ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

DATA ENCRYPTION WITH IMPROVISED ALGORITHM BASED HOSOYA POLYNOMIAL AND PERMUTATION FUNCTION

Dr. Minakshi Gaur
HOD Mathematics, NASPG College, Meerut, UP

Dr. Kapil kumar Sharma, Dept of Mathematics, sardar vallabhbhai patel University, Meerut UP

Dr. Ruchira Goel, Assistant Professor, Ajay Kumar Garg Engineering College, Ghaziabad

Abstract
In this study, researcher explore one of the most interesting aspects of cypher texts by establishing a link between mathematical approaches and a data security mechanism. We employ an improved technique to encrypt and decode the characters. By translating each character to a polynomial equation, the code is created. To add difficulty, we're working on encrypting the plaintext. We split the text into pieces and apply a cryptographic technique to encrypt it for later use. The number of characters was more than the number of characters before the enhance algorithm was used. The principle behind the technique is that the letters are mixed in with other letters, and then the code is encrypted. As a consequence, data security is quite good.

1- Introduction

The security of many presently-used cryptosystems, e.g., of all public-key cryptographic schemes, is based on the assumed hardness of computational problems in number theory such as the integer-factoring problem (e.g., RSA [1]). Cryptography involves creating written or generated codes that allows information to be kept secret.Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to betransmitted without anyone decoding it back into a readable format, thus compromising the data [D] . The difference between cryptography and hiding information. Cryptography is a discipline of computer science, where algorithms and security practices are acting as a central tool. This is traditionally based on the mathematical foundation. The practical applications contain the assurance of legitimacy, protection of information from confessing, and protected message communication systems for essentialrequirements to enforce security [W] . hide information in the digital media is known as data hidingsuch as images, video and audio data .

In a traditional definition of security of a cryptographic scheme, one usually defines a game that characterizes the capabilities of a (hypothetical) adversary. A cryptographic scheme is defined to be secure if no computationally feasible strategy allows the adversary to win the game with non-negligible probability (or advantage), for reasonable notions of feasible and negligible. The notion of " feasible" ishard-wired into the definition and is defined as some form of polynomial time. Similarly, negligible is defined in a specific manner such that, roughly speaking, feasible times negligible is still negligible. Such definitions are therefore necessarily asymptotic[R].

we examined the defects of known definitions of contrast of the VCSvisual cryptography scheme, andproposed a new definition based on our observations. Also, we have shown both experimentally and theoretically that our new definition of the contrast agree with our observations more [Z].

The extended in utilizing computer networks for transmission and management of information as wellas the fact that the users of IT is growing day by day, needs the role of security Mechanisms to assure privacy, authentication or integrity of information. Such requirements have been covered by utilizing several cryptographic protocols that often combine asymmetric and symmetric cryptosystems [N].

2- Related work

P. David and S.Jacques in 2000 proposed Homomorphic Encryption [1]**.** Diffie and Hellman used authentication and verification in RFID communication process is International Data Encryption Algorithm(IDEA) algorithm as well as to improve security on RFID access authentication and verification using cryptography algorithm, [8].

Design scheme that used threshold cryptography in which data owner divides users in groups and gives single key to each user group for decryption of data and, each user in the group shares parts of thekey. Challenges for ensuring the confidentiality, integrity and access control of the data. This scheme provides the strong data confidentiality and reduces the number of keys [9]. We were proposed Encryption algorithms based on chaos are known to satisfy the basic requirements of the cryptosystem such as high sensitivity, high computational speed and high security. The chaos-based encryption algorithm is built upon a modified quadratic map named as quadratic sinusoidal map which exhibits better array of chaotic regime when compared to the traditional logistic

map[8]. They were focused on exploiting the classic ARQ protocol for securing the exchange of secret keys between legitimate users, where even the realistic practical ARQ feedback associated with transmission errors has been considered. In conventional wireless systems, the mechanisms assuring security, reliability and throughput are designed individually and separately, which is however potentially suboptimal, since thethree factors are coupled and affect each other [4].
Proposed methodology a Cryptography key generating based on graph construction and adjacency matrix of extracted minutiae. The formation of graph relies on contour division of minutiae points' area. Results show that with singular point detection the average of minutiae points area dimension is less than in the other case and at some points of threshold, it show an Improvement performance comparingto the other one[10]

