Journal of Engineering and Applied Sciences 14 (11): 3806-3812, 2019
ISSN: 1816-949X

Implementation Diffie-Hellman by Using Standard Groups and Hosoya-Polynomial to Generate a Matrix as Key Cryptosystem

[1]Awni M. Gaftan, [1]Akram S. Mohammed and [2]Osama H. Subhi
[1]Department of Mathematics, College of Computer Science and Mathematics,
[2]College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq

Abstract: In this study we used standard groups and Hosoya polynomial to implement Diffie-Hellman method to generate matrix key cryptosystem instead of the number which is generate as a key in this method. Also, we using Dihedral group with Hosoya polynomial for group graph to encrypt plain text and to decrypt cipher text and we produce the statistical table for the ratio to any letter in plain text and every letter in cipher text.

Key words: Hosoya polynomial, dihedral group, Diffie-Hellman, encryption processes, decryption processes, cipher text

INTRODUCTION

Many encryption methods require a key to encryption and decryption the texts, this key can be a number, a matrix or an symbol, one of the most important ways you need a key is the Hill cipher method. Many cryptologists have developed certain methods and algorithms to generate numbers or matrices that are considered keys to a process, Blom (1983) presented a study on how to create a cryptographic key using matrices and Rock (2005) presented a detailed study on how to generate random numbers used for the encryption process while Stinson (1995) presented a study on how to generate a number by two people based on the choice of positive random numbers by each person and using these numbers in certain equations with the mod function.

In this study, we will present a study to implement the Diffe-Hellman method to generate a matrix as a cryptographic key rather than a number by using Hosoya polynomial For standard groups graphs and matrices such that their elements are selected from standard groups and these polynomials and matrices are introduced into certain equations with the use of the mod function and we will present a study to use Hosoya polynomial and dihedral group with immersion property to encryption the texts. This study consists of four paragraphs. The first paragraph contains some basic concepts.

The second paragraph contains explains the Diffe-Hellman method with its own work steps and example. The third paragraph contains how to implement the Diffe-Hellmn method with improved work steps and example. The fourth paragraph contain the method of encryption by using Hosoya polynomial and dihedral group to encryption the texts.

Basic concepts In this paragraph, we introduce basic concepts that relate with these mothods.

Definition: The group of integer numbers with standard n writtn as:

$$Z_n = \{[0], [1], [2], ..., [n-1]\}, [n] = 0$$

Such that:

$$[a] = \{x \in Z / x = a (\text{mod } n)\} = \{x \in Z / x = a+kn, k \in Z\}$$

The operation $(+_n)$ which defined on Z_n as:

$$[a]+_n[b]=[a+b], \text{ for all } [a], [b] \in Z$$

Then, $(Z_n, +_n)$ is abelin and cyclic groups and its called standard groups Burton (1967). i.e., if we take n = 6, then $Z_{15} = \{0, 1, 2,..., 14\}$ and $(Z_{15},+_{15})$ is abelian and cyclic group.

Definition: Let, $(Z_n,+_n)$ be agroup, n = 1, 2, ..., then, the simple graph of Z_n consist of the elements of Z_n as avertices while the edges for any tow distinict vertices a, b be adjcent if $a+_nb = e$. Where e is the identity element of the groups Z_n (Kandasamy and Smarandache, 2009), i.e., if we take the group $(Z_{12},+_{12})$ then the simple graph of this group is (Fig. 1).

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

Corresponding Author: Emad Toma Karash, Northern Technical University, Mosel, Iraq

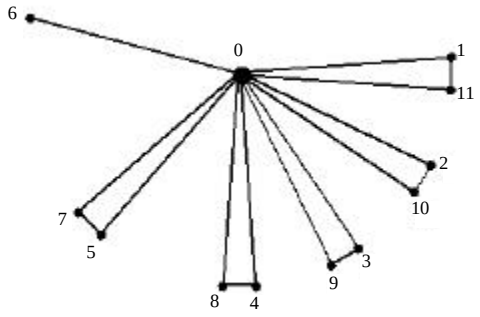

Fig. 1: The group $(Z_{12}, +_{12})$

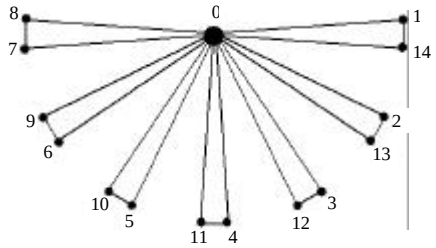

Fig. 2: The group $(Z_{15}, +_{15})$

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

where, d(G, k) is the number of vertices pairs at distance k and $k \geq 0$ (Ali, 2005).

