استخدام الدوال الرياضية وبعض التحويلات التكاملية في التشفير

بشرى الضاهر*، نصر الدين عيد، محمد هشام بوادقجي*****

*طالبة دراسات عليا(ماجستير) قسم الرياضيات، كلية العلوم، جامعة حلب

**أستاذ، قسم الرياضيات، كلية العلوم، جامعة حلب

***مدرس، قسم الرياضيات، كلية العلوم، جامعة حلب

الملخص

في هذا البحث استخدمنا بعض التحويلات التكاملية الشهيرة في الرياضيات مثل تحويل لابلاس وميلين وتحويل إس إي إي (see) في عملية التشفير حيث قمنا بتقطيع النص المشفر إلى أربعة أقسام (القسم الأول تم استخدام تحويل لابلاس وفي القسم الثاني تم استخدام تحويل ميلين والقسم الثالث see والقسم الرابع من خلال استخدام تابع لوغاريتمي) وقد أدى ذلك للحصول على خوارزمية تشفير معقدة من الصعب فك تشفيرها من قبل الآخرين، كما تم القيام بخطوات فك التشفير لهذه الخوارزمية، وبالتالي فإن هذا العمل الذي يشمل إجراء عملية التشفير وفك التشفير بخوارزمية جديدة لم يسبق أن طُرحت سابقاً وتميزت هذه الخوارزمية عن غيرها بأنها عند تغيير التابع الذي طبقنا عليه التحويلات التكاملية بشكل اختياري يؤدي إلى تغيير هذه الخوارزمية الأمر الذي يؤدي لمرونة في تعديلها ويعطي صعوبة في فك تشفيرها.

الكلمات المفتاحية: تحويل، خوارزمية، تشفير، مفتاح، لابلاس، ميلين.

ورد البحث للمجلة بتاريخ 7/12 /2023

قبل للنشر بتاريخ 24/ 9/2023

1.مقدمة:

استُخدمت أشكال التشفير البسيطة في الماضي من قبل عامة الناس لحماية رسائلهم حيث قام التجار الصينيون بحماية سر صناعة الحرير الصناعي باستخدام التشفير وكذلك قام الجنود الألمان بحماية أسرارهم العسكرية باستخدام التشفير.

يعتبر علم التشفير(encryption) من العلوم المفيدة في كافة مجالات الحياة الاقتصادية والعسكرية والتجارية والأمنية وغيرها.

إن جذر هذه الكلمة(crypt) مشتق من الكلمة اليونانية(kryptos) والتي تعني مخفي أو سر وفي الآونة الأخيرة بسبب تطور التقنيات التكنولوجية والتطبيقات بشكل سريع وجب ابتكار طرائق تشفير قوية كإدخال الدوال الرياضية المعقدة مع بعض التحويلات التكاملية لضمان سرية المعلومات بشكل أكبر وعدم فك تشفيرها بسهولة.

لنعرض بعض الأبحاث التي قام بها العلماء في التشفير.

فمثلاً في عام 2019 [1] استخدم الباحثان تحويل لابلاس في التشفير وفي نفس العام [2] قام الباحثون باستخدام التحويل N− وفي عام 2020 [3] تم اعتماد تحويل ميلين وقام الباحثان باستخدام تحويل MAHGOUB [4] وفي عام 2021 [5] تم استخدم تحويل Jafari،وفي عام 2016 [6] تم استخدام تحويل Aboodh وفي عام 2022 [7] تم استخدام تحويل تكاملي جديد (see) وفي عام 2021 [8] قام الباحث بالدمج بين تحويلي لابلاس والزاكي ومؤخراً في عام 2022 تم الاعتماد على الدوال الرياضية في التشفير حيث قام عدد من الباحثين باعتماد التابع :

$(2^x - 1)$ في التشفير [9].

