Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Dihedral Cryptographic Technique

Zainab Fahad Mhawes

Al-Qadisiya university-College of education-Department of Mathematics

zainab.alnaseri@qu.edu.iq

Recived : 16\10\2017 **Revised : 30\10\2017** **Accepted : 6\12\2017**

Available online : 21/1/2018

DOI: 10.29304/jqcm.2018.10.1.337

Abstract:

This paper focuses on a new technique of cryptography in abstract algebra. We first give the necessary review on Dihedral group and cryptography .We definition a new alphabetic of characters by additive character "blank" ,thus we have (27) characters {26 letters and "blank" },therefore we use modular 27 instead 26 such that we use the reflection and rotation which exists in Dihedral group to change the arrange of vectors of characters in plain text.

Keywords : Dihedral group, Cryptography ,Caesar Cipher ,Encryption Processes, Decryption processes.

Mathematics Subject Classification: 68P25

Introduction: Cryptography is one of the most important applications of algebra and number theory where the process is to change important information to another unclear one . The main goal of cryptography is to keep the integrity and security of this information there are many types of Cryptography techniques and we will try to consider some of them in this paper .

This paper consists of three paragraphs ,where one includes some necessary definitions on dihedral groups . In second, we defined some necessary definitions on Cryptography. Third includes a suggested technique and some example and analysis of this technique . The programs of this paper write by using V.B. language .

1. Preliminary definitions in algebra:

1.1 Definition [4]:

We say that $*: S \times S \rightarrow S$, which defined by $(x,y) \rightarrow x$ is a binary opration on a nonempty set S if it is map .

1.2 Definition[5]:

A group $(G,*)$ is a nonempty set G with a binary operation * such that the following conditions are hold:

(i) $(x* y)* z= x* (y* z)$, for all $x,y,z \in G$

(ii) There exists an element e such that:

$$x * e = x = e * x \text{ , for all } x \in G,$$

(iii) For all $x \in G$ there is an element x^{-1} in G such that:

$$x^{-1} * x = e = x * x^{-1}.$$

1.3 Definition[4]:

The set $D_n = \{r^0, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$ is called the dihedral group and has order 2n with property $sr = r^{-1}s$.

1.4 Remarks[4]:

$r^n = r^0$, $s^2 = r^0$

2. Preliminary definitions in Cryptography:

2.1 Definition[3]:

Encryption is the process of changing the text of the content (data) to the symbols and Numbers are difficult to understand using the many and varied mathematical algorithms .

2.2 Goals of Cryptography [1]:

- Data privacy (confidentiality).
- Data Authenticity (it came from where it claim).
- Data integrity(it has not been modified on the way) in the digital world.

2.3 The fundamental objects of Cryptography [2]:

- Plaint text is the original data.
- Cipher text is the message changed by using some algorithms .
- Encryption is the processes which are changing the plaintext to cipher text.
- Decryption is the processes which are changing the cipher text to plaintext.

2.4 Definition [4]:

Let $A=\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{bmatrix}$ be a vector then the cryptography transpose (CT) of A is

$$A^{CT} = \begin{bmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_2 \\ a_1 \end{bmatrix}$$

We will introduce a new term in the following definition, that is the transpose of element.

2.5 Definition:

Let $A=\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ . \\ a_{n-1} \end{bmatrix}$ be a vector and a_k be an element of A, then the transport of a_k is $(a_k)^T=a_{(n-1)}-k$

We will define a new operation in the following definition, which it very import in our paper.

2.6 Definition:

Let D_n=$\{r^0,r,\ldots\ldots,r^{n-1},s,sr,\ldots\ldots,sr^{n-1}\}$ be a dihedral group then we can define the new operation :

$r^k a$=a+k mod 27

$r^{-k} a$=a-k mod 27

sa=a^T mod 27

$sr^k a$=$(a+k)^T$ mod 27

3. The suggested algorithm :

Here we consider the blank is character , i.e the alphabet is 27 chars .

i- Encryption process :

1- Take positive integer number n .

2- Construction Dihedral group D_n .