Example: If we take the group $(Z_{15},+_{15})$ then, the simple graph of this group is and the Hosoya polynomial of this graph is $(15+21X+84X^2)$ (Fig. 2).

Definition: The set has the form "Dn = "$\{a^{\circ}, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$ is called the dihedral group with order 2n (Edwin, 2001).

Definition: Be avector, then the adverse of V is let:

$$V = [k1, k2, ..., kn\text{-}1\ kn]$$

Cherney *et al.* (2016):

$$V^R = [kn\ kn\text{-}1,..., k2\ k1]$$

Definition: Be a vector and let v_k be an element in V Let:

$$V = [v0\ v1, ...,vn\text{-}1]$$

then the adverse of "v_k is" $v_k^R = V_{n-1-k}$ "(Cherney *et al.*, 2016).

MATERIALS AND METHODS

Diffie-Hellman method: In this paragraph, we will study the Diffe-Hellman method of generating numbers which are considered as a cryptographic key and which depend on two users (Stinson, 1995) as shown in the work steps.

Work steps for Diffe-Hellman method: Work steps can be divided into four parts:

Part 1; Information for users A and B:
- Select positive integer $q \in Z^+$
- Determine the number p that will be used for the mod function

Part 2; For users A:
- Select a random number $m \in Z^+$
- Find the number a_u by using the following equation: $a_u = q^m \bmod p$
- Send the number au to user B

Part 3; For users B:
- Select a random number $n \in Z^+$
- Find the number b_u by using the following equation: $b_u = q^n \bmod p$
- Send the number b_u to user B

Part 4; For users A and B:
- User A generates the K_A key using the following equation: $K_A = (b_u \cdot q^m) \bmod p$
- User B generates the K_B key using the following equation: $K_B = (a_u \cdot q^n) \bmod p$

Where is the: same number is generated by user A.

Example; Users A and B: Let, p = 45 be q = 3.

User A:
- Choose a positive number m = 10
- Find the number au using the following equation:

$$a_u = q^m \bmod p$$

$a_u = 3^{10} \bmod 45 = 59049 \bmod 45 = 9$, This number is sent to user B

User B:
- Choose a positive number n = 7
- Find the number bu using the following equation:

$b_u = q^n \bmod p$ $b_u = 3^7 \bmod 45 = 2187 \bmod 45 = 27$

Users A and B: User A generates the K_A key using the following equation:

$$K_A = (b_u \cdot q^m) \bmod p$$
$$= (27 \cdot 59049) \bmod 45$$
$$= (1594323) \bmod 45 = 18$$

User B generates the K_B key using the following equation:

$$K_B = (a_u \cdot q^n) \bmod p$$
$$= (9 \cdot 2187) \bmod 45$$
$$= 19683 \bmod 45 = 18$$

And it is the same number generated by the user A that can be used as a key for encryption.

Implement the Diffie-Hellman method using standard groups and Hosoya polynomials to generate a matrix as a cryptographic key: Now, in this paragraph we will apply the Diffie-Hellman method by using Hosoya polynomial and standard groups to generate a matrix that is considered as a cryptographic key rather than a number which also depends on two users and according to the work steps.

Work steps (modified): Work steps can be divided into four parts.

