IASJ المجلات الاكاديمية العراقية

Tikrit Journal of Pure Science

ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)

Journal Homepage: http://tjps.tu.edu.iq/index.php/j

Hybrid Algorithms Use Monomials in Encryption

Awni M. Gaftan , Atyaf A. Abd

Department of Mathematics, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq

https://doi.org/10.25130/tjps.v25i3.257

ARTICLE INFO.

Article history:

-Received: 15 / 9 / 2019

-Accepted: 16 / 11 / 2019

-Available online: / / 2020

Keywords: Diffie-Hellman Method, Monomials, Hybrid Algorithm, Cipher text, Plain text.

Corresponding Author:

Name: Awni M. Gaftan

E-mail:

Awny.muhammed@tu.edu.iq

Tel:

ABSTRACT

In this study we used Diffie-Hellman (D-H) method with algorithms used monomials to get on hybrid algorithms to find a new key which can be used in clear text encryption.

Introduction

In this time all branches of mathematics can be used in encryption. One of these branches is algebra which has been used in this research widely. since many researchers used it in more than one way like Hill method. Thus, many of the blades have been developed and improved in different way as make , Blom (1983) [1] presented a study on how to create a cryptographic key using matrices and Rock (2005) [2] presented a detailed study on how to generate random numbers used for the encryption process while Stinson (1995) [3] 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 equation with the mod function.

Basic Concepts: In this paper, we introduce basic concepts that relate with these method.

Definition [4]: Let G be a non-empty set and let $*$ is a binary operation define on G we called (G,$*$) is Group if it satisfies the following conditions:

1- Closing property: which means that for all $x, y \in G$

2- Associative property: for all $x, y, z \in G$ then $x * (y * z) = (x * y) * z$.

3- $\exists$ an element $e \in G$ s.t $e * x = x * e = x$ for all $x \in G$ then e is called neutral element .

4-for all $x \in G$ $\exists\, y \in G$ such that satisfy $x * y = y * x = e$ and y is called inverse element.

And (G,$*$) is called commutative group if it satisfies the following condition for all $x, y \in G$ then $x * y = y * x$.

and if not satisfy then G is called noncommutative groups.

Definition [5]: The group of integer numbers with standard n written as

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

Such that :

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

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

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

Definition [6]: The order triple $(R, +, \cdot)$ consist of R is anon empty set with the binary operation $(+), (\cdot)$ is called **Ring** if it satisfies the following conditions:

1- $(R, +)$ is commutative Group.

2- $(R, \cdot)$ is associative

3- $\forall\, x, y, z \in R$; $x.(y + z) = x.y + x.z$ and $(x + y).= a.c + b.c$

4- R is called Ring with identity element if it is found element $1 \in$ R such that:

$1.x = x.1 = x \;\; \forall\, x \in R$

And R is called (Commutative Ring) if the multiplication process is abelain; for example, integers ring is commutative ring, As for if this is Noncommutative multiplication then the ring will become noncommutative ring for example matrices ring (2×2).

Definition [7]: Let A,B be anon empty sets then the map $f: A \to B$ is called **Injective map** if $\forall\, x_1, x_2 \in$ A and $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$ or if $f(x_1) = f(x_2)$ then $x_1 = x_2$ **Definition [6]:** Let R,S be a rings then $f: R \to S$ is called **Homomorphism Rings** if

1- $f(a+b) = f(a) + f(b)$

2- $f(ab) = f(a)f(b)\ \forall a, b \in R$.

If f Injective map then f is called **Monomorphism**.

