The Ministry of Higher Education and Scientific Research
University of Qadisiyah
College of education
Department of Mathematics

Solve some Cryptograph problems by the Elzaki Transform

A Research submitted to the department of mathematics college of education as partial fulfillment of the requirements for the degree of bachelor of science in mathematics .

Search submitted by student:

YOUSEF BOLBOL DOHAN

Supervised

Alaa Kamel Jaber

2018

بسم الله الرحمن الرحيم

((وَقُلْ رَبِّ زِدْنِي عِلْمًا))

صدق الله العلي العظيم

سورة طه : ١١٤

الإهداء

إلى الحبيب المصطفى محمد صلى الله عليه وآله وسلم

إلى الذين وجوههم لغير الله ما توجهت ... وأقدامهم لغير الله ما سارت ... إلى كل من في الوجود بعد الله ورسوله والأئمة الميامين ..

إلى النور الذي ينير لي درب النجاح .. إلى نبع الحنان .. **أمي العزيزة**

إلى سندي وسر بهجتي ... القلب الكبير .. **أبي الحبيب**

الى الارواح الطاهرة ... **شهداء الوطن**

إلى من كان له الفضل في المساعدة على انجاز هذا البحث الأستاذ الفاضل

((علاء كامل جابر))

المشرف على البحث الذي كان له الفضل الكبير من خلال ملاحظاته الدقيقة

الى من صاغوا لنا من فكرهم منارات ومن معرفتهم اضاءات ومن جهودهم بدايات

انارت لنا طريق السعي لطلب العلم

أساتذتنا الكرام

شكر وتقدير

اشكر الله تعالى على نعمة العقل والتعلم

بدأنا بأكثر من يد وقاسينا أكثر من هم وعانينا الكثير من الصعوبات وها نحن اليوم والحمد لله نطوي سهر الليالي وتعب الأيام وخلاصة مشوارنا بين دفتي هذا العمل المتواضع

أتقدم بخالص شكري وامتناني إلى عمادة كلية التربية /رئاسة قسم الرياضيات في جامعة القادسية لإتاحتهم الفرصة لي لإكمال البحث ، كما أتقدم بخالص الامتنان إلى أساتذتي الكرام وبالأخص الأستاذ الفاضل

علاء كامل جابر

للمساعدة السديدة والملاحظات الدقيقة التي لولاها لما اكتمل البحث . .

كما اشكر زملائي وزميلاتي للأيام الجميلة التي قضيناها معا

الى كل من ساعدني في معلومة أو نصيحة

لكم مني كل الحب والتقدير

Abstract:

Cryptography is the science of providing security for information; it has been used historically as a means of providing secure communication between individuals. Message encryption has become very essential to avoid the threat against possible attacks by hackers during transmission process of the message. In this paper authors have proposed a method of cryptography, in which authors have used ELzaki Transformfor encrypting the plain text and corresponding inverse ELzaki Transformfor decryption.

Introduction:

Cryptography, the mathematics of encryption, plays an indispensable part in numerous fields, and a vast range of daily activities, such as electronic commerce, bank card payments and electronic building and so on. Cryptography is the only most important tool that avoids the threat against possible attacks by hackers during transmission process of the message, It is one of the cornerstones of Internet security. Cryptography is the only most important tool that avoids the threat against possible attacks by hackers during transmission process of the message.

Chapter one:

Basic Concepts

Chapter one:

Basic Concepts

1.1. Introduction

In this chapter, we will introduce some definitions and concepts about the cryptography in section 1.2 and the Cryptology was introduced in 1.3, while section 1.4 gives the types of cryptography and the section 1.5 discuss the classical cryptography. In section 1.6 some concepts about ELzaki Transform were introduced.

1.2. Cryptography

Cryptography [5-10] referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or cipher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text. (Fig.1) [11-15].

Fig. 1. Basic encryption and Decryption.

1.3. Cryptology:

Cryptology: The science (and art) of building and analyzing different encryption-decryption methods.

- Cryptography: “Secret writing”
- Cryptanalysis: “Breaking (understanding) of secret writing”
- Plaintext: A message in plain English or any other standard language that the public can understand.
- Encryption: The process of disguising a message to hide its substance. Typically, this does NOT include hiding the fact that a message is sent, which is known as stenography.
- Cipher text: The output of encrypting a plaintext message.
- Decryption: The process of recovering the plaintext from the cipher text using a secret key that only the receiver (and maybe the sender) has.