Part 1: Information for users A and B:

- Choose positive integers numbers m, $n \in Z^+$
- Choose the two matrixes a, $b \in M_{n \times n}(Z_n)$
- Choose the number N to use the mod function on this number

Part 2: For users A:

- Choose Hosoya polynomial f(x) randomly for one of the standard groups graphs such that satisfy (f(a)) mod $N \neq 0$
- If (f (a)) mod $N \neq 0$ then, f(a) is considered a secret key
- Find the public key X_A according to the following equation:

$$X_A = [(f(a))^m \cdot b \cdot (f(a))^n] \bmod N$$

- Send the key X_A to user B

Part 3: For users B:

- Choose Hosoya polynomial h(x) randomly for one of the standard groups graphs such that satisfy (h (a)) mod $N \neq 0$
- If (h (a)) mod $N \neq 0$ then h(a) is considered a secret key
- Find the public key X_B according to the following equation:

$$X_B = [(h(a)^m . b . (h(a))^n] \bmod N$$

- Send the key X_B to user A

Part 4: For users A and B:

- User A generates the matrix key K_A by using the following equation:

$$K_A = [(f(a))^m \cdot X_B \cdot (f(a))^n] \bmod N$$

- User B generates the matrix key K_B by using the following equation:

$$K_B = [(h(a))^m \cdot X_A \cdot (h(a))^n] \bmod N$$

Which is the same as the matrix generated by User A.

Example: Users A and B:

- Let $2, 3 \in Z^+$
- Let:

$$a = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}, b = \begin{bmatrix} 5 & 8 \\ 9 & 4 \end{bmatrix}$$

a, $b \in M_{2\times 2}(Z_{10})$ such that

- Let N = 33

User A: Choose Hosoya polynomial of the group graph Z_5 which is:

$$f(x) = 4x2+6x+5$$

Find (f(a))modN and check that (f(a)) mod $N \neq 0$ as:

$$f(a) = \left(4\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}^2 + 6\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} + 5I\right) \bmod 33 =$$
$$\left(\begin{bmatrix} 28 & 31 \\ 30 & 22 \end{bmatrix} + \begin{bmatrix} 6 & 12 \\ 18 & 9 \end{bmatrix} + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}\right) \bmod 33 = \begin{bmatrix} 6 & 10 \\ 15 & 3 \end{bmatrix}$$

$\therefore$(f(a)) mod $N \neq 0$. Find the key X_A according to the following equation:

$$X_A = [(f(a))^m \cdot b \cdot (f(a))n] \bmod N =$$

$$\left(\begin{bmatrix}6 & 10\\ 15 & 3\end{bmatrix}^2 \cdot \begin{bmatrix}5 & 8\\ 9 & 4\end{bmatrix} \cdot \begin{bmatrix}6 & 10\\ 15 & 3\end{bmatrix}\right) \bmod 33 =$$

$$\left(\begin{bmatrix}21 & 24\\ 3 & 27\end{bmatrix} \cdot \begin{bmatrix}5 & 8\\ 9 & 4\end{bmatrix} \cdot \begin{bmatrix}24 & 18\\ 27 & 12\end{bmatrix}\right) \bmod 33 = \begin{bmatrix}15 & 3\\ 21 & 24\end{bmatrix}$$

Send the key X_A to user B.

User B: Choose Hosoya polynomial of the group graph Z_{10} which is: $h(x) = 32x^2+13x+10$. Find $(h(a))\bmod N$ and check that $(h(a)) \bmod N \neq 0$ as:

$$h(a) = \left(32\begin{bmatrix}1 & 2\\ 3 & 7\end{bmatrix}^2 + 13\begin{bmatrix}1 & 2\\ 3 & 7\end{bmatrix} + 10\,I\right) \bmod 33 =$$

$$\left(\begin{bmatrix}26 & 17\\ 9 & 11\end{bmatrix} + \begin{bmatrix}13 & 26\\ 6 & 25\end{bmatrix} + \begin{bmatrix}10 & 0\\ 0 & 10\end{bmatrix}\right) \bmod 33 =$$

$$\begin{bmatrix}16 & 10\\ 15 & 13\end{bmatrix}$$

$\therefore (h(a)) \bmod N \neq 0$. Find the key X_B according to the following equation:

$$X_B = [(h(a))^m \cdot b\cdot] \bmod N \left(h\left(a\right)\right)N$$

Send the key X_B to user A.

