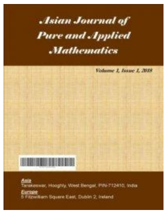

Asian Journal of Pure and Applied Mathematics

3(1): 13-18, 2021; Article no.AJPAM.518

An Application of Integral Transform Based Method in Cryptograph

Akinola Emmanuel Idowu[1*], Alao Saheed[2], Oderinu Rasaq Adekola[2] and Folorunso Esther Omofa[1,2]

[1]Mathematics Programme Bowen University Iwo, Osun State, Nigeria.
[2]Department of Pure and Applied Mathematics, Ladoke Akintola University of Technology Ogbomoso, Oyo State, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. Aauthors AEI, ORA and AS designed the study and wrote the algorithm, author FEO wrote the protocol and the first draft of the manuscript. All authors read and approved the final manuscript.

Received: 05 June 2021
Accepted: 11 August 2021
Published: 16 August 2021

Original Research Article

Abstract

Information security and confidentiality in our day-to-day activities cannot be overemphasis due to the ways hackers are intruding into several messages and information that ought to be personal or confidential. Hence there is a need to write or make the information secret or hidden as much as possible. Cryptography provides a resounding solution to this aforementioned problem by certifying that messages and information shared or transferred remain confidential. In this research work a mathematical approach is being proposed to encrypt and decrypt information using an integral transform called "Kamal Transform" for encrypting the plain text and its corresponding inverse transform for decryption alongside congruence modulo operator as a means of protecting and securing valuable data or information from hackers.

Keywords: Integral transform; kamal transform; cryptography; congruence modulo; decrypt; encrypt.

1 Introduction

There is no doubt that the world is now a global village and communication has become more easier than ever imagine visa vis advancement in technology through various means. But the major concern of all and sundry is the issue of confidentiality and safety of their messages or information due to the prevalence of hackers hence the cryptographic.

**Corresponding author: E-mail: emmanuel.idowu@bowen.edu.ng;*

Cryptography is the science of transmission and reception of secrete message- Encrypting and Decrypting. It has been used for providing secure communication between individuals [1-5]. An encryption algorithm or cipher is a means of transforming plain text into cipher text under the control of a secret key. The reverse process is called decryption.

In this research work, the concept of encrypting and decrypting a message by using a new integral transform called Kamal transform was examined [6,7]. Kamal Transform was derived by Abdelilah Kamal from the classical Fourier integral. Based on its mathematical simplicity Kamal transform was introduced to facilitate the process of solving ordinary and partial differential equations in the time domain.

2 Kamal Transform

A new transform called the Kamal transform defined for function of exponential order, consider functions in the set *A* defined by:

$$A\left\{ f(t) : \exists M, k_1, k_2 > 0. \left| f(t) \right| < Me^{\frac{|t|}{k_j}}, if \quad t \in (-1)^j \times [0, \infty) \right\} \qquad (1)$$

For a given function in the set A, the constant M must be finite number, k_1, k_2 may be finite or infinite

The Kamal transform denoted by the operator $K(\bullet)$ defined by the integral equation:

$$K[f(t)] = G(v) = \int_0^\infty f(t) e^{\frac{-t}{v}} dt, \qquad t \geq 0, \qquad k_1 \leq v \leq k_2 \qquad (2)$$

The variable v in this transform is used to factor the variable t in the argument of the function f. This transform has deeper connection with the Laplace, Elzaki, Aboodh, Mahgoub transforms [8-12].

2.1 Kamal Transform and Kamal Inverse of Some Elementary Functions

For any function $f(t)$, we assume that the integral (2) exist. The sufficient conditions for the existence of Kamal transform are that $f(t)$ for $t \geq 0$ be piecewise continuous and of exponential order.