1.4. Types of Cryptography:

- Symmetric Cryptography
  - Deploy the same secret key to encrypt and decrypt messages
  - The secret key is shared between two parties
  - Encryption algorithm is the same as decryption algorithm
- Asymmetric (Public-key) Cryptography
  - Private key, Public key “2"
  - The secret key is not shared and two parties can still communicate using their public keys
  - Encryption alg. is different from decryption alg.

1.5. Classical Cryptography:

Three major methods (algorithms):

Substitution - Plaintext symbols are replaced with cipher text symbols using a substitution algorithm.

(e.g., If A=T, T = X, then AT = TX).

Transposition - Plaintext symbols are permuted (re-arranged) using a permutation algorithm.

(e.g., if position l=position 2, position 2 = position 1, then AT = TA)

Product - Uses alternate steps of substitution and transposition.

1.5.1. Substitution Ciphers:

Monalphabetic - Each symbol of the plaintext alphabet is mapped into a single cipher text symbol (Caesar cipher).

Homophonic - Each symbol is mapped into one of several possible cipher text symbols (or reverse) (Play fair).

Polyalphabetic - Each symbol is mapped into a cipher symbol as in the mono case, but the substitution changes For every symbol (variable substitution) (Vigenére).

Polygram - Symbol groups in plaintext are substituted for groups in cipher text (Hill).

1.5.2. Monoalphabetic Substitution Ciphers:

The key space is the set of all permutations on {O, l, 2, …… ,25 }. For a given key π and algorithm $E_k(P) = C$:

$E\,\pi\,(X_1X_2, ...X_n) = \pi\,(X_1)\,\pi\,(X_2)\,\pi\,(X_n)$, and

D π (y_1y_2-y_n) = π^{-1} (y_1) π^{-1} (y_2)- π^{-1} (y_n)

Caesar: C = E_k(P) = (P + k) mod 26

Where:

C = cipher text symbol, P= Plaintext symbol “

k = O≤ k≤ 26, E = (P+k)mod 26

1.6.3. Caesar Cipher:

The symbol key relationship is defined numerically:

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Suppose K = 11, P = wewillmeetatmidnite

E Algorithm is (P + k)mod 26

Text =224228111112 4 41901912 8 313 8 6 719

Add11 715719222223151541l4 231914241917184

Cipher= HPHTWW X P P ELE X T O Y T R SE

1.6. ELzaki Transform

Elzaki transform was introduced by Tarig ELzaki in 2013. ELzaki Transformis a widely used integral transform in mathematics and electrical engineering that transforms a function of time into a function of complex frequency. The inverse ELzaki Transform takes a complex frequency domain function and yields a function defined in the time domain.

Definition: Consider functions in the set A defined by

$$A = \left\{ f(t): \exists M, k_1, k_2 > 0, |f(t)| < Me^{\frac{|t|}{K_j}}, if\ t\ \in (-1)\ X\ [0,\infty) \right\}$$

For a given function in the set M must be finite number, k_1, k_2 may be finite or infinite. ELzaki Transform denoted by the operator E[.] is defined by the integral equation

$$E[f(t)] = T(u) = u\int_0^{\infty} f(t)e^{\frac{t}{u}}dt\,, t \geq 0\,, k_1 \leq u \leq k_2$$

1.6.1. Properties of ELzaki Transform:

- Linearity: ELzaki Transformis a linear transformation which means that the transform of a sum of waveforms is the sum of their transforms. Stated formally the linearity property is

  $$A[a.f(t) + b.g(t)] = a.A[f(t)] + b.A[g(t)]$$

  Where $a\ and\ b$ are constants. The above result can easily be generalized to more than two functions.

- ELzaki Transformation & Inverse ELzaki Transform of some elementary functions:-

  a) $let\ f(t) = 1\,, then: E(1) = u\int_0^{\infty} e^{\frac{-1}{u}}dt = u\left[-ue^{\frac{-1}{u}}\right]_0^{\infty} = u^2$

  b) $left\ f(t) = t\,, then: E(t) = u\int_0^{\infty} e^{\frac{t}{u}}dt,$

  Integrating by parts to find that : $E(t) = u^3$

  In the general case if $n > 0$ is integer number, then .

  $$E(t^n) = n!\ u^{n+2}$$

  c) $E^{-1}(u^2) = 1$

  $E^{-1}(u^3) = t$

  $E^{-1}(u^{n+2}) = \dfrac{t^n}{n1}$

Chapter tow

Application of ELzaki Transform in the Cryptograph Problem

Chapter tow:

Application of ELzaki Transform in the Cryptograph Problem

2.1. Intoduction

In the present chapter, a new cryptographic scheme is proposed using ELzaki Transform [1-4]. ELzaki Transform is used for encrypting the plain text and corresponding inverse ELzaki Transform is used for decryption. An example was introduced to illustrate this technique.

