ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 6, Issue 3, pp: (182-186), Month: July - September 2018, Available at: www.researchpublish.com

Application of 'Kamal' Transform in Cryptography

P. Senthil Kumar[1], S. Vasuki[2]

[1] Professor, Department of Mathematics, SNS College of Technology

[2] Student, B.Tech (Information Technology), Sri Ramakrishna Engineering College

[1,2] Coimbatore, Tamil Nadu, India

***Abstract*: Cryptography is the science of using mathematics to encrypt and decrypt data (message). The art of science that concealing the messages to introduce secrecy in information security is recognized as cryptography. This paper aims to encrypt and decrypt a message by using a new integral transform "Kamal" transform and congruence modulo operator.**

***Keywords*: Caesar Cipher, Kamal transform.**

1. INTRODUCTION

Cryptography is the study of secret messages. A message is a plaintext or clear text. An encryption algorithm or cipher, is a means of transforming plain text into cipher text under the control of a secret key. This process is called an encryption. The encrypted message is called cipher text. The reverse process is called decryption. A Cipher is an algorithm for performing encryption or decryption in a series of well-defined steps that can be followed as a procedure. One of the earliest ciphers is called the Caesar cipher [6] or Shift cipher. In this scheme, encryption is performed by replacing each letter by the letter a certain number of places on in the alphabet. For example, if the key was three, then the plain text A would be replaced by the cipher text D, the next letter B would be replaced by E and so on. This is the process of making a message secret. This can be represented mathematically as $p(t) = (t + k) mod\ 26$. The function p that assigns to the non-negative integer $t, t \le 26$, the integer in set { 1,2,3,…26 } with $p(t) = (t + k) mod\ 26$.

In this paper, our research concept to encrypt and decrypt a message by using a new integral transform Kamal transform [8]. Kamal transform is derived from the classical Fourier integral and is widely used in applied mathematics and engineering fields. This transform has deeper connection with Laplace, EL-zaki [1], Mahgoub [2] and Aboodh transforms [3]. Based on the mathematical simplicity of this transform and its fundamental properties, we have to apply encryption and decryption algorithms to get the message in a simple way. Shaikh Jamir Salim, et.al [4] and Uttam Dattu Kharde [7] proposed a method to encrypt and decrypt a plain text message by using Elzaki transform. Abdelilah K. Hassan Sedeeg, et.al [5] proposed a method by using Aboodh transform. P. Senthil Kumar and S. Vasuki [9] proposed a encryption and decryption procedure by using Mahgoub transform

2. KAMAL TRANSFORM

The Kamal transform is defined for the function of exponential order. We consider functions in the set A defined by

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

where the constant M must be finite number, k_1 , k_2 may be finite or infinite.

The Kamal transform denoted by the operator K(.) defined by the integral equation

$$K\,[\,f(t)] = G(v) = \int_0^\infty f(t)\, e^{-\frac{t}{v}}\, dt\,, t \geq 0\,, k_1 \leq v \leq k_2 \quad (1)$$

2.1 Some Standard Functions:

For any function $f(t)$, we assume that the integral equation (1) exist.

(i) Let $f(t) = 1$ then K [1] = v

(ii) Let $f(t) = t$ then K [t] = v^2

(iii) Let $f(t) = t^2$ then K [t^2] = 2 v^3 = 2! v^3

(iv) In general case, if n > 0, then K [t^n] $= n!\ v^{n+1}$

2.2 Inverse Kamal transform:

(v) $K^{-1}[v] = 1$

(vi) $K^{-1}[\,v^2\,] = t$

(vii) $K^{-1}\,[\,v^3\,] = \frac{t^2}{2\,!}$

(viii) $K^{-1}\,[\,v^4\,] = \frac{t^3}{3\,!}$ and so on.

3. ENCRYPTION ALGORITHM

(I) Assign every alphabet in the plain text message as a number like A = 1, B = 2, C = 3, … Z = 26, and space = 0

(II) The plain text message is organized as a finite sequence of numbers based on the above conversion.