2.تعاريف أساسية:

1.2.تعريف تحويل لابلاس[1]:

ليكن $f(t)$ تابع معرف على $t \geq 0$ ولتكن s نقطة من المستوي العقدي $\mathbb{C}$ المعرف بالتكامل:

$$l\{(f(t))\} = f(s) = \int_0^{\infty} e^{-st} f(t) dt$$

وهذا التكامل متعلق بالمتحول العقدي s كوسيط.

وفي الخوارزمية المقترحة سنستخدم تحويل لابلاس لقوىt^n فقط والتي تعطى بالشكل:

$$l(t^n) = \frac{n!}{s^{n+1}} \; ; n \in N$$

2.2.تعريف تحويل ميلين[3]:

ليكن التابع $f(t)$ المعرف فوق المحور الحقيقي الموجب $0 < t < \infty$

إن تحويل ميلين هو عملية تحويل التابع f لـ التابع F المعرف فوق المستوي العقدي المعرف بالتكامل:

$$M\{f;s\} \equiv F(s) = \int_0^\infty f(t)\, t^{s-1} dt$$

التابع F(s) يدعى تحويل مللين ل التابع $f(t)$ و s نقطة من المستوي العقدي,

وفي الخوارزمية المقترحة سنستخدم تحويل ميلين لقوى $\{x^{n+2}\}$ فقط والتي تعطى بالشكل:

$$M\{x^{n+2}\} = \frac{x^{n+h+2}}{n+h+2} \quad , n = 0,1, \dots \dots, h = 1$$

3.2.تحويل SEE[7]:

ليكن لدينا التابع $f(t)$ من المجموعة A المعرفة بـ :

$$A = \{f(t): there\ exist\ M, L_1, L_2 > 0, |f(t)| < M^{L_j|t|},$$
$$if\ t \in (-1)^j \times [0, \infty\}, j = 1,2\}$$

والمعرف بالتكامل:

$$s\{f(t)\} = T(v)$$
$$= \frac{1}{v^n} \int_0^\infty f(t) e^{-vt} dt \quad , n \in z, t \geq 0, l_1 \leq v \leq l_2$$

يلزمنا في التشفير المقترح:

سنستخدم في الخوارزمية المقترحة تحويل see لقوى t^m فقط والمحسوبة بالشكل:

$$s\{k\} = \frac{k}{v^{n+1}} \; , k$$ ثابت

$$s\{t^m\} = \frac{m!}{v^{n+m+1}} \quad , m \in N$$

$$S^{-1}\left\{\frac{1}{v^{n+1}}\right\} = 1 \qquad s^{-1}\left\{\frac{m!}{v^{n+m+1}}\right\} = t^m$$

3.الفكرة الأساسية في عملية التشفير:

لنعرض فكرة التشفير باستخدام التحويل التكاملي للابلاس المذكورة في[1]

ليكن لدينا كثير الحدود:

$$f(x) = x^2 + x^4 + x^6 + x^8 + x^{10} + x^{12} + \cdots$$

لنشفر الكلمة التالية BUSHRA لنعطي ترميز جديد للأحرف:

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

فتكون قيم النص المقابل لهذه الأحرف هي: B=2 ,U=21 ,S=19 ,H=8 ,R=18 ,A=1,

نضع هذه الأرقام في أمثال كثير الحدود $f(x)$

$$f(x) = 2x^2 + 21x^4 + 19x^6 + 8x^8 + 18x^{10} + x^{12}$$

بتطبيق تحويل لابلاس على طرفي كثير الحدود الأخير نجد أن:

$$l\{f(x)\} = \frac{2 \times 2!}{y^3} + \frac{21 \times 4!}{y^5} + \frac{19 \times 6!}{y^7} + \frac{8 \times 8!}{y^9} + \frac{18 \times 10!}{y^{11}} + \frac{12!}{y^{13}}$$

لنرمز لأمثال كثير الحدود السابق بالرمز p_n

p_n: 4 504 13680 322560 65318400 479001600

ومن أجل إرجاع قيم p_n لقيم شيفرة أسكي بالترميز الجديد نأخذ قياس بالنسبة لـ 26 لجميع قيم p_n ونرمز لها بالرمز f_n.

