixed permutation table and fixed same rounds of encryption. To avoid this, construction of new primitives using Variable Length Input (VIL) have been developed in the history. The situation where the encryption algorithm deals with varying packet lengths, presenting the property of having same plain text and cipher text size is usual in internet and wireless applications.

1.1 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

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

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

$C_0 = 1 \qquad C_1=1$

$C_n = \frac{4n-2}{n+1} C_{n-1}$ for $n \geq 2$

For example

If $n=20$, $C_n = 6564120420$

The Catalan number sequence for first 10 natural numbers are given below

Table 1: Catalan number sequence

S.No.	n	C_n
1	1	1
2	2	2
3	3	5
4	4	14
5	5	42

6	6	132
7	7	429
8	8	1,430
9	9	4,862
10	10	16,796

1.2 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 and in abstract algebra and sports. Polygon triangulation and Catalan numbers have several applications in cryptography. They are used to design encryption algorithms, cryptography key generation algorithms in the history of cryptography.Interesting problem on Catalan numbers One interesting problem on Catalan numbers is that the sequences of Catalan numbers can be arranged in the form of matrices in a special pattern. The Catalan number sequences are 1, 1, 2, 5, 14, 42, 132, 429, …

These number sequences can be arranged as 2 x 2, 3 x 3, 4 x 4 matrices as

$$\begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 5 \\ 2 & 5 & 14 \\ 5 & 14 & 42 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 5 & 14 \\ 2 & 5 & 14 & 42 \\ 5 & 14 & 42 & 132 \\ 14 & 42 & 132 & 429 \end{bmatrix}$$ and so on.

All the matrices are symmetric and having the determinant one. This special property of Catalan numbers is used to develop variable length packet cipher in the present paper. All these matrices are symmetric with degrees of freedom 3, 5, 7, 9 and so on. That is 3 elements are required to describe the first (2 x 2) matrix, 5 elements require to describe second (3 x 3) matrix, 7 elements to (4 x 4) matrix and so on.

In this work, we developed proposed Encryption and Decryption algorithms to balances both security and integrity of the transmission. The proposed Encryption algorithm encrypts given plain text based on the catalan number sequences, symmetric matrices and MDF(Matrix Diagonal Function). The proposed Decryption algorithm produces plain text for the cipher text by the same steps as enciphering with inverse matrix multiplication..

2. LITERATURE SURVEY

Bellare and Rogway [1] introduced the conversion of FIL packet cipher to VIL packet cipher. They proposed a new technique for constructing packet ciphers with arbitrary length input using Parsimonious Pseudo Random functions and schemes. Later, number of other papers were published in this direction. Ruby and Rackoff [2] showed the conversion of n bit Pseudo Random function into packet cipher, operating on 2n bits. The following work by Naor and Reingold [3] was conversion of packet cipher operating on n bits to packet cipher C*n bits for constant C ≥ 1. Sarvar Patel et.al [4] constructed a variable input packet cipher which is an improvement of Bellare and Rogway. K.C. Syamala Bai et.al [5] suggested variable size packet encryption using dynamic key mechanism.

Muzafer saracevic [6] et.al. Proposed cryptographic key generation algorithm of polygon triangulation and Catalan numbers in three phases. Faruk selimovic[7] et.al. applied Delaunay triangulation and Catalan objects in steganography. In that chapter the authors used image encryption technique D.Sravan kumar et.al.[8] proposed a novel encryption scheme based on catalan numbers. Muzafer Saracevic[9] et.al. suggested method in biometric identification process in application of triangulation combination with face recognition technique.

Moses Liskov et.al [10] proposed the construction of tweakable packet ciphers. Christot Beierle et.al. [11] developed a lightweight tweakable packet cipher with efficient protection against DFA attack.

V. U. K. D. Kakarla, C. H. Suneetha[12] applied special property of Fibonacci sequences to generate positioned stream cipher.

Kalika Prasad, Hrishikesh Mahato [13] introduced generalized Fibonacci matrices in Hine-Hill ciphers. They have also established a key exchange matrix method with the help of multinacci sequences under prime modulo.

Katha chanda [14] 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.