(III) If n is the number of terms in the sequence, then consider a polynomial $p(t)$ of degree n – 1

(IV) Now replace each of the numbers t by $p(t) = (\,t + k) mod\ 26$

(V) Apply Kamal transform of polynomial $p(t)$

(VI) Find r_i such that $q_i \equiv r_i\ mod\ 26$ for each $i, 1 \leq i \leq n$

(VII) Consider a new finite sequence $r_1, r_2, r_3, \ldots\ r_n$

(VIII) The output text message is in cipher text.

4. DECRYPTION ALGORITHM

(I) Convert the cipher text in to corresponding finite sequence of numbers $r_1, r_2, r_3, \ldots\ r_n$

(II) Let $q_i = 26\ c_i + r_i\,, \forall\ i = 1,2,3, \ldots n$

(III) Let $p(t) = \sum_{i=1}^{n} q_i v^i$

(IV) Take the inverse Kamal transform

(V) The coefficient of a polynomial $p(t)$ as a finite sequence

(VI) Now replace each of the numbers by $p^{-1}(t) = (\,t - k) mod\ 26$

(VII) Translate the number of the finite sequence to alphabets. We get the original text message.

5. PROPOSED METHODOLOGY

5.1 Example (1)

Consider the plain text message is **" STUDENT "** .

5.1.1 Encryption Procedure:

Now the corresponding finite sequence is 19, 20, 21, 4, 5, 14, 20. The number of terms in the sequence is 7. That is n = 7. Consider a polynomial of degree n – 1 with coefficient as the term of the given finite sequence. Hence the polynomial $p(t)$ is of degree 6. The above finite sequence shift by k letters (k = 3), this results 22, 23, 24, 7, 8, 17, 23.

Now the polynomial $p(t)$ is $p(t) = 22 + 23.t + 24.t^2 + 7.t^3 + 8.t^4 + 17.t^5 + 23.t^6$

Take Kamal transform on both sides

K $[p(t)] = K\{ 22 + 23.t + 24.t^2 + 7.t^3 + 8.t^4 + 17.t^5 + 23.t^6 \}$

= 22 K[1] + 23 K [t] + 24 K [t^2] + 7 K [t^3] + 8 K [t^4] + 17 K [t^5] + 23 K [t^6]

= $22\,v + 23\,v^2 + 48\,v^3 + 42\,v^4 + 192\,v^5 + 2040\,v^6 + 16560\,v^7$

K [$p(t)$] = $\sum_{i=1}^{7} q_i\, v^i$, where $q_1 = 22, q_2 = 23, q_3 = 48$, $q_4 = 42$, $q_5 = 192$, $q_6 = 2040, q_7 = 16560$,

Find r_i such that $q_i \equiv r_i \bmod 26$

$$q_1 = 22\,, 22 \equiv 22 \bmod 26 \Rightarrow r_1 = 22$$

$$q_2 = 23\,, 23 \equiv 23 \bmod 26 \Rightarrow r_2 = 23$$

$$q_3 = 48\,, 48 \equiv 22 \bmod 26 \Rightarrow r_3 = 22$$

$q_4 = 42\,, 42 \equiv 16 \bmod 26 \Rightarrow r_4 = 16$

$$q_5 = 192\,, 192 \equiv 10 \bmod 26 \Rightarrow r_5 = 10$$

$$q_6 = 2040\,, 2040 \equiv 12 \bmod 26 \Rightarrow r_6 = 12$$

$q_7 = 16560\,, 16560 \equiv 24 \bmod 26 \Rightarrow r_7 = 24$

Now consider a new finite sequence is $r_1, r_2, r_3, \ldots r_7$. That is, 22, 23, 22, 16, 10, 12, 24 and the key (c_i) is 0, 0, 1, 1, 7, 78, 636. The corresponding cipher text is **" VWVPJLX "**

5.1.2 Decryption Procedure:

To recover the original message encrypted by Caesar cipher, the inverse p^{-1} is used. For that, take the finite sequence corresponding to cipher text is 22, 23, 22, 16, 10, 12, 24.