ومن أجل فك التشفير يلزمنا معرفة قيم المفتاح التالي r_n

$$f_n = p_n(mod26) \qquad r_n = \frac{p_n - f_n}{26}$$

f_n: 4 10 4 4 4 12

r_n: 0 19 526 12406 2512246 18423138

حيث أن f_n هي المفتاح الثاني الذي سنستخدمه في فك التشفير وهذه القيم ستظهر للمستخدم على الشاشة.

النص المشفر الذي سيظهر للمستخدم هو المقابل لقيم f_n

فيكون f_n: 4 10 4 4 4 12

والأحرف المقابلة لهذه القيم في الترميز الجديد هي D J D D D L

و(DJDDD)هي الرسالة المشفرة ولفك تشفير هذا النص يلزمنا معرفة قيم المفاتيح التالية f_n r_n

ويمكننا استخراج الأمثال p_n من العلاقة التالية $p_n = 26r_n + f_n$

فيكون: p_n: 4 504 13680 322560 65318400 479001600

نضع هذه القيم كأمثال للتابع

$$F(y) = \frac{4}{y^3} + \frac{504}{y^5} + \frac{13680}{y^7} + \frac{322560}{y^9} + \frac{65318400}{y^{11}} + \frac{479001600}{y^{13}}$$

وبأخذ تحويل لابلاس المعاكس:

$$l^{-1}\{F(y)\} = \frac{4 \times x^2}{2!} + \frac{504 \times x^4}{4!} + \frac{13680 \times x^6}{6!} + 322560 \times \frac{x^8}{8!} + \frac{65318400x^{10}}{10!} + 479001600 \times \frac{x^{12}}{12!}$$

وقيم أمثال كثير الحدود الأخير هي:

2 21 19 8 18 1

والتي تقابل BUSHRAفي الترميز الجديد.

وفي[9] تم استخدام التابع الأسي والتابع اللوغاريتمي في التشفير فقد تم إدخال قيم النص المرمّزة سابقاُ في التابع $f(x) = 2^x - 1$ ولفك التشفير تم استخدام التابع العكسي $f^{-1}(x) = \log_2(x+1)$

فمثلاً النص المقترح

K O S O V A

والقيم المقابلة لهذه الأحرف في الترميز الجديد المذكور سابقاً:

10 14 18 14 21 0

نعوض هذه القيم في التابع:

$f(10) = 2^{10} - 1 = 1024 - 1 = 1023$
$f(14) = 2^{14} - 1 = 16384 - 1 = 16383$

وبنفس الطريقة لبقية الأرقام، ولفك التشفير نستخدم التابع العكسي لهذا التابع ومنه:

$$f^{-1}(1023) = \log_2(1023 + 1) = \log_2(1024) = \log_2 2^{10} = 10$$
$$f^{-1}(16383) = \log_2(16383 + 1) = \log_2(16384) = \log_2 2^{14} = 14$$

وبأخذ المقابل للرقم 10 في الترميز الجديد نجد أنه يقابل الحرف k والمقابل للرقم 14نجد أنه يقابل الحرف o وبالمثل لبقية الأرقام.

4.الخوارزمية المقترحة:

بعد عرض طريقة التشفير باستخدام التحويل التكاملي للابلاس وطريقة استخدام التابع الأسي والتابع اللوغاريتمي، سنقترح خوارزمية جديدة من خلال تجزئة النص إلى أربعة أجزاء، الجزء الأول يتم تشفيره باستخدام التحويل التكاملي للابلاس [1]والجزء الثاني باستخدام التحويل التكاملي لـ ميلين[2] والجزء الثالث باستخدام تحويل إس إي إي(see) [7]والجزء الرابع باستخدام التابع اللوغاريتمي $f(x) = \log_5(2x - 1) - 7$.لنقطع النص إلى أربعة أقسام متساوية كالتقطيع المذكور سابقاً.

