Cryptography by Using Hosoya Polynomials for Graphs Groups of Integer Modulen and Dihedral Groups with Immersion Property

Awni M.Gaftan
awnijeh@yahoo.com
Akram S. Mohammed
akr_tel@tu.edu.iq
Osama H. Subhi
osama.hameed67@gmail.com
Department of Mathematics, College of Computer Science and Mathematics, University of Tikrit, Iraq.

Received 15 May 2018, Accepted 1 July 2018, Published December 2018

Abstract

In this paper we used Hosoya polynomial ofgroupgraphs $Z_{1},...,Z_{26}$ after representing each group as graph and using Dihedral group to encrypt the plain texts with the immersion property which provided Hosoya polynomial to immerse the cipher text in another cipher text to become very difficult to solve.

Keywords: Hosoya polynomials,Dihedral groups,Cryptography,Encryption processes , Decryption processes.

1. Introduction

In modern times, cryptography is an important science in algebra and graph theory, where many articles linked in this side, In 2014, Natalia tokareva [1] linked the graph theory and cryptography, with conclusion good results [2]. Thomas Risse studied this concept and gave some important example, Simon Richard, Carlos Cid and Ciaran Mullan in [3], presented and studied of group theoryand cryptography where they get good results.

The main goal of cryptography is to secure and save important messages by special methods that cannot be easily identified.

The second partsuggested The first part is the basic concepts. This paper includes three parts algorithm of the method.

The third part is the application method.

2. Basic Concepts

In this section, we will provide some basic concepts known

Definition1 [4]

Let $(Z_n ,+_n)$ be a group of integers module n ,then the graph of Z_n consists of the elements of Z_n as avertices ,while the edges for any two distinict vertices a,b would be adjcent if $a+_nb =e$ and the element 0 associated with all elements of Z_n.

e is the identity element of the groups Z_n.

Example 2

If we take the group (Z_8 ,$+_8$) then the graph of this group is:

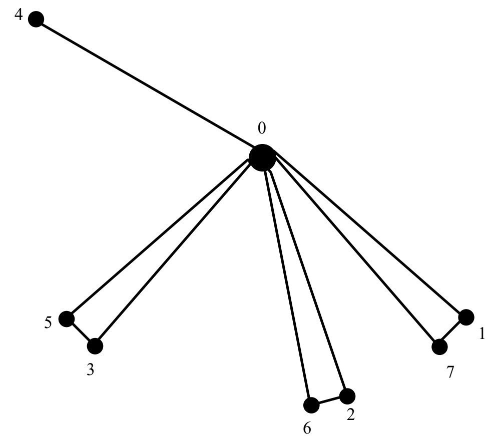


Figure 1. Neutral Graph of Z_8

Definition 3[5]

Let G be a graph, then the Hosoya polynomial of G is

$$H(G,X)=\sum_{k=0}^{diam(G)} d(G\ ,\ k)X^k$$

Where d(G,k) is the number of vertices pairs at distance k , k≥0 , dim(G) is the diameter of the geaph G and X is the guide of the polynomial.

Example 4

If we take the group (Z_5 ,$+_5$) then the simple graph of this group is

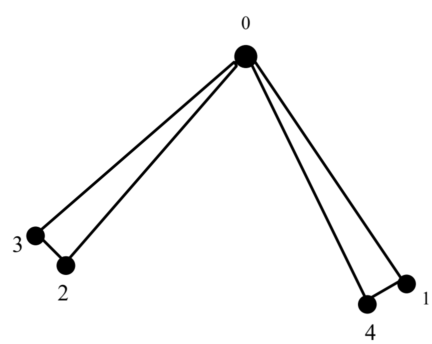


Figure 2. Neutral Graph of Z_5

and the hosoya polynomial of this graph is $5+6X+4X^2$

https://doi.org/10.30526/ 31.3.2008 Vol. 31 (3) 2018

Definition 5 [6]

The set has the form $D_n= \{a^{\circ} , a , a^2 , \dots , a^{n-1} , b , ba , ba^2 ,\dots, ba^{n-1} \}$ is called the dihedral group with order 2n, a, b the elements of this group.

Definition 6 [7]

Cryptographyis the scientific and practical activity associated with developing of cryptographic security facilities of information and also with argumentation of their cryptographic resistance .

Definition 7 [7]

Encryption is the process of disguising a message in such a way as to hide its substance (the process of change the plaintext into cipher text by virtue of cipher) .

Definition 8 [7]

Decryption is the process of turning a cipher text into the plain text .