Sravana Kumar et.al [15] suggested password encryption scheme based on elliptic curve cryptography over finite fields. Amounas et-al [16] designed Novel Encryption Schemes Based on Catalan Numbers. Higgins P.M.[17] explained how different kinds of numbers arose and why they are useful. Koscielny C et-al [18] 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.

Considering the literature on variable block ciphers and application of Catalan numbers in cryptography the present technique is designed to overcome the difficulties arose in the above-mentioned techniques.

PROPOSED SCHEME

As explained in the previous section, Catalan number sequences can be arranged as symmetric matrices in a special pattern as

$$C_1 = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 2 & 5 \\ 2 & 5 & 14 \\ 5 & 14 & 42 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 1 & 2 & 5 & 14 \\ 2 & 5 & 14 & 42 \\ 5 & 14 & 42 & 132 \\ 14 & 42 & 132 & 429 \end{bmatrix} \quad \text{and so on.}$$

These matrices are used as keys for encryption and decryption along with a secret agreed upon random function. Prior to the transmission, the legitimate users agree upon to use a random Matrix Diagonal Function (MDF) of diagonal elements of the cipher packet matrices.

MDF [a_{11}, a_{22}, a_{33}....] = $a_{11}+a_{22}+a_{33}+\ldots+$ [3 or 5 or 7…] depending on the key matrices used for encrypting plain text packets. a_{11}, a_{22}, a_{33}… are the diagonal elements of the matrices C_1, C_2, C_3 and so on; (a_{11}, a_{22}) are diagonal elements of first C_1 with degree of freedom 3 ;(a_{11}, a_{22}, a_{33}) of second cipher packet matrix with degree of freedom 5;(a_{11}, a_{22}, a_{33}, a_{44}) of third cipher packet with degree of freedom 7 and so on.

The whole message is divided into plain text packets M_1, M_2, M_3… of different sizes with lengths 4, 9, 16, 25, 36 and so on, equal to the sizes of square matrices C_1, C_2, C_3 and so on. The characters are coded to ASCII equivalent decimals.

3.1 Encryption

The following steps are involved in encryption process.

1. First data packet matrix is multiplied with C_1, to yield the cipher packet matrix S_1 (say)
$$S_1 = C_1 M_1 = \begin{bmatrix} S_{11} & S_{12} \\ S_{13} & S_{14} \end{bmatrix}$$
2. MDF (S_{11}, S_{14}) = $S_{11} + S_{14} + 3 = n_1$ (say)
3. Second key matrix C_2 is multiplied with n_1
4. Second plain text packet matrix M_2 is multiplied with n_1C_2 yielding second cipher packet matrix S_2 (say)
$$S_2 = n_1 C_2 M_2 = \begin{bmatrix} S_{21} & S_{22} & S_{23} \\ S_{24} & S_{25} & S_{26} \\ S_{27} & S_{28} & S_{29} \end{bmatrix}$$
5. Compute $n_2 = S_{21} + S_{25} + S_{29} + 5$
6. Compute $S_3 = n_2 C_3 M_3$

Same iteration of encryption is done for all plain text packets.

Here Matrix Diagonal Function (MDF) acts as secret key (private key). Enciphering of variable input length packets contributes easier migration path. The entire data is enciphered in the same way by considering packets with variable lengths, coded to equivalent ASCII characters that constitute the Cipher text. As the block size is varying, the whole plain text and cipher text sizes are same unnecessary involvement of adversary can be reduced and code reuse can be maintained. To add on more security for the packets, the present cipher text packet is concatenated if the succeeding packet key using a random MDF.

3.2 Decryption

As the present Methodology is Symmetric enciphering technique (Private Key Cryptography), deciphering follows the same steps as enciphering with inverse matrix multiplication. For the first packet decryption,

$$S_1 = C_1 M_1 \Rightarrow M_1 = S_1 C_1^{-1}$$

Compute $n_1 = S_{11} + S_{14} + 3$.

Second packet deciphering is $M_2 = \dfrac{1}{n_1} S_2 C_2^{-1}$, For third packet, $M_3=\frac{1}{n_2} S_3\, C_3^{-1}$

where $N_2=S_{21}+S_{25}+S_{29}+5$ and so on.