3- Proposed algorithm Encryption algorithm [14]:-

a – Extraction Hosoya polynomial for all letters in the text which we wante to encrypt.

b – Take positive integer number n.

c – Divide the text with length 2n by using dihedral group as:

$$w = \begin{bmatrix} W1 \\ W2 \\ \cdot \\ \cdot \\ W2n \end{bmatrix} = \begin{bmatrix} U \\ V \end{bmatrix} \quad where\ U = \begin{bmatrix} W1 \\ W2 \\ \cdot \\ \cdot \\ W2n \end{bmatrix} \quad and\ V = \begin{bmatrix} Wn+1 \\ \vdots \\ \cdot \\ W2n \end{bmatrix}$$

d – Apply the dihedral operations (x,y):

k=0,1,..n-1

$$D_n w = \begin{bmatrix} (x^k & U_{k+1}) & mod\ 27 \\ (Yx^k & V_{k+1})^R & mod\ 27 \end{bmatrix}$$

$$D_n w = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ n-1 & 1 & 1 \end{bmatrix} + [hosoya\ polynomial\ of\ Zi\ vectors] \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ n-1 & 1 & 1 \end{bmatrix} + [hosoya\ polynomial\ of\ Zi\ vectors] \right)^R \end{bmatrix}$$

Note(1):- To improve this method we must encryption the first letter because the first letter by usingthis method stay the same letter always.

- - encryption the first letter by this equation:

$c_i = w_i + (2*n) \bmod 27$New addition:

d. Segmentation the text crypto to segment.

e. Each segment content to four charter.

f. Apply on text the permutation functionSegment k old=[1 2 3 4 5 6]

K new=[6 2 4 1 3 5]

ii- Decryption algorithm

a- Decryption text[14]
First decryption the first letter by the equation
b-w1=c1-(2*n) mod 27
c- for other letter using :

k=0,1..n-1

$$D_nC = \begin{bmatrix} (x^{-k} & U_{k+1}) & mod\ 27 \\ (Yx^{-k} & V_{k+1}) & mod\ 27 \end{bmatrix}$$

Example

word(FADYA)

F=Z6=6 , A=Z1=1, D=Z4=4, Y=Z25=25

F→ $6+7x+8x^2$

A→ $1+0x+0x^2$

D→ $4+4x+2x^2$

Y→ $25+36x+264x^2$

A→ $1+0x+0x^2$

Now let n=2 , D_{2n} = D_4 ={ i° , I , j , ji }

Then {FADYA}→ {FADY} + {A- - -}

$$\text{where } U = \begin{bmatrix} 6 \\ 1 \end{bmatrix} \text{ and } V = \begin{bmatrix} 4 \\ 25 \end{bmatrix}$$

$$\{FADY\} \rightarrow w_1 = \begin{bmatrix} 6 \\ 1 \\ 4 \\ 25 \end{bmatrix} = \begin{bmatrix} U \\ V \end{bmatrix}$$

(mod 27)

$$D_1w_1 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 7 & 8 \\ 1 & 0 & 0 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 4 & 4 & 2 \\ 25 & 36 & 264 \end{bmatrix} \right)^R \end{bmatrix}$$

$$= \begin{bmatrix} \begin{bmatrix} 6 & 8 & 9 \\ 2 & 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 4 & 5 & 3 \\ 26 & 10 & 6 \end{bmatrix} \end{bmatrix}$$

FHIBAADECZJF

The first letter F→6→6+4=10→JJHIBAADECZJF

$$\text{where } J = \begin{bmatrix} 0 \\ 27 \end{bmatrix} \text{ and } K = \begin{bmatrix} 27 \\ 27 \end{bmatrix}$$

$$= \begin{bmatrix} J \\ K \end{bmatrix} \{A \ldots\} \rightarrow W_2 = \begin{bmatrix} 0 \\ 27 \\ 27 \\ 27 \end{bmatrix}$$