Definition [8]: The **Monomials** is a linear combination to certain number of polynomials, also the monomials number from (d) degree at (n) from variables is combination number with frequency which given by a factor multiple sets $\binom{n}{d}$ as in the following relation and by the definition for combination:

$$\binom{n}{d} = \binom{n+d-1}{d} = \binom{d+(n-1)}{(n-1)} = \frac{1}{(n-1)!}(d+1)^{n-1}$$

For example the monomials number from 3 variables (n=3) is

$$\binom{3}{d} = \binom{3+d-1}{d} = \binom{d+2}{2} = \frac{1}{2!}(d+1)^2 = \frac{1}{2}(d+1)^2 = \frac{1}{2}(d+1)(d+1)$$

Definition [9]: Let H is **Hash Function** define as follows:

$$H: \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 \end{pmatrix} \to \left(g^{2^0.\sigma_1 + 2^1.\sigma_2 + 2^2.\sigma_3 + 2^3.\sigma_4}\right) \bmod p$$

(1-1) Diffie-Hellman (D-H) Method [10]

method that allows two sets of people with no prior knowledge of each other to create a shared secret key on an unlocked chat channel. This key can later be used to encrypt subsequent conversations.

(1-1-1) (D-H) Work [11]: We will suppose the presence of users A and B, now we show the action steps.

1- Users A,B

Agree on two prime numbers p, g

2- User A

selects a random integer let be a. then A find a_u by the following equation:

$a_u = g^a mod p$

now A send a_u to B

3- User B

selects a random integer, let be b. then B find b_u by the following:

$b_u = g^b mod p$

now B send b_u to A

4- User A

Finds the final key K_A by the following equation:

$K_A = g^a mod p$

5- User B

Finds the final key K_B by the following equation:

$K_B = g^b \bmod p$

Now $K_A = K_B$

(1-1-2) D-H Method Using Standard Groups to Generate A Matrix Key [7]

The basic working principle of this methods is also done by two people (user), we will use matrixes instead of numbers and use Hosoya polynomials to find the public key and then by using certain equation, both users will get the same key.

Example

1- Information defined for both users A,B

2,4 $\in Z^+$and selection $a = \begin{bmatrix} 1 & 7 \\ 5 & 3 \end{bmatrix}, b = \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$ such that $a, b \in M_{2\times 2}(Z_9)$,N=11

2- User A

selects a Hosoya polynomial of the group Z_{11},which is :

$f(x) = 11 + 15x + 40x^2$

A find $f(a) mod N$ such that $f(a) mod N \neq 0$

$$f(a) mod 11 = \left(11\mathrm{I} + 15\begin{bmatrix} 1 & 7 \\ 5 & 3 \end{bmatrix} + 40\begin{bmatrix} 1 & 7 \\ 5 & 3 \end{bmatrix}^2\right) \bmod 11 = \begin{bmatrix} 3 & 4 \\ 6 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

User A use matrix b to find public key following equation:

$$X_A = \left(\left(f(a)\right)^m . b . \left(f(a)\right)^n\right) mod N$$

$$= (f(a)^2 . b . f(a)^4) \bmod 11$$

$$= \left(\begin{bmatrix} 3 & 4 \\ 6 & 1 \end{bmatrix}^2 . \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix} . \begin{bmatrix} 3 & 4 \\ 6 & 1 \end{bmatrix}^4\right) mod 11 = \begin{bmatrix} 1 & 0 \\ 5 & 3 \end{bmatrix}$$

Now A send X_A to B

3- User B

selects a Hosoya polynomial of the group Z_6,which is:

$h(x) = 6 + 7x + 8x^2$

A find $h(a) mod N$ such that $h(a) mod N \neq 0$

$$h(a) mod 11 = \left(6\mathrm{I} + 7\begin{bmatrix} 1 & 7 \\ 5 & 3 \end{bmatrix} + 8\begin{bmatrix} 1 & 7 \\ 5 & 3 \end{bmatrix}^2\right) \bmod 11 = \begin{bmatrix} 4 & 9 \\ 8 & 5 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