Users A and B: User A generates the matrix key K_A by using the following equation:

$$K_A = [(f(a))^m \cdot X_B \cdot (f(a))^n] \bmod N =$$

$$\left(\begin{bmatrix}6 & 10\\ 15 & 3\end{bmatrix}^2 \cdot \begin{bmatrix}20 & 22\\ 21 & 4\end{bmatrix} \cdot \begin{bmatrix}6 & 10\\ 15 & 3\end{bmatrix}^3\right) \bmod 33 =$$

$$\left(\begin{bmatrix}21 & 24\\ 3 & 27\end{bmatrix} \cdot \begin{bmatrix}20 & 22\\ 21 & 4\end{bmatrix} \cdot \begin{bmatrix}24 & 18\\ 27 & 12\end{bmatrix}\right) \bmod 33 =$$

$$\begin{bmatrix}18 & 30\\ 12 & 9\end{bmatrix}$$

User B generates the matrix key K_B by using the following equation:

$$K_B = [(h(a))^m \cdot X_A \cdot (h(a))^n] \bmod N =$$

$$\left(\begin{bmatrix}16 & 10\\ 15 & 13\end{bmatrix}^2 \cdot \begin{bmatrix}15 & 3\\ 21 & 24\end{bmatrix} \cdot \begin{bmatrix}16 & 10\\ 15 & 13\end{bmatrix}^3\right) \bmod 33 =$$

$$\left(\begin{bmatrix}10 & 26\\ 6 & 22\end{bmatrix} \cdot \begin{bmatrix}15 & 3\\ 21 & 24\end{bmatrix} \cdot \begin{bmatrix}22 & 9\\ 30 & 16\end{bmatrix}\right) \bmod 33 =$$

$$\begin{bmatrix}18 & 30\\ 12 & 9\end{bmatrix}$$

Which is the same as the matrix generated by user A. Now, we have a key matrix that can be used to encrypt HILL or other methods.

Using Hosoya polynomial fpr standard groups graphs and dihedral group to encryption the texts and decryption the cipher texts: In this paragraph we will discuss how to use Hosoya polynomial of the standard groups graphs and the dihedral group to encrypt texts and decrypt cipher text, in the first example we will encrypted a word and In the second example we will encrypted a statement with a table of ratio of letters in plan text and cipher text with statistical schemas.

The suggested algorithm: We will introduce two algorithms, the first one is algorithm of encryption process and the second is algorithm of decryption process.

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

Algorithm of encryption process:

- Converts each letter with corresponding standard groups $Z_1, Z_2, ..., Z_{26}$.
- Representing each standard groups $Z_1, Z_2, ..., Z_{26}$ as a graph
- Extraction Hosoya polynomial for all standard group graph
- Take positive integer number n
- Divide the text with length 2n by using dihedral group as:

$$W = \begin{bmatrix}W1\\ W2\\ .\\ .\\ .\\ W2n\end{bmatrix} = \begin{bmatrix}U\\ V\end{bmatrix} \text{ Where } U = \begin{bmatrix}W1\\ W2\\ .\\ .\\ .\\ Wn\end{bmatrix}$$

$$V = \begin{bmatrix}Wn+1\\ .\\ .\\ .\\ W2n\end{bmatrix}$$

apply the dihedral operations (x, y):

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

$$D_n w = \left[\left[\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ . & . & . \\ . & . & . \\ . & . & . \\ n\text{-}1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} \text{Hosoya polynomial} \\ \text{of } Z_i \text{ vectors} \end{bmatrix} \right] = \left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ . & . & . \\ . & . & . \\ . & . & . \\ n\text{-}1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} \text{Hosoya polynomial} \\ \text{of } Z_i \text{ vectors} \end{bmatrix} \right)^R \right]$$

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:

$$c_i = w_i + (2*n) \bmod 28$$

Algorithm of decryption process: First decryption the first letter by the equation:

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

For other letter using:

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

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

Note: 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.