Definition 9 [8]

Let $V=\begin{bmatrix} 1k \\ 2k \\ . \\ . \\ . \\ 1-nk \\ nk \end{bmatrix}$ be a vector , then the adverse of V is $V^R =\begin{bmatrix} kn \\ kn-1 \\ . \\ . \\ . \\ k2 \\ k1 \end{bmatrix}$

Definition 10 [8]

Be a vector and let W_k be an element in W , Let $W =\begin{bmatrix} W0 \\ W1 \\ . \\ . \\ . \\ Wn-1 \end{bmatrix}$

Then the adverse of $W_k$is $W_k^R=W_{n-1-k}$

2.1. The Suggested Algorithm

In this section we introduce two algorithms, the first is algorithm of encryption process and the second is algorithm of decryption process

Note 11

We consider the blank is character, that is the alphabet is 27 letters and we used the function (mod 28).

i- algorithm of encryption process

1 – Converts each letter with corresponding groups $Z_1,Z_2,\dots,Z_{26}$.

2-Representing each groups $Z_1,Z_2,\dots,Z_{26}$ as a graph.

3-Extraction of Hosoya polynomial for all groups graphs.

https://doi.org/10.30526/ 31.3.2008 Vol. 31 (3) 2018

4–Take positive integer number n .

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

$$W=\begin{bmatrix} W1 \\ W2 \\ . \\ . \\ . \\ W2n \end{bmatrix}=\begin{bmatrix} \boldsymbol{U} \\ \boldsymbol{V} \end{bmatrix} \quad \text{Where } U=\begin{bmatrix} W1 \\ W2 \\ . \\ . \\ . \\ Wn \end{bmatrix} \quad \text{and } V=\begin{bmatrix} Wn+1 \\ . \\ . \\ . \\ W2n \end{bmatrix}$$

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

$$D_n w=\begin{bmatrix} (x^k \ \ u_{k+1}) & mod\ 28 \\ (yx^k \ \ v_{k+1})^R & mod\ 28 \end{bmatrix} \qquad k=0,1\ldots n-1.$$

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

7-To improve this method we must encryption the first letter because the first letter by using this method stay the same letter always then we encryption the first letter by this equation $c_i = w_i+(2*n) \bmod 28$

ii- Algorithm of Decryption Process

First decryption the first letter by the Equation (1)**:**

$w_1=c_1-(2*n) \bmod 28$

2- For other letter using:

$$D_n C=\begin{bmatrix} (x^{-k}\ u_{k+1}) & mod\ 28 \\ (yx^{-k} v_{k+1}) & mod\ 28 \end{bmatrix} \ k=0,1\ldots n-1$$

Note 12

If the number 0 appears, then it always takes the code #:

Note 13

After the decryption, we always take the first letter and then we cancel two letters after it and take the fourth letter and cancel two letters after it and so on because the clear text is immersed in another text.

3. Application Method

Now, we apply the above method in two examples.

Example 14

Take the plain text (**college**)

1- Encryption

We converts each letter with corresponding groups $Z_1, Z_2, \ldots, Z_{26}$ and representing this groups as graphs and extract hosoya polynomaial for all this graphs

- C→ Z_3, and the graph of this

group is

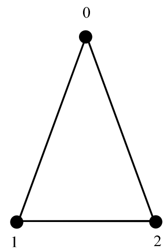


Figure 3. Neutral Graph of Z_3

and the hosoya polynomail of this graph is $(3+3X+0X^2)$

- O→Z_{15}, and the graph of this group is

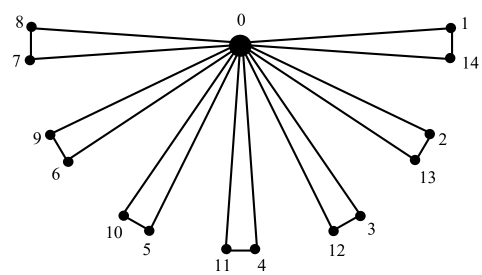


Figure 4. Neutral Graph of Z_{15}

and the hosoya polynomail of this graph is $(15+18X+84X^2)$

and for all letters we will get

c→ $(3+3X+0X^2)$

o→ $(15+18X+84X^2)$

l→ $(12+16X+50X^2)$

e→$(5+6X+4X^2)$

g→ $(7+9X+12X^2)$

Now let $n=2$, $D_{2n} = D_4 =\{ a^{\circ}, a , b , ab \}$

Then {college}→ {coll} + {ege_}

$$\{\text{coll}\} \to w_1 = \begin{bmatrix} 3 \\ 15 \\ 12 \\ 12 \end{bmatrix} = \begin{bmatrix} U \\ V \end{bmatrix} \qquad \text{where } U=\begin{bmatrix} 3 \\ 15 \end{bmatrix} \text{ and } V=\begin{bmatrix} 12 \\ 12 \end{bmatrix}$$

$$D_1w_1 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 3 & 3 & 0 \\ 15 & 18 & 84 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 12 & 16 & 50 \\ 12 & 16 & 50 \end{bmatrix}\right)^R \end{bmatrix} \pmod{28}$$

$$= \begin{bmatrix} \begin{bmatrix} 3 & 4 & 1 \\ 16 & 19 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 12 & 17 & 23 \\ 13 & 17 & 23 \end{bmatrix}\right)^R \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 3 & 4 & 1 \\ 16 & 19 & 1 \end{bmatrix} \\ \begin{bmatrix} 16 & 11 & 5 \\ 15 & 11 & 5 \end{bmatrix} \end{bmatrix}$$