B find public key by the following equation:

$$X_B = \left(\left(h(a)\right)^m . b . \left(h(a)\right)^n\right) mod 11$$

$$= (h(a)^2 . b . h(a)^4) mod 11$$

$$= \left(\begin{bmatrix} 4 & 9 \\ 8 & 5 \end{bmatrix}^2 . \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix} . \begin{bmatrix} 4 & 9 \\ 8 & 5 \end{bmatrix}^4\right) mod 11$$

$$= \begin{bmatrix} 5 & 0 \\ 3 & 4 \end{bmatrix}$$

Now B send X_B to A

4- Users A,B

i- user A finds the final key from the following equation:

$$K_A = \left(\left(f(a)\right)^m . X_B . \left(f(a)\right)^n\right) mod N$$

$$= \begin{bmatrix} 6 & 0 \\ 9 & 7 \end{bmatrix}$$

ii- user B finds the final key from the following equation:

$$K_B = \left(\left(h(a)\right)^m . X_A . \left(h(a)\right)^n\right) mod 11$$

$$= \begin{bmatrix} 6 & 0 \\ 9 & 7 \end{bmatrix}.$$

Now $K_A = K_B$

Plain Text Encryption Method:

We choose plain text to let it be (**KARM**) and we encrypt it in one way, let (Simple Shift Vigenere) [12] we move the letters five steps to the right by using the following function $f(x) = x + 5$ from which we get that text encoded for that word (**PFWR**) now we encrypt the encrypted text by the encryption key ,that we got in the previous example

by D-H method and by one of the encryption methods and let it be the Hill method [13] we switch alphabets to numbers by using the following table(1).

Table 1 (Coding for Alphabet)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	P	Q	R	S	T	U	V	W	X	Y	Z	φ	σ	δ
	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Now the cipher word matrix will become as follows

$$P = \begin{bmatrix} F & M \\ V & H \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 21 & 7 \end{bmatrix}$$
$$= \begin{bmatrix} 138 & 84 \\ 189 & 49 \end{bmatrix}$$

Now we find mod29 of the consequent and the new encrypted matrix will appear

$$(P \times K) mod 29 = \begin{bmatrix} 22 & 26 \\ 15 & 20 \end{bmatrix}$$

By taking the letters that correspond to the numbers, the following coded characters will appear

(1-2) Monomials Like Key Exchange Algorithm

The key exchange algorithm uses a monomials and presented as follows:

m, n: integers Z^+

a, b: group elements from ring

and $(G, ., \mathrm{I}_G)$ is a Noncommutative group with identity of this group I_G, $(R, ., \mathrm{I}_R)$ is a ring with identity of this ring I_R, and $\tau: (G, ., \mathrm{I}_G) \to (R, ., \mathrm{I}_R)$ is Monomorphism map.

User A key public

i- $f(x)$ is random polynomial select by A

ii- Find $f(a)$ which define as follows $f(\tau(a)) \in \tau(G)$, then A findX_{A} by the following equation: $\mathrm{X_A} = (\mathrm{f(a)}^{\mathrm{m}}.b\,.f(a)^n)$

User B key public

i- $h(x)$ is random polynomial select by B

ii- Find $h(a)$ which define as follows $h(\tau(a)) \in \tau(G)$, then A findX_{B} by the following

equation: $\mathrm{X_B} = (\mathrm{h(a)}^{\mathrm{m}}.b\,.h(a)^n)$

Find the final key by A

$K_A = f(a)^m.X_B.f(a)^n$

Find the final key by B

$K_B = h(a)^m.X_A.h(a)^n$

then $K_A = K_B$

We will illustrate this with an example

Example: Let m=3,n=4 , $a = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix}$, $b = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix}$ and $\tau: (G, ., I_G) \to (\mathrm{R}, ., \mathrm{I_R})$ is Monomorphism, there is a probability of group 8 we suppose it from$G_1 \to \mathrm{G}_8$ and it correspond mono ring $R_1 \to \mathrm{R}_8$. This group and ring elements are assigned in the following sequence [6]