MP: ميلين	CO: لابلاس
ER: لوغاريتمي تابع	$UT: SEE$

1) نأخذ الحرف الأول والثاني CO

والأرقام المقابلة لهذه الأحرف في الترميز الجديد للحرف C هو 3وللحرفO هو15

ليكن لدينا التابع التالي: $f_1(x) = x^2 + x^4$

نضع هذه القيم كأمثال لهذا لمنشور:

$$f_1(x) = 3x^2 + 15x^4$$

بتطبيق تحويل لابلاس:

$$l\{f_1(x)\} = \frac{3\times 2!}{y^3} + \frac{15\times 4!}{y^5}$$

$$p_1 = 6 \qquad p_2 = 360$$

وبأخذ القياس بالنسبة لـ 26 لهذه القيم نجد:

$F_1 = 6 \quad F_2 = 22$ الأحرف المقابلة لهذه القيم هي:FV

لدينا $r_n = \frac{p_n - f_n}{26}$

فيكون $r_1 = 0 \qquad r_2 = 13$

2)القسم الثاني: لنشفر الحرفين الآخرين بنفس الطريقة:

ليكن التابع $f_2(x) = 2^2x^2 + 2^4x^4$

نضع قيم الحرفين التالين MP في أمثال المنشور السابق، حيث أن الحرف M يقابل الرقم 13 في الترميز الجديد والحرف P يقابل الرقم 16 في الترميز الجديد فيكون:

$$f_2(x) = 13 \times 2^2x^2 + 16 \times 2^4x^4$$

بتطبيق تحويل ميلين للطرفين:

$$M\{f_2(x)\} = \frac{13\times 2^2}{3}y^3 + \frac{16\times 2^4}{5}y^5$$

بحساب قيم الأمثال نجد أن

$$p_3 = 17.33333333 \qquad p_4 = 51.2$$

بأخذ القياس بالنسبة لـ 26 لهذه القيم

$F_3 = 17.33333333 \quad F_4 = 25.2$ الأحرف المقابلة لهذه القيم هي: QY

$$r_3 = 0 \qquad r_4 = 1$$

3)القسم الثالث: T U بأخذ المقابل لهذه الأحرف في الترميز الجديد ونضعها كأمثال للتابعf_3

$f_3(x) = 21x^3 + 20x^4$ ومنه $f_3(x) = x^3 + x^4$

بتطبيق تحويل SEE

$$see\{f_3(x)\} = \frac{21 \times 3!}{y^{n+4}} + \frac{20 \times 4!}{y^{n+5}}$$

$p_5 = 126 \qquad p_6 = 480$ والأمثال هي

بأخذ القياس بالنسبة لـ 26 لهذه القيم

$F_6 = 12$ $F_5 = 22$ والأحرف المقابلة لهذه القيم هي:VL

وبحساب $r_n = \frac{p_n - f_n}{26}$

$r_6 = 18$ $r_5 = 4$

الآن الحرفان ER والقيم المقابلة لهذه الأحرف هي 5و18

نعوضها في التابع:

$f(x) = \log_5(2x - 1) - 7$ والتابع العكسي للتابع f يعطى:

$$f^{-1}(x) = (5^{x+7} + 1)/2$$
$$f(5) = -5.634787611$$
$$f(18) = -4.790938045$$

والنص المشفر يعطى بالشكل:FVQYVL−5.634787611−4.790938045

فك التشفير:

لفك تشفير النص السابق يلزمنا معرفة قيم النص المشفر f_n والمفتاح r_n من أجل استخراج قيم النص p_n

(n=1,2,3,4,5,6)

لفك تشفير أول حرفين: لدينا

$F_1 = 6$ $F_2 = 22$ $r_1 = 0$ $r_2 = 13$

ولدينا $p_n = 26r_n + f_n$ ومنه

$p_1 = 6$ $p_2 = 360$

$$f_1(y) = \frac{6}{y^3} + \frac{360}{y^5}$$

بأخذ تحويل لابلاس العكسي:

$$l^{-1}(f(y)) = \frac{6x^2}{2!} + \frac{360x^4}{4!}$$

وأمثال هذا المنشور هي 15 3 والأحرف المقابلة لهذه القيم في الترميز الجديد هي CO

فك تشفير القسم الثاني:

$F_3 = 17.33333333$ $F_4 = 25.2$ $r_3 = 0$ $r_4 = 1$

$p_3 = 17.33333333$ $p_4 = 51.2$

$$f_2(y) = 17.33333333y^3 + 51.2y^5$$

بأخذ تحويل ميلين العكسي:

$$M^{-1}\{f_2(y)\} = 17.33333333 \times 3x^2 + 51.2 \times 5x^4$$

نقسم على 2^i

$$M^{-1}\{f_2(y)\} = 17.33333333 \times \frac{3}{2^2}x^3 + 51.2 \times \frac{5x^4}{2^4}$$

وأمثال هذا المنشور هي 16 13 والأحرف المقابلة لهذه القيم هي:MP

فك تشفير القسم الثالث:

$$F_5 = 22 \quad F_6 = 12 \quad r_5 = 4 \quad r_6 = 18$$
$$p_5 = 126 \quad p_6 = 480$$
$$f_3(y) = \frac{126}{y^{n+4}} + \frac{480}{y^{n+5}}$$

بأخذ تحويل SEE المعاكس:

$$see^{-1}\{f_3(y)\} = \frac{126x^3}{3!} + \frac{480x^4}{4!}$$

وأمثال هذا المنشور هي 20 21 والأحرف المقابلة لهذه القيم هي: UT

فك تشفير القسم الرابع:

$$f^{-1}(y) = \frac{5^{x+7}+1}{2}$$
$$f^{-1}(-5.634787611) = 5 \quad f^{-1}(-4.790938045) = 18$$

وهي تقابل الأحرف ER في الترميز الجديد.

ومن فك تشفير الأقسام الأربعة نحصل على الكلمة COMPUTER وهو المطلوب.

6.كود التشفير:

فيما يلي سنعطي الكود البرمجي للخوارزمية المقترحة بلغة C++

فيما يلي سيتم عرض الكود البرمجي للخوارزمية المقترحة.

```
#include<iostream>
#include<math.h>
#include<iomanip>
using namespace std;
long long fa(int n);
float a[10];
char gt[10];
float p[10];
long long r[10];
void write(int nt);
a[i]=p[i]-(26*int(a[i]/26));
r[i]=(p[i]-a[i])/26;
}
 }
void cut2(int nt)
{long long i;
int t=2;
for(i=(nt/4)+1;i<(2*nt/4)+1;i++)
{a[i]=a[i]*pow(2,t);
a[i]=a[i]/(t+1);
```

```
float read(int nt);
void cut1(int nt);
void cut2(int nt);
void cut3(int nt);
void cut4(int nt);
int main()
{
int nt;
cout<<" Enter the number of
characters(+1)"; cin>>nt;cout<<endl;
cout.precision(12);
long long i;
read(nt);
cut1(nt);
cut2(nt);
cut3(nt);
cut4(nt);
write(nt);
return 0;}
long long fa(int n)
{long long i; long long f=1;
for(i=1;i<=n;i++)
f=f*i;
return f;}
float read(int nt)
{int i; cout<<endl; cout<<"Enter the
text with great characters"; cout<<endl;
for(i=1;i<nt;i++)
{cin>>gt[i];
a[i]=int(gt[i]);
a[i]=a[i]-64;} }
void cut1(int nt)
{long long i;
        for(i=1;i<(nt/4)+1;i++)
{a[i]=a[i]*fa(2*i);
p[i]=a[i];
t=t+2;}

for(i=(nt/4)+1;i<(2*nt/4)+1;i++)
{p[i]=a[i];
a[i]=p[i]-(26*int(a[i]/26));
r[i]=(p[i]-a[i])/26;
}}
void cut3(int nt)
{long long i;
int kr=3;
for(i=(2*nt/4)+1;i<3*nt/4+1;i++)
{a[i]=a[i]*fa(kr); kr++;}
for(i=(2*nt/4)+1;i<3*nt/4+1;i++)
{p[i]=a[i];
a[i]=p[i]-(26*int(a[i]/26));
r[i]=(p[i]-a[i])/26;
 }cout<<endl;
}
void cut4(int nt)
{long long i;
        for(i=3*nt/4+1;i<nt;i++)
a[i]=log(2*a[i]-1)/log(5)-7;
}
void write(int nt)
{int i;cout<<" Keys"; cout<<endl;
for(i=1;i<3*nt/4+1;i++)
cout<<r[i]<<"\t";
for(i=1;i<nt;i++)
cout<<a[i]<<"\t";
cout<<endl;
cout<<"Encrypted text    ";
for(i=1;i<3*nt/4+1;i++)
cout<<char(a[i]+64);
for(i=3*nt/4+1;i<nt;i++)
cout<<a[i];}
```