(i) Let $f(t) = 1$,

by definition we have:

$$K[1] = G(v) = \int_0^\infty e^{\frac{-t}{v}} dt = \left[ve^{\frac{-t}{v}} \right]_0^\infty = v$$

It inverse is given as $K^{-1}[v] = 1$

(ii) Let $f(t) = t$, then:

$$K\left[t\right]=G\left(v\right)=\int_{0}^{\infty}te^{\frac{-t}{v}}dt=\left[ve^{\frac{-t}{v}}\right]_{0}^{\infty}=-tve^{\frac{-t}{v}}\Big|_{0}^{\infty}+\int_{0}^{\infty}ve^{\frac{-t}{v}}dt=0+v^{2}=v^{2}$$

The inverse is $K^{-1}\left[v^{2}\right]=t$

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

(iii) $K\left[t^{n}\right]=\int_{0}^{\infty}t^{n}e^{\frac{-t}{v}}dt=n!v^{n+1}$

The inverse is

$$K^{-1}\left[n!v^{n+1}\right]=t^{n}$$

or

$$K^{-1}\left[v^{n+1}\right]=\frac{t^{n}}{n!}$$

3 Methodology

The details of the procedure or algorithm to be applied in encrypting and decrypting the problem to be considered under the next section are itemized below:

Encryption:

(i) Assign every letter in the plain text to encrypt as a number in such a way that A = 1, B = 2, C = 3, … Z = 26 and space= 0. Thus, the original message is now converting into a finite sequence of numbers.

(ii) Suppose n is the number of terms in the sequence, we then consider a polynomial $y(t)$ of degree (n-1) with coefficients as the term of the given finite sequence

(iii) Apply Kamal transform to polynomial $y(t)$ in (ii) and obtain the general terms for Kamal Transform $G[v]$

(iv) For each i, find quotient k_i and remainder q_i such that $d_i=26k_i+q_i$. Hence the finite sequence $k_1,k_2,k_3,...,k_n$ forms the Key [13]

(v) Consider a new finite sequence of numbers $q_1,q_2,q_3,...,q_n$. Using step (i) given above to convert the numbers of the new sequence into text called as cipher text.

Decryption:

(vi) Convert the cipher text obtained in (v) above in to corresponding finite sequence of numbers as we did in (i)

(vii) Using key k_i and the values of q_i to find d_i

(viii) Apply inverse Kamal transform to $G[v]$ obtain from (ii) to get $y\left(t\right)=K^{-1}\left[f\left(t\right)\right]$

(ix) The coefficients of $y\left(t\right)$ is then consider as a finite sequence of numbers

(x) Using the same step as in (i) of the encryption given above to get the original message

4 Application

Illustration 1. **NO TO EVIL**

From the steps itemized above the plain text message is now:
14,15,0,20,15,0, 5,22,9,12

The number of terms of the sequence $n+1=10$, $n=9$, then the polynomial $y(t)$ would be of degree 9. So,

$$y(t)=14+15t+0t^2+20t^3+15t^4+0t^5+5t^6+22t^7+9t^8+12t^9 \qquad (3)$$

Taking the Kamal Transform of (3) to have

$$G(v)=14v+15v^2+0\times 2!v^3+20\times 3!v^4+15\times 4!v^5+0\times 5!v^6+5\times 6!v^7+22\times 7!v^8+9\times 8!v^9+ 12\times 9!v^{10} \qquad (4)$$

$$G(v)=14v+15v^2+0v^2+120v^4+360v^5+0v^6+3600v^7+110880v^8+362880v^9+ 4354560v^{10} \qquad (5)$$

$$G(v)=\sum_{i=1}^{10} d_i v^i \qquad (6)$$

We find q_i such that $d_i = q_i \bmod 26$ for each i, $1 \le i \le n+1$,

Therefore,

$$d_1 = 14 = 14 \bmod 26, \quad d_2 = 15 = 15 \bmod 26 \quad d_3 = 0 = 0 \bmod 26,$$
$$d_4 = 120 = 16 \bmod 26, \; d_5 = 360 = 22 \bmod 26, \; d_6 = 0 = 0 \bmod 26,$$
$$d_7 = 3600 = 12 \bmod 26, \qquad d_8 = 110880 = 16 \bmod 26, \qquad d_9 = 362880 = 24 \bmod 26,$$
$$d_{10} = 4354560 = 2 \bmod 26$$

For each i we shall find quotient k_i such that $d_i = 26k_i + q_i$ so we have

$$d_1 = 26k_i + q_i$$
$$14 = 26 \times k_i + 14, \qquad 15 = 26 \times k_2 + 15$$
$$k_1 = 14, \qquad k_2 = 15$$