(mod 27)

$$D_1 w_1 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 27 & 0 & 0 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 27 & 0 & 0 \\ 27 & 0 & 0 \end{bmatrix} \right)^R \end{bmatrix}$$

$$= \begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 28 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 27 & 1 & 1 \\ 28 & 1 & 1 \end{bmatrix} \right)^R \end{bmatrix} = = \begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{bmatrix}$$

AAAAAA#AAAAA
The first letter A→15→1+4=5→EEAAAAA#AAAAA
Then the cipher text is: JHIBAADECZJF EAAAAA#AAAAA
Segment1=JHIB Segment2=AADE Segment3=CZJF Segment4=EAAA Segment5=AA#A Segment6=AAAA K old=[1 2 3 4 5 6]
NEW ARRANGE K new=[6 2 4 1 3 5]
Then the new cipher text is: AAAAAADEEAAAJHIBCZJFAA#A

2-Decryption:-

K new= [6 2 4 1 3 5]

AAAAAADEEAAAJHIBCZJFAA#A
Knew to K old
JHIBAADECZJF EAAAAA#AAAAA
Notice that
C_1→″ JHIBAADECZJF ″
The first letter E→10→10-4=6→F

(mod 27)

$$D_1 C_1 = D_n = \begin{bmatrix} \begin{bmatrix} 6 & 8 & 9 \\ 2 & 1 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 4 & 5 & 3 \\ 26 & 10 & 6 \end{bmatrix} \right)^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} \begin{bmatrix} 6 & 7 & 8 \\ 1 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 4 & 4 & 2 \\ 25 & 36 & 264 \end{bmatrix} \end{bmatrix}$$

where $U = \begin{bmatrix} 6 \\ 1 \end{bmatrix}$ and $V = \begin{bmatrix} 4 \\ 25 \end{bmatrix}$

$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \\ 4 \\ 25 \end{bmatrix} = \{FADY\}$$

C_2→EAAAAA#AAAAA
The first letter E→5→5-4=A→A

(mod 27)

$$D_2 C_2 = D_n = \begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right)^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{bmatrix}$$

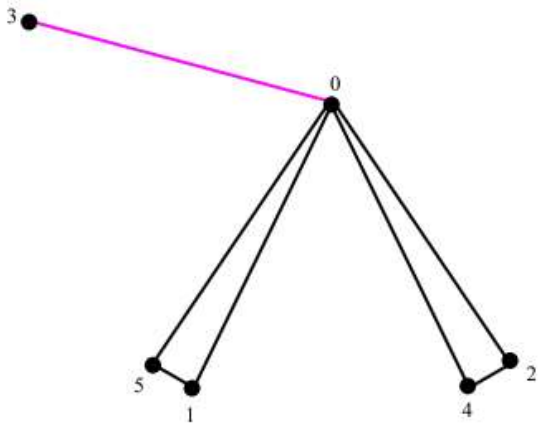
$$= \begin{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{bmatrix}$$