7.كود فك التشفير:

```
#include<iostream>
#include<math.h>
using namespace std;
long long fa(int n);
int main()
{float a[10];  float r[10];
float p[10];
float f[10];
int i; int nt;
a[i]=a[i]/fa(2*i);
int t=2;
for(i=(nt/4)+1;i<(2*nt/4)+1;i++)
{
a[i]=a[i]/pow(2,t);
a[i]=a[i]*(t+1);
t=t+2;}
int kr=3;
for(i=(2*nt/4)+1;i<3*nt/4+1;i++)
```

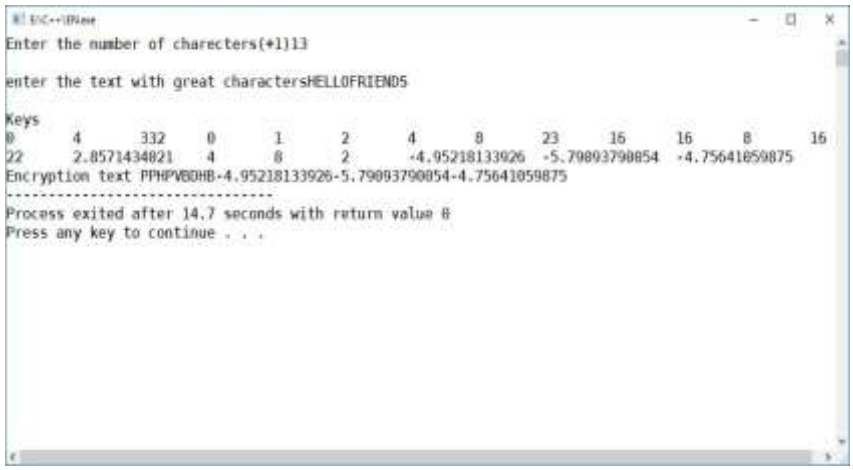
```
cout<<" Enter the number of
characters+1"; cin>>nt; cout<<endl;
cout<<" Enter the keys in order";
for(i=1;i<3*nt/4+1;i++)
cin>>r[i];
for(i=1;i<3*nt/4+1;i++)
cin>>f[i];
for(i=1;i<3*nt/4+1;i++)
a[i]=26*r[i]+f[i];

for(i=1;i<(nt/4)+1;i++)
{a[i]=a[i]/fa(kr);kr++;}
out<<endl;
for(i=3*nt/4+1;i<nt;i++)
cin>>p[i];
for(i=3*nt/4+1;i<nt;i++)
a[i]=(pow(5,p[i]+7)+1)/2;
for(i=1;i<nt;i++)
cout<<char(a[i]+64);
return 0;}
long long fa(int n)
{long long i; long long f=1;
for(i=1;i<=n;i++)
f=f*i;
return f;}
```

8.الشاشات التنفيذية:

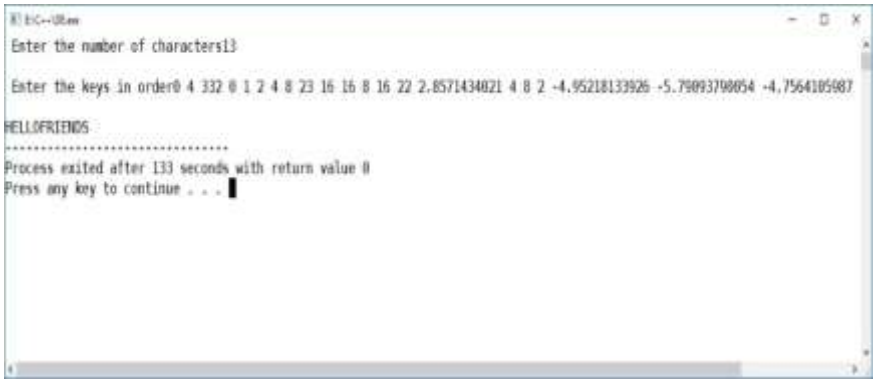
تم تنفيذ الكود البرمجي بلغة c++ على الحاسوب وأعطى النتائج التالية:

تم تشفير كلمة HELLOFRIENDS كما يلي:



الشكل(1) يمثل ناتج تنفيذ تشفير كلمة HELLOFRIENDS

وناتج فك التشفير بعد إدخال قيم المفاتيح كالتالي:



الشكل (2) يمثل وناتج فك التشفير بعد إدخال قيم المفاتيح

9.نتيجة البحث:

مما تقدم نجد أنه بتطبيق بعض التحويلات التكاملية على كثيرات الحدود ودمجها مع بعض الدوال الرياضية اللوغاريتمية تم الحصول على خوارزمية تشفير يصعب كسرها وذلك لأنه تم استخدام التوابع الرياضية والتحويلات التكاملية بنفس الخوارزمية، وتم اختبار هذه الخوارزمية من خلال تنفيذ الكود البرمجي لها وعرض النتائج من خلال إدخال نص.

10.التوصيات:

نوصي من خلال هذا البحث بما يلي:

1-تطبيق التحويلات التكاملية على توابع مثلثية بدلاً من كثيرات الحدود.

2-تقسيم النص إلى أكثر من أربعة أقسام واستخدام تابع أسي بدلاً من تابع لوغاريتمي.

3-اختيار تحويلات تكاملية مختلفة عن لابلاس وميلين وsee وتطبيقها في تشفير النصوص وخاصة عندما يكون النص طويلاً.

References

[1]Hemant,Undegaonkar,2019-**security in communication by using laplace transforms and cryptography**.ISSN-8616.

[2]Dharshini Priya,Muthu Amirtha,Senthil Kummar,2019-**application of N-transform in cryptography.**IJSRR.

[3]Sadiqa Bhatti,Rabia Safdar,Khurrem Shehzad,Muhammad Jawad,Hira Ahmed,2020-**New Cryptographic Scheme with Mellin Transformation**.PJMR.

[4]Senthil Kumar,Vasuki,2018-**An Application of MAHGOUB Transform in Cryptography.**Advances in Theoretical and Applied Mathematics.

[5]Eman A.Mansour,Noor Kadhim Meftin,2021-**Mathematical modeling for cryptography using Jafari transformation method.**Periodicals of Engineering and Natural Sciences.

[6]Abdelilah,Hassan Sedeeg,Mohand,Abdelrahim Mahgoub,Muneer Saif Saeed,2016-**An Application of the New Integral Aboodh Transform in Cryptography**.pure and Applied Mathematics Journal.

[7]Iman Ajel Mansour,Sadiq A.Mehdi,Emad Kuffi,2022-**Samarra Journal of Pure and Applied Science Applying SEE Integral Transform in Cryptography**.Samarra Journal of Pure and Applied Science.

[8]Anil Hiwarekar,2021-**New Method for Cryptography using Laplace-Elzaki Transform.**PSYCHOLOGY AND EDUCATION.

[9]Mirlinda Reqica,Diellza Berisha,Azir Jusufi,Meriton Reqica,2022-**Exploitation of exponential and logarithmic functions for data encryption and decryption**.IFAC.