Following the same procedure, we have,

$$k_3 = 0, k_4 = 4, k_5 = 13, k_6 = 0, k_7 = 138, k_8 = 4264, k_9 = 13956, k_{10} = 167483,$$

The key is $14, 15, 0, 4, 13, 0, 138, 4264, 13956, 167483$

And the new finite sequence q_i is now written as $14,15,0,16,22,0,12,16,24,2$

Hence the original plain text **NO TO EVIL** is now resulted into a cipher text **NO PV LPXB** according to (i)

Therefore, the sender sends encrypting text **NO PV LPXB** alongside equation (10) publicly but at the same time privately send the unlock key and Kamal Transform [6].
To unravel the cipher text received, the receiver follows the following steps:

Use (i) to convert the cipher text **NO PV LPXB** to a finite sequence given as 14,15,0,16,22,0,12,16,24,2.

Apply (vii) on $d_i = 26k_i + q_i$ to find d_i and thereby obtain back

$$G(v) = 14v + 15v^2 + 0v^2 + 120v^4 + 360v^5 + 0v^6 + 3600v^7 + 110880v^8 + 362880v^9 + 4354560v^{10} \tag{7}$$

Apply Kamal inverse transform on (7) to eventually have,

$$K^{-1}\left[G(v)\right] = y(t) = 14 + 15t + 0t^2 + 20t^3 + 15t^4 + 0t^5 + 5t^6 + 22t^7 + 9t^8 + 12t^9 \tag{8}$$

Write out the coefficients of (8) as a finite sequence to have.

$14,15,0,20,15,0,5,22,9,12$

The procedure (i) is then employed to have the original message as:

NO TO EVIL

5 Conclusion

So far in this research work, we have discussed the application of new integral transform-Kamal transform in Cryptography at the same time use it for encrypting the plain text and its corresponding inverse used for decryption through the help of a private key which is the number of multiples of modulo 26. The result obtained showed that Kamal Transform is a powerful tool which can be employed to tackle the issues of message or communication insecurity posed by hackers.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Bodkhe DS, Panchal SK. Use of Sumudu Transform in Cryptography, Bulletin of the Marathwada Mathematical Science. 2015;16(1):1-6.

[2] Hiwarekar AP. A new method of Cryptography using Laplace Transform, Intr. J. Math. Arch. 2012;3(3):1193-1197.

[3] Naga Lakshmi G, Ravi Kumar B, Chandra Sekhar A. A cryptographic Scheme of Laplace Transforms, Intr. J. Math. Arch. 2011;2(12):2515-2519.

[4] Abdelilah K, Hassan Sedeeg, Mohand M.,Abdelrahim Mahgoub, Munner A Saif Saeed. An Application of the New Integral Aboodh Transform in Cryptography, Pure and Applied Mathematics Journal. 2016;5(5):151-154.

[5] Burton DM. Elementary Number Theory, Tata McGraw Hill, New Delhi. K; 2002.

[6] Abdelilah, Hassan S. The new integral transform Kamal Transform, Advances in Theoretical and Applied Mathematics. 2016;11(4):451-458.

[7] Ahmad A, Kamal Adomian. Decomposition method for solving nonlinear wave-like equation with variable coefficients. Journal of Advances in Mathematics and Computer Science. 2019;1-11.

[8] Naga Lakshmi G, Ravi Kumar B, Chandra Sekhar A. A cryptographic Scheme of Laplace Transforms, Intr. J. Math. Arch. 2011;2(12):2515-2519.

[9] Tarig M Elzaki. The new integral transform elzaki transform, Global Journal of Pure and Applied Mathematics. 2011;7(1):57–64.

[10] Mohand M, Abdelrahim Mahgoub. The new integral transform mahgoub transform, Advances in Theoretical and Applied Mathematics. 2016;11(4):391–398.

[11] Tarig M Elzaki, Salil M Elzaki, Elnour EA. On the new integral transform elzaki transform fundamental properties investigations and applications, Global Journal of Mathematical Sciences: Theory and Practical. 2012;4(1):1-13.

[12] Tarig M Elzaki, Salil M Elzaki. On the connection between Laplace and Elzaki Transforms, Advances in Theoretical and Applied Mathematics. 2011;6(1):1-10.

[13] Stallings W. Cryptography and Network Security, Prentice Hall (4th Ed.); 2005.