$\mathrm{G}_1 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix} \to R_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $G_2 = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,2\,3 \end{pmatrix} \to R_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$G_3 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix} \to R_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $G_4 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} \to R_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$G_5 = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} \to R_5 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, G_6 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix} \to R_6 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$G_7 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix} \to R_7 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, G_8 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix} \to R_8 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

In calculation we used mod-2

User A: choose a random polynomial:

$f(x) = 4x^3 + 2x + 1$

Find $f(a)$mod-2 and check that $f(a) mod - 2 \neq 0$

$f(a) = \tau^{-1}(f(\tau(a))$

$= \tau^{-1}\left(\left(4\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^3 + \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} + 1\right) mod - 2\right)$

$= \tau^{-1}\left(4\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \mathrm{mod} - 2)$

$= \tau^{-1}\left(\begin{pmatrix} -5 & 0 \\ 0 & 5 \end{pmatrix} mod - 2\right)$

$= \tau^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \xrightarrow{R_3 \to G_3} \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}$

Generate the public key and then send it to the user B

$\mathrm{X_A} = \mathrm{f(a)}^{\mathrm{m}}.b.f(a)^n$

$= \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}^3 . \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} . \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}^4 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix}$

User A : choose a random polynomial:

$h(x) = 6x^4 + x^3 + 2x$

Find $h(a)$mod-2 and check that $h(a) mod - 2 \neq 0$

$h(a) = \tau^{-1}(h(\tau(a))$

$= \tau^{-1}\left(\left(6\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^4 + \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^3 + 2\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right) mod - 2\right)$

$= \tau^{-1}\left(\begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix} mod - 2\right)$

$= \tau^{-1}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix}$

Generate the public key and then send it to the user B

$X_B = h(a)^m.b.h(a)^n$

$= \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix}^3 . \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix} . \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix}^4 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix}$

Find the final key by A

$\mathrm{K_A} = f(a)^m.X_B.f(a)^n$

$= \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}^3 . \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} . \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix}^4 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix}$

Find the final key by A

$\mathrm{K_B} = \mathrm{h(a)}^{\mathrm{m}}.X_A.h(a)^n$

$= \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix}^3 . \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix} . \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix}^4 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix}$

(1-2-1) Improved D-H by The Key Exchange Monomials Algorithm

In this method, we replace the matrixes with a group of element and we use the map Monomorphism $\tau: (G, ., I_G) \to (\mathrm{R}, ., \mathrm{I_R})$, where G is Non abelain group, R is ring, N=-2, use the Hosoya polynomial and the elements are represented in the reference [6].

Now take 2,3$\in Z^+$and

$a = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,1\,2\,3 \end{pmatrix}, b = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix}$

User A

Choose Hosoya polynomial to group Z_5

$f(x) = 5 + 6x + 4x^2$

Now find $f(a)$ such that $f(a) mod - 2 \neq 0$

$f(a) = \tau^{-1}(f(\tau(a))$

$$= \tau^{-1}\left(\begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix} + 6\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + 4\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2\right)$$

$$= \tau^{-1}\begin{pmatrix}1 & 6\\ -6 & 1\end{pmatrix}$$

$$f(a) mod - 2 = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix}1\,2\,3\,4\\ 2\,1\,4\,3\end{pmatrix}$$

Find the generate key and then send it to B

$$X_A = (f(a)^m . b . f(a)^n) mod N$$

$$= \tau^{-1}\left(\left(\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2 \cdot \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^3\right) mod - 2\right)$$

$$= \tau^{-1}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix} \xrightarrow{R_5 \to G_5} \begin{pmatrix}1\,2\,3\,4\\ 4\,3\,2\,1\end{pmatrix}$$