Table 2: Encryption/Decryption Chart

Enciphering Decipher		Plain Text M ↓ ASCII Decimals ↓				
		4 length	9 Length	16 Length	25 Length	… …..
		2 x 2 Matrix M_1	3 x 3 Matrix M_2	4 x 4 Matrix M_3	5 x 5 Matrix M_4	
Key → Catalan sequences of Natural numbers →	2 x 2 Matrix C_1	$S_1 = C_1M_1$ $M_1 = S_1\, C_1^{-1}$	$n_1 = s_{11}+s_{14}+3$	$n_2=s_{21}+s_{25}+s_{29}+5$	$n_3= s_{31}+s_{36}+s_{3(11)}+s_{3(16)}+7$	. . . . . .
	3 x 3 Matrix C_2	$S_2=n_1C_2M_2$ $M_2=\frac{1}{n_1} S_2C_2^{-1}$				
	4 x 4 MatrixC3	$S_3=n_2C_3M_3$		$M_3=\frac{1}{n_2} S_3C_3^{-1}$		
	5 x 5 Matrix C_4	$S_4=n_3C_4M_4$		$M_4=\frac{1}{n_3} S_4C_4^{-}$ 1		
	. . .	………..				

Example

Consider the message "PATIENCE AND SILENCE ARE TWO POWERFUL ENERGIES". Now divide the message into packets of lengths 4, 9, 16, 25---. Let the plain texts be M_1, M_2, M_3---. Convert each Character of M_1 as ASCII decimal and form a 2 x 2 matrix. Multiply M_1 with C_1 we get $S_1=M_1C_1=\begin{bmatrix}210 & 485\\ 230 & 533\end{bmatrix}$

$$S_1(\text{mod } 256) = \begin{bmatrix}210 & 229\\ 230 & 21\end{bmatrix}$$

Calculate $n_1= 210+21+3 = 234$

Now multiply C_2 with n_1,

$$n_1C_2=\begin{bmatrix}234 & 468 & 1170\\ 468 & 1170 & 3276\\ 1170 & 3276 & 9828\end{bmatrix}$$

Calculate $S_2=M_2\, n_1C_2$

$$S_2=M_2\, n_1C_2 = \begin{bmatrix}147420 & 388674 & 1132092\\ 140634 & 370422 & 1078038\\ 124020 & 325026 & 943254\end{bmatrix}$$

$S_2\,(\text{mod } 256) = \begin{bmatrix}220 & 66 & 60\\ 90 & 246 & 22\\ 116 & 162 & 150\end{bmatrix}$ and

$n_2 = 220 + 246 + 150 + 5 = 621 \ (\text{mod } 256) = 109$

Multiply C_3 with n_2 we get

$$n_2\, C_3=\begin{bmatrix}109 & 218 & 545 & 1526\\ 218 & 545 & 1526 & 4578\\ 545 & 1526 & 4578 & 14388\\ 1526 & 4578 & 14388 & 46761\end{bmatrix}$$

Now calculate $S_3 = M_3\, n_2\, C_3$ =

$$\begin{bmatrix}180068 & 515243 & 1577666 & 5041795\\ 166334 & 475676 & 1456131 & 4652883\\ 187807 & 540422 & 1659961 & 5315821\\ 181158 & 519712 & 1593907 & 5099456\end{bmatrix}$$

$$S3 \text{ (mod 256)} = \begin{bmatrix} 100 & 171 & 194 & 131 \\ 190 & 28 & 3 & 83 \\ 159 & 6 & 57 & 237 \\ 166 & 32 & 51 & 192 \end{bmatrix}$$

Cipher for I packet is Ò å æ NAK

Cipher for II packet is Ü B < Z ö SYN t ¢ –

Cipher for III packet is d « Â ƒ ¾ FS ETX S Ÿ ACK 9 í ¦ space 3 À

The cipher text is Ò å æ NAK Ü B < Z ö SYN t ¢ – d « Â ƒ ¾ FS ETX S Ÿ ACK 9 í ¦ space 3 À