CDAPSAPKEOKE

The first letter C→3→3+4=7→G

C_1→ "GDAPSAPKEOKE"

$$\{\text{ege\_}\} \to W_2 = \begin{bmatrix} 5 \\ 7 \\ 5 \\ 27 \end{bmatrix} = \begin{bmatrix} J \\ K \end{bmatrix} \qquad \text{where } J=\begin{bmatrix} 5 \\ 7 \end{bmatrix} \text{ and } K=\begin{bmatrix} 5 \\ 27 \end{bmatrix}$$

$$D_1w_1 = \begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 4 \\ 7 & 9 & 12 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 4 \\ 27 & 0 & 0 \end{bmatrix}\right)^R \end{bmatrix} \pmod{28}$$

$$= \begin{bmatrix} \begin{bmatrix} 5 & 7 & 5 \\ 8 & 10 & 13 \end{bmatrix} \\ \left(\begin{bmatrix} 5 & 7 & 5 \\ 0 & 1 & 1 \end{bmatrix}\right)^R \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 5 & 7 & 5 \\ 8 & 10 & 13 \end{bmatrix} \\ \begin{bmatrix} 23 & 21 & 23 \\ 0 & 27 & 27 \end{bmatrix} \end{bmatrix}$$

EGEGJMWUW#_ _ The first letter E→5→5+4=9→I
C_2→"IGEHJMWUW#_ _"
Then the cipher text is:
C→"GDAPSAPKEOKEIGEHJMWUW#_ _"

2-Decryption

Notice that
C_1→″GDAPSAPKEOKE ″
The first letter G→7→7-4=3→C

$$D_1C_1 = D_n = \begin{bmatrix} \begin{bmatrix} 3 & 4 & 1 \\ 16 & 19 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 16 & 11 & 5 \\ 15 & 11 & 5 \end{bmatrix}\right)^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{bmatrix} \pmod{28}$$

$$= \begin{bmatrix} \begin{bmatrix} 3 & 3 & 0 \\ 15 & 18 & 0 \end{bmatrix} \\ \begin{bmatrix} 12 & 16 & 22 \\ 12 & 16 & 22 \end{bmatrix} \end{bmatrix}$$

CC#***O***R#***L***PV***L***PV

C_2→"IGEHJMWUW#_ _"

The first letter I→9→9-4=5→E

$$D_2C_2 = D_n = \begin{bmatrix} \begin{bmatrix} 5 & 7 & 5 \\ 8 & 10 & 13 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 23 & 21 & 23 \\ 0 & 27 & 27 \end{bmatrix}\right)^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{bmatrix} \pmod{28}$$

$$= \begin{bmatrix} \begin{bmatrix} 5 & 6 & 4 \\ 7 & 9 & 12 \end{bmatrix} \\ \begin{bmatrix} 5 & 6 & 4 \\ 27 & 0 & 0 \end{bmatrix} \end{bmatrix}$$

EFD***G***IL***E***FD_##

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

Example 15

If we encryption the text (college of computer science and mathematics) by the same technique with choose n=3 then we will get
P→"college of computer science and mathematics"

C→"IDAPVAMQWPKEVUWTROKGEPVAGHIYX_LGENJMKGEPVAGHIYX_LGENJ M IDAJMYFGENHKXX_VUWGAAOTQEECOIWZ_ _G_ENKSFGENSE_ _ _G_EROC CDAT#E#AAA_ _#_ _#_ _"