2.2. Proposed Technique

Proposed algorithm provides as many transformations as per the requirements, which are the most useful factor for changing key. Therefore, it is very difficult for an eyedropper to trace the key by any attack. The implementation has been done in Matlab program.

2.2.1 Encryption Algorithm

I) Treat every letter in the plain text message as a number, so that A = 1, B = 2, C = 3, … Z = 26, [space] = 0.

II) The plain text message is organized as finite sequence of numbers based on the above conversion. For example our text is "DEFINED". Based on the above step; we know that,

$$D = 4 \ , E = 5 \ , F = 6 \ , I = 9 \ , N = 14 \ , E = 5 \ , D = 4$$

Therefore our plaintext finite sequence is

$$4 \ , 5 \ , 6 \ , 9 \ , 14 \ , 5 \ , 4$$

III) If n + 1 is the number of term in the sequence; consider a polynomial of degree nwith coefficient as the term of the given finite sequence. Above finite sequence contains 7 + 1 terms. Hence consider a polynomial p(t) of degree 7.

$p(x) = 4 + 5x + 6x^2 + 9x^3 + 14x^4 + 5x^5 + 4x^6$

Take Elzaki transform of polynomial p(x).

$E(p(x)) = E(4 + 5x + 6x^2 + 9x^3 + 14x^4 + 5x^5 + 4x^6)$

$= E(4) + E(5x) + E(6x^2) + E(9x^3) + E(14x^4) + E(5x^5) + E(4x^6)$

$= 4u^2 + 5u^3 + 12u^4 + 54u^5 + 336u^6 + 600u^7 + 2880u^8$

$$= \sum_{i=1}^{7+1} qi\, u^{i+1}$$

Next find r_i such that $q_i \equiv r_i \bmod 26$ for each i, $1 \leq i \leq n + 1$. Therefore q1 = 4

$$\equiv 4 \bmod 26 \ , \quad q2 = 5 \equiv 5 \bmod 26 \quad q3 = 12 \equiv 12 \bmod 26 \ , \ q4 = 54 \equiv 54 \bmod 26$$

$$q5 = 336 \equiv 336 \bmod 26 \ , q6 = 600 \equiv 600 \bmod 26 \ , q7 = 2880 \equiv 2880 \bmod 26$$

IV) Hence $q_i = 26k_i + r_i$. Thus we get a key k_i for

i = 1, 2, 3, … , n + 1.

$$\therefore k = 0 \ , k2 = 0 \ , k3 = 0 \ , k4 = 2 \ , \quad k5 = 12 \ , \ k6 = 23 \ , \ k7 = 110$$

Now consider a new finite sequence $r_1, r_1, r_1, \ldots, r_{n+1}$ i.e.

4 , 5 , 12 , 2 , 24 , 2 , 20

Then the cipher text is DELBXBT

2.2.2. Decryption Algorithm

I) Consider the cipher text and key received from sender. In the above example cipher text is " D E L B X B T " and key is 0 , 0, 0, 2, 12, 23, 110.

II) Convert the given cipher text to corresponding finite sequence of numbers $r_1, r_1, r_1, \ldots, r_{n+1}$

4 , 5 , 12 , 2 , 24 , 2 , 20

III) Let $q_i = 26k_i + r_i, \forall i = 1, 2, 3, \ldots, n+1$.

$$q_1 = 26(0) + 4 = 4 \text{ , } q_2 = 26(0) + 5 = 5, \; q_3 = 26(0) + 12 = 12,$$

$$q_4 = 26(2) + 2 = 54 \text{ , } q_5 = 26(12) + 24 = 336 \text{ , } q_6 = 26(23) + 2 = 600,$$

$$q_7 = 26(110) + 20 = 2880 .$$

lV)

$$\sum_{i=1}^{7+1} qi\, u^{i+1}$$

$$= 4\,u^2 + 5\,u^3 + 12\,u^4 + 2\,u^5 + 24\,u^6 + 2\,u^7 + 20\,u^8$$

V) Now take the Inverse Elzak transform of p(v).

$$E^{-1}\,(p\,(u), x) = E^{-1}\,(= 4\,u^2 + 5\,u^3 + 12\,u^4 + 2\,u^5 + 24\,u^6 + 2\,u^7 + 20u^8)$$

$$= 4\,E^{-1}\,u^2 + 5\,E^{-1}\,u^3 + 12\,E^{-1}\,u^4 + 2\,E^{-1}\,u^5 + 24\,E^{-1}\,u^6 + 2\,E^{-1}\,u^7 + 20\,E^{-1}\,u^8$$

$$P(x) = 4 + 5x + 6x^2 + 9x^3 + 14x^4 + 5x^5 + 4x^6$$

VI) Consider the coefficient of a polynomial p(x) as a finite sequence.