3- Cut block of plain text with length 2n character as :

$$P=\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ . \\ p_{2n} \end{bmatrix}=\begin{bmatrix} A \\ B \end{bmatrix} \quad ,A=\begin{bmatrix} p_1 \\ . \\ \vdots \\ . \\ p_n \end{bmatrix}, \mathbf{B}=\begin{bmatrix} p_{n+1} \\ . \\ \vdots \\ . \\ p_{2n} \end{bmatrix}$$

4- Apply the Dihedral operations (r,s):

$$D_n p=\begin{bmatrix} (r^k a_{k+1})\ mod27 \\ (sr^k b_{k+1})\ mod27 \end{bmatrix} \quad , k=0,1,\ldots,n-1$$

$$DnP=\begin{bmatrix} \left(\begin{bmatrix} 0 \\ 1 \\ \vdots \\ n-2 \\ n-1 \end{bmatrix}+\begin{bmatrix} p_1 \\ . \\ \vdots \\ . \\ p_n \end{bmatrix}\right) mod27 \\ \left(\begin{bmatrix} 0 \\ 1 \\ \vdots \\ n-2 \\ n-1 \end{bmatrix}+\begin{bmatrix} p_{n+1} \\ . \\ \vdots \\ . \\ p_{2n} \end{bmatrix}\right)^T mod27 \end{bmatrix}$$

For enhanced this technical we must encryption the first letter of plaintext because the first letter by using this technical stay the same letter always.

Encryption the first letter

$C_1=p_1+(2*n)$ mod 27

ii) Decryption process:

$P_i=C_i-(2*n)$ mod 27

$$D_nC=\begin{bmatrix} (r^{-k} a_{k+1})\ mod27 \\ (r^{-k} sB_{k+1}^T)\ mod27 \end{bmatrix}$$

3.1 Example:

Take plain text="hello"

Encryption by using Dihedral Cryptographic Technique

Solution

1- **Encrption**

Let n=2

$D_n=D_2=\{r^0,r,s,sr\},|D_2|=4$

Hello={Hell}+{o_ _ _}

"Hell"→$P_1=\begin{bmatrix}7\\4\\11\\11\end{bmatrix}=\begin{bmatrix}A\\B\end{bmatrix}$, $A=\begin{bmatrix}7\\4\end{bmatrix}$

, $B=\begin{bmatrix}11\\11\end{bmatrix}$

$$D_1P_1=\begin{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}7\\4\end{bmatrix}\\ (\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}11\\11\end{bmatrix})^T\end{bmatrix}=$$

$$\begin{bmatrix}\begin{bmatrix}7\\5\end{bmatrix}\\ (\begin{bmatrix}11\\12\end{bmatrix})^T\end{bmatrix}=\begin{bmatrix}\begin{bmatrix}7\\5\end{bmatrix}\\ \begin{bmatrix}15\\14\end{bmatrix}\end{bmatrix}=\begin{bmatrix}7\\5\\15\\14\end{bmatrix}\rightarrow HFPO=C_1$$

The first letter:

H →7 → 7+4=11→ L

"O"→"O---"→$P_2\rightarrow\begin{bmatrix}14\\26\\26\\26\end{bmatrix}\rightarrow\begin{bmatrix}\begin{bmatrix}14\\26\end{bmatrix}\\ \begin{bmatrix}26\\26\end{bmatrix}\end{bmatrix}$

$$D_2P_2=\begin{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}14\\26\end{bmatrix}\\ (\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}26\\26\end{bmatrix})^T\end{bmatrix}=$$

$$\begin{bmatrix}\begin{bmatrix}14\\0\end{bmatrix}\\ (\begin{bmatrix}26\\0\end{bmatrix})^T\end{bmatrix}=\begin{bmatrix}14\\0\\0\\26\end{bmatrix}\rightarrow C_2=OAA-$$

Then

O→14→14+4=18→S

P="Hello"→C="LFPOSAA-"

2-Decryption :

C=" LFPOSAA-"

C_1="LFPO" ,C_2="SAA-"

C_1:

L → 11-4=7 →H

$$D_2C_1=D_n=\begin{bmatrix}\begin{bmatrix}7\\5\end{bmatrix}\\ \begin{bmatrix}15\\14\end{bmatrix}\end{bmatrix}=$$

$$\begin{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}7\\5\end{bmatrix}\\ -\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}15\\14\end{bmatrix}^T\end{bmatrix}=$$

$$\begin{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}7\\5\end{bmatrix}\\ -\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}11\\12\end{bmatrix}\end{bmatrix}=\begin{bmatrix}7\\4\\11\\11\end{bmatrix}$$

→"HELL"=P_1

C_2:

S→ 18-4=14→O

$$D_nC_2=D_n=\begin{bmatrix}\begin{bmatrix}14\\0\end{bmatrix}\\ \begin{bmatrix}0\\26\end{bmatrix}\end{bmatrix}=$$

$$\begin{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}14\\0\end{bmatrix}\\ -\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}0\\26\end{bmatrix}^T\end{bmatrix}=$$

$$\begin{bmatrix}-\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}14\\0\end{bmatrix}\\ -\begin{bmatrix}0\\1\end{bmatrix} & + & \begin{bmatrix}26\\0\end{bmatrix}\end{bmatrix}=\begin{bmatrix}14\\-1\\26\\-1\end{bmatrix}=\begin{bmatrix}14\\26\\26\\26\end{bmatrix}$$

→"O---"=P_2

Then p="Hello---"

3.2 Example:

Encryption the text:

College of education university of al Qadisiya

Solution:

P=" College of education university of al Qadisiya"

C=" GPPOIHW SGAVHVYZXJMMDVNRZFJHMU C SGAZPAKZHJIRBBA"

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.1 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

3.3 Example:

In example (3.1) and example (3.2) we take n=1, now we will change value of n and compare between them:

P="Hello"

n=1 → C=" LFPOSAA-"

n=100→C="
SFNOSEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJ"

n=10→C=" AFNOSEFGHIA ZYXWVUTS"

P=" College of education university of al Qadisiya"

n=1→C="GPPOIHW
SGAVHVYZXJMMDVNRZFJHMUC
SGAZPAKZHJIRBBA"

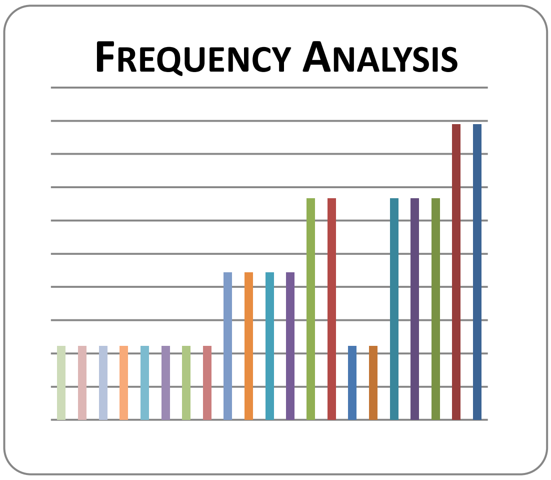
n=10→C="
WPNOILKGWOAVVDUVBLEETVPLZJXZ
QBC KSXVJUCRXJULBFFGHIA
ZYXWVUTS"

n=100→C="
NPNOILKGWOJPPGQPIZFFTOIESCQSJVA
DTLGIUJAMQWGYOSSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJIHGFEDCBA
ZYXWVUTSRQPONMLKJ"

We note that the complexity of cryptography increasing when the value n increasing.

3.4 Frequency analysis:

A	8.89%	P	6.67%	F	2.22%	W	2.22%
H	8.89%	J	6.67%	C	2.22%	X	2.22%
Z	8.89%	R	4.44%	K	2.22%		
V	6.67%	S	4.44%	U	2.22%		
G	6.67%	B	4.44%	D	2.22%		
M	6.67%	I	4.44%	Y	2.22%		
O	2.22%						
N	2.22%						



4. Conclusions:

1. The technique consists of an algebraic concept depends on recycling and displacement in forming the elements which led to the raising
Confidentiality and complexity level.

2. technical included some original ideas, whether in design or implementation making
Her privacy.

3. encryption keys used random and difficult to detect.

References

1- Alfred M. and paul v. ,A, Handbook of Applied Cryptography , CRC press ,2001.

2- Jonathan K. and Lindell Y., Introduction to modern Cryptography,CRC press, New york,2007 .

3- Neal K. ,A course in number theory and Cryptography , spinger , 1994 .

4-

5- Schneier B., Applied Cryptography ,John wiley and son press ,New York ,1996.

6- Thomas W.,Abstract algebra , Austin state university , 2010.

تقنية التشفير ثنائي السطوح

زينب فهد مهوس
جامعة القادسية - كلية التربية - قسم الرياضيات
zainab.alnaseri@qu.edu.iq

المستخلص :

يركز هذا البحث على تقنية جديدة في التشفير في الجبر المجرد. في البداية اعطينا عرض ضروري عن زمر السطوح الثنائية و التشفير. عرفنا ابجدية جديدة للرموز بأضافة "الفراغ" ، لذلك اصبح لدينا (٢٧) رمز (٢٦ رمز و الفراغ) ، لذلك استخدمنا معيار ٢٧ بدل ٢٦ حيث استخدمنا الانقلابات و التدوير الموجودة في زمرة السطوح الثنائية لتغيير ترتيب متجهات الرموز في لانص الصريح.