User B

Choosing Hosoya polynomial to group Z_6

$$h(x) = 6 + 7x + 8x^2$$

Now find $h(a)$ such that $h(a) mod - 2 \neq 0$

$$h(a) = \tau^{-1}(h(\tau(a))$$

$$= \tau^{-1}\left(\left(\begin{pmatrix}6 & 0\\ 0 & 6\end{pmatrix} + 7\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + 8\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2\right) \text{mod} - 2\right)$$

$$= \tau^{-1}\left(\begin{pmatrix}-2 & 7\\ -7 & -2\end{pmatrix} mod - 2\right)$$

$$= \tau^{-1}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \xrightarrow{R_6 \to G_6} \begin{pmatrix}1\,2\,3\,4\\ 3\,2\,1\,4\end{pmatrix}$$

Find the generate key and then send it to A

$$X_B = (h(a)^m . b . h(a)^n) mod N$$

$$= \tau^{-1}\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^2 \cdot \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^3\right)$$

$$= \tau^{-1}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix} \xrightarrow{R_5 \to G_5} \begin{pmatrix}1\,2\,3\,4\\ 2\,3\,4\,1\end{pmatrix}$$

$X_A = X_B \; then \; K_A = K_B$

(1-3) Improved Monomials Algorithm

We have made some modifications to the monomials algorithm mentioned in source [8] let's get a hybrid or improved the D-H method and the monomials algorithm.

1- **Information defined for both users A,B**

$m, n \in Z^+$, a, b group elements from ring , $\tau: (G, ., I_G) \to (R, ., I_R)$ Monomorphism where G is non abelain group and R is a ring , p, q secure numbers only known to users, g generator function.

2- **User A** :

i- $f(x, y)$ is random polynomial of the second order with two variables selected by A

ii- Find $f(a, b)$ such that $f(\tau(a, b)) \in \tau(G)$, then finds the public key from the following equation:

$X_A = f(a, b)^m . b . f(a, b)^n$

Then A is send X_A to B

3- **User B** :

i- $h(x, y)$ is random polynomial of the second order with two variables selected by B

ii- Find $h(a, b)$ such that $h(\tau(a, b)) \in \tau(G)$, then finds the public key from the following equation:

$X_B = h(a, b)^m . b . h(a, b)^n$

then B is send X_B to A

4- Find the final key by user A :

$K_A = f(a, b)^m . X_B . f(a, b)^n$

5- Find the final key by B:

$K_B = h(a, b)^m . X_A . h(a, b)^n$

(1-4) Improved Encryption Algorithm

We assume user B wants to send a message to user A , user B will perform the following steps:

1- Convert the message to an matrix.

2- Now, by using Encryption Matrix (5×5).

Table 2 (Encryption Matrix)

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

3- B take all two consecutive characters and encodes as follows:

i- If the two letters are in a row, take the letter to the right of each letters.

ii- If the two letters are on one column, take the letter below each letter.

iii- If the two letters do not fall on the same row or column, B will complete a square that passes the two letters and will takes the letters that complete the square heads.

4- An encrypted $\dot{M}$ message converts it to numbers with the following table 3.

Table 3 (Encryption Table)

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

5- After obtaining the encrypted message consisting of numbers, let be $\ddot{M}$ the last step of encryption is the use of the Hash Function of the final key and collected with $\ddot{M}$:

$C = H(K_B) + \ddot{M}$, To get a new encrypted message

(1-5) Improved Decryption Algorithm

User A receives the encrypted message C and performs the following steps to get the clear massage:

1- Find hash function for the final key.

2- Collect C with the resulting inverse that appeared from step1.

3- Switch the letters instead of the numbers from the table in step3 in the encryption.

4- Find the clear message by using the table in step2 in the improved encryption algorithm, which tests the characters and reverses the action in steps (i-ii-iii).