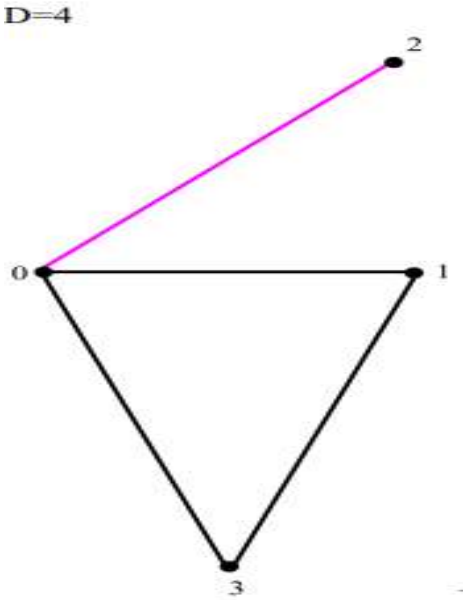
$\{A\text{----}\}$

Then the plain text is (**FADYA).**

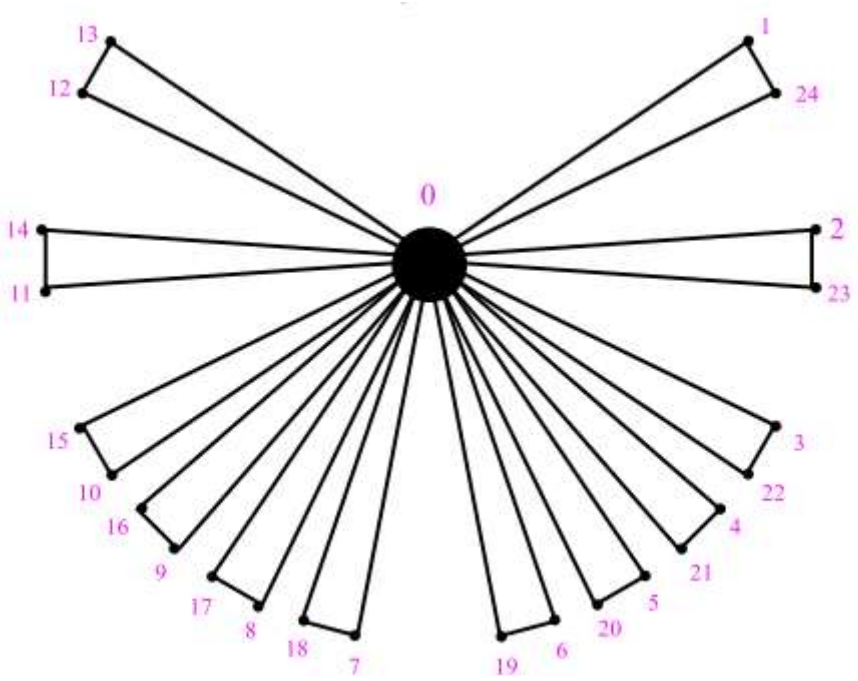
Details graph

F=6





Y=25



CONCLUSION

In this research, researcher introduce an algorithm that links mathematics and cipher science to computer science. This algorithm can be applied to computer networks to keep the information transmitted from the sender to the recipient safe and ensure the integrity of the transmitted message. In addition, the immersion method is used by immersing the encoded character into a character set, Easy guess content. The result high security and robust crypto. The future work using ASCcode instead normal charter

References

1- P. David and S.Jacques, " Security Arguments for Digital Signatures and Blind Signatures" , J. Cryptology ,13: 361– 396 ,2000.

2- Doha, H.M. (2018)."Representation of groups (Z1_Z26) by graph and ciphering every graph". MSc thesis, Department of mathematical science, university of tikrit, Iraq.

3-W. Chua, C. Yuen, Y. Guan, and F. Chin, " Robust multi-antenna multi-user precoding based on generalized multi-unitary decomposition withpartial CSI feedback," IEEE Trans. Veh. Tech., vol. 62, no. 2, pp. 596-605, Feb. 2013 .

4- N .Sarah ,K. Stefan, M. Mira, and B. Eric . (2016). Jumping Through Hoops: Why Do Java Developers Struggle with Cryptography APIs?. In Proceedings of the 38th International Conferenceon Software Engineering (ICSE ' 16). ACM, New York, NY, USA, 935– 946.

5- R. Zhang, L. Song, Z. Han, and B. Jiao, " Physical layer security fortwo-way untrusted relaying with friendly jammers," IEEE Trans. Veh.Tech., vol. 61, no. 8, pp. 3693-3704, Aug. 2012.

6-Z. Ding, M. Xu, J. Lu, and F. Liu, " Improving wireless security forbidirectional communication scenarios," IEEE Trans. Veh. Tech., vol.61, no. 6, pp. 2842-2848, Jun. 2012.

7- Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis for opportunistic relaying", IEEE Transactions on Vehicular Technology, vol. 63, no. 6, pp. 2653-2661, July 2014.

8- N. Nesa and I. Banerjee ,"A Lightweight Security Protocol for IoT Using Merkle Hash Tree and Chaotic Cryptography", Advanced Computing and Systems for Security, 3-16,2020.

9- S. Sushil; C. Sanjeev; S. Aravendra;V.Sundaram Vats ," Threshold Cryptography Based Data Security in Cloud Computing" IEEE International Conference on Computational Intelligence & Communication Technology, April,2015.

10 S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay" ,Crypto key generation using contour graphalgorithm " in Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications Innsbruck, Austria ACTA Press, 95-98,2006