4. PERFORMANCE AND STRENGTH ANALYSIS OF THE ALGORITHM

In the present variable packet encryption algorithm, entire message is divided into different segments (packets) of variable size. In packet encryption schemes, when an adversary tries to decrypt one packet, all the packets in that session will be compromised because of uniform length of the packets and same encryption key for all the packets. But, in the present scheme the packet size differs, plain text and cipher text sizes are identical. Also encryption/decryption keys are different for different packets. By varying packet length leakage of the packets can be avoided to some extent. Here the key matrices C1, C2, C3…, the matrices of Catalan sequences arranged in a special pattern are public and known to everyone. So, a random function; Matrix Diagonal Function (MDF) is an agreement between the legitimate users (secret key). To add more security previous cipher packet is concatenated with the present key packet, used for encrypting the present plain text packet. So, the whole cipher will not be damaged even though one packet is compromised. The execution time (encryption/decryption) for different size messages are recorded on a machine with 1GB RAM and 1.6 GHz processor speed on Win XP platform using MATLAB14, given in table 2. Fig.1 shows the execution time plot for different sizes of data.

Table 3: Encryption/Decryption Time Graph

S.No.	Size of the data in KB	Encryption/Decryption Time in Milli Seconds
1	1	0.0306
2	2	0.04216
3	3	0.0813
4	4	0.1224
5	5	0.1452
6	6	0.1932
7	7	0.2031
8	8	0.2438
9	9	0.2052
10	10	0.316

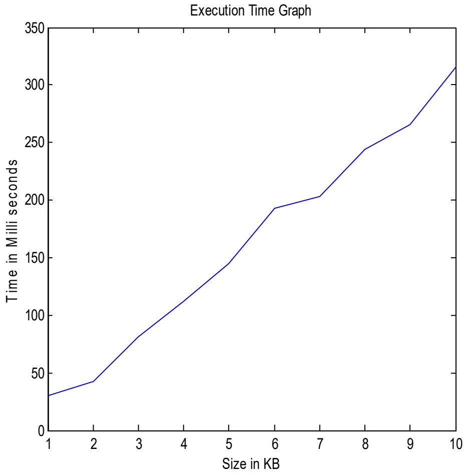

Figure 1: Execution Time Graph

Average execution time for one round of encryption of conventional packet encryption algorithms AES, DES and 3DES are calculated and compared with the present variable packet cipher as given in table.3 and Figure 2

Table 4: Comparison table with conventional techniques

Encryption Algorithm	Average time (m sec) for packets of different size		
	84 Bytes	256Bytes	512 Bytes
AES (For 1 round)	48.2	46.2	43.4
DES (For 1 round)	37.3	49.3	52.3
3DES (For 1 round)	46.2	50.1	53.3
Present technique	30.6	71.3	69.4

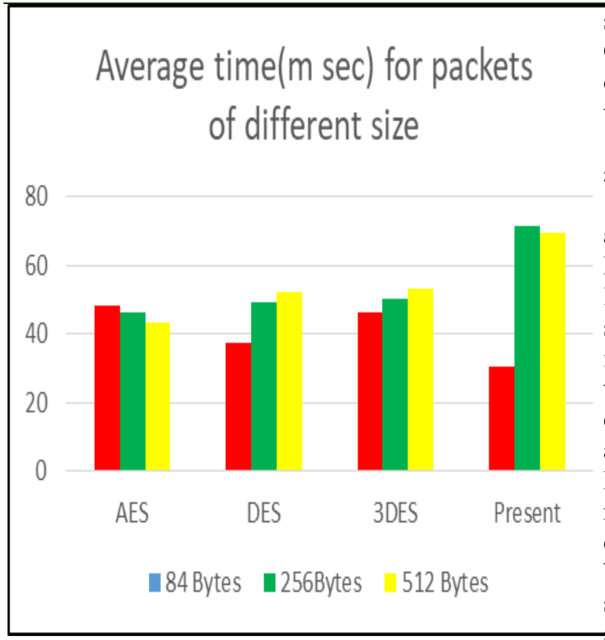

Figure 2: Comparison graph with conventional techniques

From the above Table2 and Figure 2, it is clear that the execution time for the present algorithm is slightly higher than one round of encryption of AES, DES and 3DES in all the three cases of different data size. So, when compared for 16 rounds of AES, DES and 3DES the present execution time very low. Though AES, DES and 3DES encrypt the data in 16 rounds, these are fixed block cipher modes, vulnerable to linear and differential crypt analysis.