Example

1- **Users A,B**

2,3$\in Z^+$, $a = \begin{pmatrix}1\,2\,3\,4\\ 4\,1\,2\,3\end{pmatrix}$, $b = \begin{pmatrix}1\,2\,3\,4\\ 2\,3\,4\,1\end{pmatrix}$, N=-2

2- **User A**

$f(x, y)$ is random polynomial of the second order with two variables select

$$f(x, y) = 5y^2 + 6xy + 4x^2$$

Find $f(a, b) mod N$ such that $f(a, b) mod N \neq 0$

$$f(a, b) = \tau^{-1}(f(\tau(a, b)) mod N$$

$$= \tau^{-1}\left(5\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}^2 + 6\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} + 4\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^2\right) \text{mod} - 2$$

$$= \tau^{-1}\left(5\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + 6\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + 4\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right) mod - 2$$

$= \tau^{-1}\left(\begin{pmatrix}1 & 6\\ 6 & 1\end{pmatrix} \bmod -2\right)$

$= \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

Find the public key and send to B

$X_A = (f(a,b)^m . b . f(a,b)^n)$

$= \tau^{-1}\left(\left(\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2 \cdot \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^3\right) mod -2\right)$

$= \tau^{-1}\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right) mod -2$

$= \tau^{-1}\left(\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right) mod -2$

$= \tau^{-1}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \xrightarrow{R_6 \to G_6} \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$

3- **User B**

$h(x,y)$ is random polynomial of the second order with two variables select $h(x,y) = 6y^2 + 7xy + 8x^2$ and find $h(a,b) mod N$ such that $h(a,b) mod N \neq O$.

$h(a,b) = \tau^{-1}\left(6\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^2 + 7\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + 8\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}^2\right)$

$= \tau^{-1}\left(6\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + 7\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + 8\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right)$

$h(a,b) mod -2 = \tau^{-1}\begin{pmatrix}-2 & 7\\ 7 & -2\end{pmatrix} mod -2$

$= \tau^{-1}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix} \xrightarrow{R_5 \to G_5} \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

Now B finds public key and send to A

$X_B = (h(a,b)^m . b . h(a,b)^n) mod N$

$= \tau^{-1}\left(\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}^2 \cdot \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}^3\right) mod -2$

$= \tau^{-1}\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right) \bmod -2$

$= \tau^{-1}\left(\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right) \bmod -2$

$= \tau^{-1}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \xrightarrow{R_4 \to G_4} \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$

4- **Users A,B**

A finds the final key

$K_A = f(a,b)^m . X_A . f(a,b)^n$

$= \tau^{-1}\left(\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2 \cdot \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^3\right)$

$= \tau^{-1}\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right)$

$= \tau^{-1}\left(\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right)$

$= \tau^{-1}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_3 \to G_3} \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

B finds final key

$K_B = h(a,b)^m . X_A . h(a,b)^n$

$= \tau^{-1}\left(\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}^2 \cdot \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}^3\right)$

$= \tau^{-1}\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right)$

$= \tau^{-1}\left(\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right)$

$= \tau^{-1}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_3 \to G_3} \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

Then $K_A = K_B$

Use The Encryption Algorithm In Clear Text Encryption

Assume user B wants to send the word (MONA) to user A to perform the following steps: with confidential numbers defined for both users $g = 2, p = 23$

1- Convert the word into a matrix as follows:

$M = \begin{pmatrix}M & N\\ O & A\end{pmatrix}$

2- Find the message encrypted by the table in paragraph 2 in the enhanced encryption algorithm which will be as follows:

$\dot{M} = \begin{pmatrix}N & C\\ P & L\end{pmatrix}$

3- Conversion of matrix elements from alphabets to numbers through the table in paragraph3 in the improved encryption algorithm

$\ddot{M} = \begin{pmatrix}13 & 2\\ 15 & 11\end{pmatrix}$

4- Final key compensation K_A by Hash Function as follows:

$H: \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \to g^{2^0.3+2^1.4+2^2.1+2^3.2} mod 23$

$= 2^{31} mod 23$

$= 2147483648 mod 23$

$= 6$

Now we find encrypted text

$C = 6 + \ddot{M}$

$= 6\mathrm{I} + \begin{pmatrix}13 & 2\\ 15 & 11\end{pmatrix}$

$= \begin{pmatrix}19 & 2\\ 15 & 17\end{pmatrix}$

Decryption: User A receives the encrypted message C and performs the following steps to obtain the original message