RESULTS AND DISCUSSION

Example: Take the plain text (college).

Encryption: We Converts each letter with corresponding standard groups Z_1, Z_2, ..., Z_{26} and representing this groups as graphs and extract Hosoya polynomaial for all this graphs - $C \rightarrow Z_3$ and the graph of this group is and the hosoya polynomail of this graph is $(3+3X+0X^2)$-$O \rightarrow Z_{15}$ and the graph of this group is and the hosoya polynomail of this graph is $(15+18X+84X^2)$ and for all letters we will get (Fig. 3 and 4):

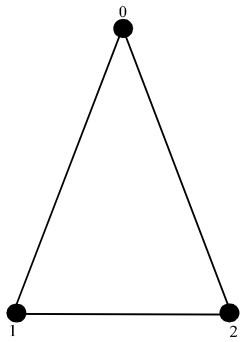

Fig. 3: The Hosoya polynomail

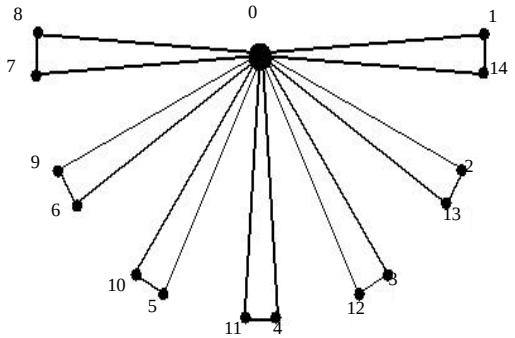

Fig. 4: Graph is $(15+18X+84X^2)$

$$c \rightarrow (3+3X+0X^2)$$
$$o \rightarrow (15+18X+84X^2)$$
$$l \rightarrow (12+16X+50X^2)$$
$$e \rightarrow (5+6X+4X^2)$$
$$g \rightarrow (7+9X+12X^2)$$

Now, let n = 2, $D_{2n} = D_4 = \{r^\circ, r, s, rs\}$. Then, {college} → {coll} + {ege_}. Where:

$$U = \begin{bmatrix} 3 \\ 15 \end{bmatrix} \text{ and } V = \begin{bmatrix} 12 \\ 12 \end{bmatrix}$$

$$\{coll\} \rightarrow w_1 = \begin{bmatrix} 3 \\ 15 \\ 12 \\ 12 \end{bmatrix} = \begin{bmatrix} U \\ V \end{bmatrix}$$

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

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

CDAPSAPKEOKE: The first letter C→3→3+4 = 7→G

$$C_1 \rightarrow \text{"GDAPSAPKEOKE"}$$

Where:

$$J = \begin{bmatrix} 5 \\ 7 \end{bmatrix} \text{ and } K = \begin{bmatrix} 5 \\ 27 \end{bmatrix}$$

$$\{ege\_\} \rightarrow W2 = \begin{bmatrix} 5 \\ 7 \\ 5 \\ 27 \end{bmatrix} \begin{bmatrix} J \\ K \end{bmatrix} D_1w_1 \pmod{28} =$$

$$\begin{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 4 \\ 7 & 19 & 12 \end{bmatrix} \\ \left(\left(\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 4 \\ 27 & 0 & 0 \end{bmatrix} \right)^R \right) \end{bmatrix} =$$

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

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

Decryption: Notice that C_1→ "GDAPSAPKEOKE" The first letter G→7→7-4 = 3→C.

$$D_1C_1 = D_n \pmod{28} =$$

$$\begin{bmatrix} \begin{bmatrix} 3 & 4 & 1 \\ 16 & 19 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 16 & 11 & 5 \\ 15 & 11 & 5 \end{bmatrix}^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 3 & 3 & 0 \\ 15 & 18 & 0 \end{bmatrix} \\ \begin{bmatrix} 12 & 16 & 22 \\ 12 & 16 & 22 \end{bmatrix} \end{bmatrix}$$