4 , 5 , 6 , 9 , 14 , 5 , 4

VII) Now translating the number of above finite sequence to alphabets. We get the original plain text as “DEFINED”.

2.3. Implementation of the Algorithm

Programming language is one of the most widely use high level language today because of its advantages [16]. In this part program has been written in Matlab program, for the implementation of the Encryption Algorithm and Implementation Decryption Algorithm.

2.3.1. Implementation Encryption Algorithms

```
function [Crp_Msg,Qi]=crp(b)
syms x t s
a='abcdefghijklmnopqrstuvwxyz';
```

```
n=length(b);
for i=1:n
   ind(i)=find(a==b(i));
end
ind1=ind(n:-1:1);
f1=poly2sym(ind1,t);
f2=laplace(f1,t,x)*x^n;
ind2=sym2poly(f2);
ri=mod(ind2-1,26)+1;
qi=(ind2-ri)/26;
for i=1:n
   b2(i)=a(ri(i));
end
Crp_Msg=b2;
Qi=qi;
```

2.3.2. Implementation Decryption Algorithms

```
function Incrp_Msg=incrp(b2,qi)
 syms x t s
 n=length(b2);
 a='abcdefghijklmnopqrstuvwxyz';
 for i=1:n
    ind3(i)=find(a==b2(i));
 end
 ind4=qi*26+ind3;
 f3=poly2sym(ind4)/x^n;
 f4=ilaplace(f3,x,t);
 ind5=sym2poly(f4);
 b3=a(ind5(n:-1:1));
 Incrp_Msg=b3;
```

References :

[1] A. P. Hiwarekar "A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM"International Journal of Mathematical Archive-3 (3), 2012, Page: 1193-1197.

[2] A. P. Hiwarekar, A NEW METHOD OF CRYPTOGRAPHY USING LAPLACE TRANSFORM, International Journal of Mathematical Archive-3 (3), 2012, Page: 1193-1197.

[3] A. P. Hiwarekar, Application of Laplace Transform For Cryptographic Scheme, Proceedings of the World Congress on Engineering 2013 Vol I, WCE 2013, July 3 - 5, 2013, London، U.K.

[4] A. P. Stakhov, "The golden matrices and a new kind of cryptography", Chaos, Soltions and Fractals.

[5] A.Kilicman and H.E.Gadain. An application of double Laplace transform and sumudu transform, Lobachevskii J. Math.30 (3) (2009), pp.214-223.

[6] Abdulkadir Baba HASSAN, Matthew Sunday ABOLARIN، Onawola Hassan JIMOH, The Application of Visual Basic Computer Programming Language to Simulate Numerical Iterations, Leonardo Journal.

[7] Adomian, G., 1994. Solving Frontier Problems of Physics: The Decomposition Method, Kluwer Acad. Publ. Boston.

[8] Aghili, B. Salkhordeh Moghaddam, Laplace transform Pairs of Ndimensions and second order Linear partial differential equations with constant coefficients , Annales Mathematicae et Informaticae, 35 (2008),pp,310.

[9] Barr T. H., Invitation to Cryptography, Prentice Hall, (2002.(

[10] Blakley G. R., Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedingsof the IEEE Symposium, 9-12, May 1999.

[11] Overbey J. - Traves W. and Wojdylo J. – On the Key space of the Hill Cipher, Cryptologia, 29 (1), January 2005, 59-72.

[12] Petersen K. – Notes on Number Theory and Cryptography، http://www.math.unc.edu/ Faculty petersen/ Coding/cr2.pdf.

[13] Some new solutions of the higher-order Sawada-Kotera equation via the Exp-function method, Middle-East J. Scientific Research, 11(12): 1659-1667.

[14] Stallings W., Cryptography and Network Security, Fourth Edition, Prentice Hall, 2005.

[15] Swati Dhingra, Archana A. Savalgi, Swati Jain, Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications Volume 136 – No. 7, February 2016.

[16] Yasir Khan, 2009. An effective modification of the Laplace decomposition method for nonlinear equations, International Journal of Nonlinear Sciences and Numerical Simulation, 10: 73-1376.