With the added benefit of faster execution and less computational overhead, the current variable packet cipher is more secure against all sorts of active and passive attacks. In cloud computing packet encryption is a real time application, where the whole message packet is encrypted with the same session key.

When the third party succeeds to decrypt the packet, the whole message can be compromised. As the packet size is variable, the whole message cannot be damaged though it is partially compromised. Even the partial compromise of the message can be restricted by changing the random function MDF time to time.

The proposed algorithms work on catalan number sequences, Matrices and MDF to produce the variable length packet ciphers .Evaluated studies on variable block ciphers and application of Catalan numbers in cryptography for cryptography operations to provide the security during the data transmission.

5. CONCLUSION

In the present work, we propose Encryption and Decryption algorithms. The proposed Encryption algorithm resulted an output of variable length packet ciphers using catalan Number sequences. The proposed Decryption algorithm was implemented on the variable size ciphers which were produced as an output of plain text. When comparing the results of proposed work to existing algorithms, we found that proposed Encryption and Decryption algorithms have been effective in minimizing the average execution time of packets of different sizes.The present algorithm balances both security and integrity of the transmission. The strength of the cipher is primarily based on the secret key used. The present algorithm uses varying of keys, the keys can be changed frequently and suddenly to maintain perfect secrecy of the cipher. So, the present variable packet cipher is equivalent to the conventional block ciphers in all aspects of security and integrity with lesser execution time and relatively less computational risk.

REFERENCES

[1] M. Bellare and P. Rogaway. On the construction of Variable-Input-Length ciphers. In Proc. Fast Software Encryption, 1999.

[2] Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Computing, 17(2):373–386, April 1988.

[3] Naor and O. Reingold. On the construction of pseudo-random permutations: Luby-Rackoff revisited. J. of Cryptology, 12:29–66, 1999. Previously in STOC 97.

[4] Sarvar Patel, Zulfikar Ramzan and Ganapathy S. Sundaram Efficient Constructions of Variable-Input-Length Packet Ciphers, H. Handschuh and A. Hasan (Eds.): SAC 2004, LNCS 3357, pp. 326–340, 2005. c Springer-Verlag Berlin Heidelberg 2005

[5] K.C.Shyamala Bai ,M.V.Satyanarayana , P.A. Vijaya Variable Size Packet Encryption using Dynamic-key Mechanism (VBEDM), International Journal of Computer Applications (0975 – 8887) Volume 27– No.7, August 2011

[6] M Saracevic, A Selimi, F Selimovic Generation of cryptographic keys with

algorithm of polygon triangulation and catalan numbers- Computer Science, 2018

[7] Selimovi´c, F.; Stanimirovi´c,P.; Saraˇcevi´c, M.; Krtolica, P.Application of DelaunayTriangulation and Catalan Objects inSteganography. Mathematics 2021, 9,1172.

[8] D. Sravana Kumar, CH. Suneetha, A. Chandrasekhar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.161-166

[9] Saračevič M., Elhoseny M., Selimi A., Lončeravič Z. (2021) Possibilities of Applying the Triangulation Method in the Biometric Identification Process. In: Bilan S., Elhoseny M., Hemanth D.J. (eds) Biometric Identification Technologies Based on Modern Data Mining Methods. Springer, Cham.

[10] Liskov, M., Rivest, R.L. & Wagner, D. Tweakable Block Ciphers. J Cryptol 24, 588–613 (2011)

[11] Beierle, C., Leander, G., Moradi, A., & Rasoolzadeh, S. (2019). CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks. IACR Transactions on Symmetric Cryptology, 2019(1), 5–45.

[12] V. U. K. D. Kakarla, C. H. Suneetha, Information and Communication Technology for Competitive Strategies (ICTCS 2022), Lecture Notes in Networks and Systems 623, (199-211)2022.

[13] Kalika Prasad, Hrishikesh Mahato arxiv:2003.11936v1[CS.CR]25 March2020

[14] 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

[15] 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

[16] 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.

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

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