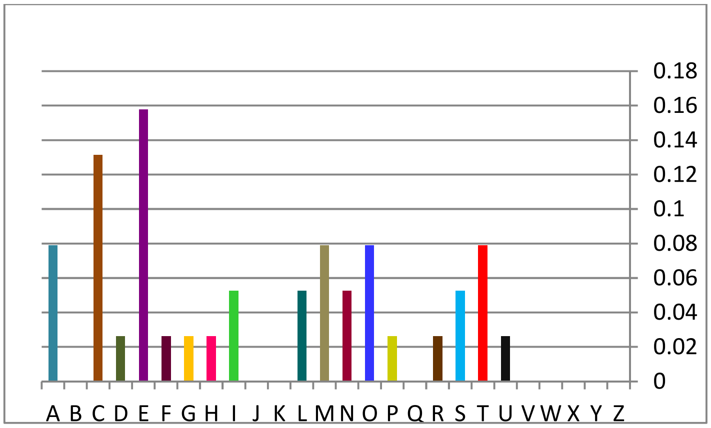
Now we find a table of ratios of letters and a statistical scheme of plan text and cipher text and try to compare these two texts

For plan text

Table 1. The ratio of plan text characters

A	B	C	D	E	F	G
0.07894737	0	0.13157895	0.02631579	0.15789474	0.02631579	0.02631579
H	**I**	**J**	**K**	**L**	**M**	**N**
0.02631579	0.05263158	0	0	0.05263158	0.07894737	0.05263158
O	**P**	**Q**	**R**	**S**	**T**	**U**
0.07894737	0.02631579	0	0.02631579	0.05263158	0.07894737	0.02631579
V	**W**	**X**	**Y**	**Z**		
0	0	0	0	0		

And the statistical scheme



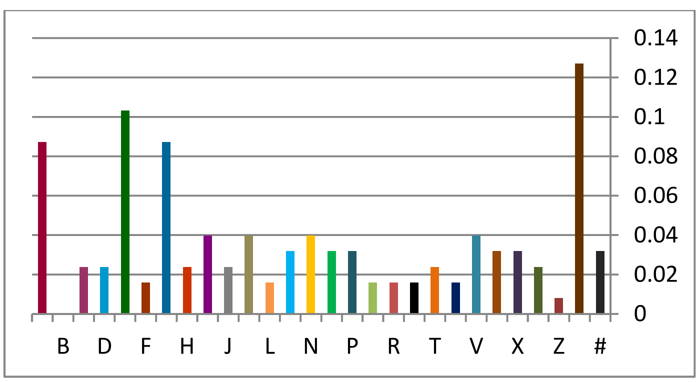
Scheme 1. Histogram of Plan Text

For cipher text

Table 2. The Ratio of Cipher Text Characters

A	B	C	D	E	F	G
0.08730159	0	0.02380952	0.02380952	0.1031746	0.01587302	0.08730159
H	**I**	**J**	**K**	**L**	**M**	**N**
0.02380952	0.03968254	0.02380952	0.03968254	0.01587302	0.03174603	0.03968254
O	**P**	**Q**	**R**	**S**	**T**	**U**
0.03174603	0.03174603	0.01587302	0.01587302	0.01587302	0.02380952	0.01587302
V	**W**	**X**	**Y**	**Z**	**_**	**#**
0.03968254	0.03174603	0.03174603	0.02380952	0.00793651	0.12698413	0.03174603

And the statistical scheme



Scheme 2. Histogram of Cipher Text

Now to compare these percentages we give some observations

1-Notice that the clear text consists of 38 characters while the encrypted text consists of 126 characters this means that each letter of clear text corresponds to three letters of the encryption text and this is the immersion property we mentioned.

2-Notice in the statistical scheme of the encryption text that almost all alphabets were used as well as the symbols added to the alphabet, whereas in the plan text there are nine non-existent characters.

https://doi.org/10.30526/ 31.3.2008 Vol. 31 (3) 2018

3-Notice that the highest ratio of letters or symbols in the encoded text is the ratio of the symbol _ which has been added to the alphabet which does not represent any letter of the clear text and this indicates that this code added to the alphabet has increased the strength of encryption significantly.

References

1. Natalia, T. *Connections between graph theory and Cryptography*. G2C2: Graphs and Groups, Cycles and Coverings; 24–26, Novosibirsk, Russia. 2014.
2. Thomas, R.*Cryptography and Graph theory two Examples of DiscreteMathematics SAGA*. HSB university of applied sciences. 2011.
3. Simon, R.; Carlos, C.; Ciaran, M. *Group theory and Cryptography*. university of London. 2010**.**
4. Vasantha, K. W. B; Florentins,S.*Groups As Graphs*,Editura CuArt, Slatina,Judctul olt, Romania, 2009.
5. Ali, A.M. *Wiener polynomial of Generalized Distance in graph*. Mosuluniversity. 2005.
6. Edwin, C. *Elementary Abstract Algebra*. university of south Florida, 2001.
7. Hans, D.; Helmut, K. *Introduction to Cryptography,Principles and application*. second edition, verlay Berlin Heidelberg, 2007.
8. David, C.; Tom, D.; Rohit, T. ; Andrew, W. *Linear Algebra* . Davis California. 2013.