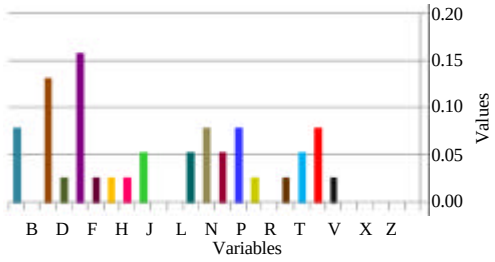

Fig. 5: Statistical scheme 1

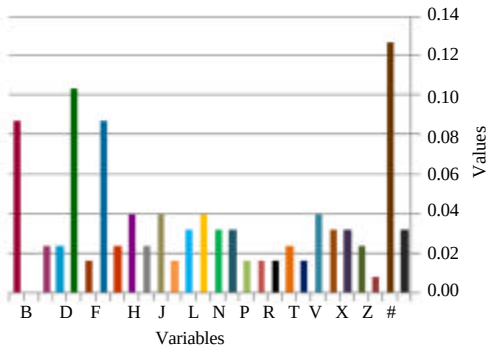

Fig. 6: Statistical scheme 2

CC#OR#LPVL; PV: C_2→ "IGEHJMWUW#_ _" The first letter I→9→9-4 = 5→E

$$(\text{mod } 28)\ D_2C_2 = D_n =$$

$$\begin{bmatrix} \begin{bmatrix} 5 & 7 & 5 \\ 8 & 10 & 13 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \\ \left(\begin{bmatrix} 23 & 21 & 23 \\ 0 & 27 & 27 \end{bmatrix}^R - \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 5 & 6 & 4 \\ 7 & 9 & 12 \end{bmatrix} \\ \begin{bmatrix} 5 & 6 & 4 \\ 27 & 0 & 0 \end{bmatrix} \end{bmatrix}$$

EFD**G**IL**E**FD_## Then, the plain text is (college).

Example: 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_LGENJMIDAJMYFGENHKXX_VUWGAAOTQEECOIWZ_ _G_ENKSFGENSE_ _ _G_EROC CDAT#E#AAA_ _#_ _#_ _"

Now, we find a table of ratios of letters and a statistical scheme of plain text and cipher text and try to compare these two texts (Table 1 and 2; Fig. 5 and 6).

For plain text: And the statistical scheme; for cipher text and the statistical scheme 2. Now, to compare these percentages we give some observations.

Table 1: Ratios of letters of plain text

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		

Table 2: Raios of letters of cipher text

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

Notice that the plain text consists of 38 characters while the cipher text consists of 126 characters This means that each letter of plain text corresponds to three letters of the cipher text and this is the immersion property we mentioned.

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

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

CONCLUSION

This study has implemented the Diffie-Helleman to generate the key generator in cryptosystem and we applied immersion property to immerse the real cipher text in other cipher text to increase the complexity for the system.

REFERENCES

Ali, A.M., 2005. Wiener polynomial of generalized distancein graph. MSc Thesis, University of Mosul, Mosul, Iraq.

Blom, R., 1983. Non-Public Key Distribution. In: Advances in Cryptology, Chaum, D. (Ed.). Plenum Press, New York, USA., ISBN:978-1-4757-0604-8, pp: 231-236.

Burton, D.M., 1967. Introduction to Modern Abstract Algebra. Addison-Wesley Publisher, ?Boston, Massachusetts, Pages: 310.

Cherney, D., T. Denton and A. Walton, 2016. Linear Algebra. CreateSpace, Scotts Valley, California, USA., ISBN:9781530903863, Pages: 398.

Edwin, C., 2001. Elementary Abstract Algebra. University of South Florida, Tampa, Florida,.

Kandasamy, W.B.V. and F. Smarandache, 2009. Groups as Graphs. EdituraCuArt, Slatina, Romania, ISBN:9781599730936, Pages: 168.

Rock, A., 2005. Pseudorandom Number Generators for Cryptographic Applications. University Salzburg, Salzburg, Austria, Pages: 108.

Stinson, D.R., 1995. Cryptography: Theory and Practice. CRC Press, Boca Raton, Florida, USA., ISBN:9780849385216, Pages: 434.