1- Find the hash function for the final key K_A

$= 2^{31} mod 23$

$= 2147483648 mod 23$

$= 6$

2- Subtract the resulting product from the matrix C

$\begin{pmatrix}19 & 2\\ 15 & 17\end{pmatrix} - 6\mathrm{I} = \begin{pmatrix}13 & 2\\ 15 & 11\end{pmatrix} = \ddot{\mathrm{M}}$

3- Switch characters instead of numbers from the table in paragraph 3 in the encryption algorithm

$\dot{\mathrm{M}} = \begin{pmatrix}N & C\\ P & L\end{pmatrix}$

4- Create the original message by using the table in step2 in the improved encryption algorithm

$M = \begin{pmatrix}M & N\\ O & A\end{pmatrix}$

Conclusion

After obtaining the results in this research, it is possible to conclude that the use of monomials in the algorithms gives us the possibility of obtaining more than one result when we change the ring with the group associated with an appropriate difference. Also more than one result can be obtained using the function of permutation on the rows of the matrix used or on column.

References

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

[2] Rock .A, (Pseudorandom Number Generators for Cryptographic Applications) University Salzburg, Austria , Pages: 108, 2005.

[3] Stinson .D.R, (Cryptography: Theory and Practice), CRC press, Boca Raton, Florida, USA, ISBN:9780849385216, Pages:434, 1995.

[4] S.C.COUTINHO, (The Mathematics of Ciphers ; Number Theory and RSA Cryptography), Department of Compute Science Federal University of Riode Janeiro, Brazil, 1997.

[5] Awni M.Gaftan, Akram S.Mohammed and Osama H.Subhi (Cryptography by using Hosoya polynomials for Graphs Groups of Integer Module and Dihedral Groups with Immersion Property), Ibn Al Haitham Jour for Pure and Apple . sci, IHJPAS: VOL. 31 (3) 2018 .

[6] Karl-Heinz. F, (Groups, Rings and Field), Uppsala, 2010.

[7] D. Saba .N.M, (Foundations of Mathematics), College of Ibn Al Haitham Of Science, University of Baghdad, Lectures Notes in Fund, 2010.

[8] Gautam Kumar and Hem raj Saini, (Novel Noncommutative Cryptography Scheme Using Extra Special Group), Security and Communication Networks, University of Information Technndogy Solan, 21 page, India 2017.

[9] Z. Cao, X .Dong and L. Wang, (New public key cryptosystems using polynomials over noncommutative), Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, P.R, China, 2002.

[10] William Stallings,(Cryptography and Network Security Principles and Practices Fourth Edition), Publisher: Prentice Hall, ISBN-10: 0-13-187316-4, 2005.

[11] Sivahagaswathi Kallam, (Diffie-Hellman: Key Exchange and Public Key Cryptosystems),Math and computer Science Department,(MSC. TH.) Indiana state University, Terre Haute, IN, USA, 2015.

[12] Wajdy A. A, (Introduction to Classical Cryptography), Romansy, Sudan Geek, 2007.

[13] Murray Eisenberg,(Hill ciphers and Modular Linear Algebra), Copyright © 1998 by Murray Eisenberg, November 3, 1999.

خوارزميات هجينة لاحاديات متعددات الحدود في التشفير

عوني محمد كفطان , اطياف احمد عبد

قسم الرياضيات ، كلية علوم الحاسوب والرياضيات ، جامعة تكريت ، تكريت ، العراق

الملخص

في هذا الدراسة استخدمنا طريقة (Diffie-Hellman) مع خوارزميات تستخدم احاديات الحدود للحصول على خوارزميات تشفير هجينه لايجاد مفتاح جديد يستخدم في تشفير النصوص الواضحة .