Let $q_i = 26\, c_i + r_i\,, \forall\, i\,, i = 1, 2, 3\,, \ldots n$

$q_1 = 26 \times 0 + 22 = 22$

$q_2 = 26 \times 0 + 23 = 23$

$q_3 = 26 \times 1 + 22 = 48$

$q_4 = 26 \times 1 + 16 = 42$

$q_5 = 26 \times 7 + 10 = 192$

$q_6 = 26 \times 78 + 12 = 2040$

$q_7 = 26 \times 636 + 24 = 16560$

Let $K[p(t)] = \sum_{i=1}^{7} q_i\, v^i$

= $22\,v + 23\,v^2 + 48\,v^3 + 42\,v^4 + 192\,v^5 + 2040\,v^6 + 16560\,v^7$

Take inverse Kamal transform on both sides, we get

$p(t) = K^{-1}\{ 22\, v + 23\, v^2 + 48\, v^3 + 42\, v^4 + 192\, v^5 + 2040\, v^6 + 16560\, v^7 \}$

$\boldsymbol{p(t) = 22 + 23t + 24t^2 + 7t^3 + 8t^4 + 17t^5 + 23t^6}$

The coefficient of a polynomial p(t) as a finite sequence 22, 23, 24, 7, 8, 17, 23. Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (t-3) mod\ 26$. The corrected new finite sequence is 19, 20, 21, 4, 5, 14, 20. Now by translating the numbers to alphabets. We get the original plain text message **"STUDENT"**

5.2 Example (2)

Consider the plain text message is **" BROTHER "** .

5.2.1 Encryption Procedure:

Now the corresponding finite sequence is 2,18,15,20,8,5,18. The number of terms in the sequence is 7. That is n = 7. Consider a polynomial of degree n – 1 with coefficient as the term of the given finite sequence. Hence the polynomial $p(t)$ is of degree 6. The above finite sequence shift by k letters (k = 5), this results 7, 23, 20, 25, 13, 10, 23

Now the polynomial is

$p(t) = 7 + 23.t + 20.t^2 + 25.t^3 + 13.t^4 + 10.t^5 + 23.t^6$

Take Kamal transform on both sides

K $[p(t)] = K\{7 + 23.t + 20.t^2 + 25.t^3 + 13.t^4 + 10.t^5 + 23.t^6\}$

= 7 K[1] + 23 K [t] + 20 K [t^2] + 25 K [t^3] + 13 K [t^4] + 10 K [t^5] + 23 K [t^6]

= $7v + 23\, v^2 + 40\, v^3 + 150\, v^4 + 312\, v^5 + 1200\, v^6 + 16560\, v^7$

K [$p(t)$] = $\sum_{i=1}^{7} q_i\, v^i$, where $q_1 = 7$, $q_2 = 23$, $q_3 = 40$, $q_4 = 150$, $q_5 = 312$, $q_6 = 1200$, $q_7 = 16560$

Find r_i such that $q_i \equiv r_i\, mod\ 26$

$$q_1 = 7\,,7 \equiv 7\, mod\ 26 \Rightarrow r_1 = 7$$

$$q_2 = 23\,,23 \equiv 23\, mod\ 26 \Rightarrow r_2 = 23$$

$$q_3 = 40\,,40 \equiv 14\, mod\ 26 \Rightarrow r_3 = 14$$

$$q_4 = 150\,,150 \equiv 20\, mod\ 26 \Rightarrow r_4 = 20$$

$$q_5 = 312\,,312 \equiv 0\, mod\ 26 \Rightarrow r_5 = 0$$

$$q_6 = 1200\,,1200 \equiv 4\, mod\ 26 \Rightarrow r_6 = 4$$

$q_7 = 16560\,,16560 \equiv 24\, mod\ 26 \Rightarrow r_7 = 24$

Now consider a new finite sequence is $r_1, r_2, r_3, \ldots r_7$ .That is, 7,23,14,20,0,4,24 and the key (c_i) is 0,0,1,5,12,46,636

The corresponding cipher text is **" GWNT DX "**

5.2.2 Decryption Procedure:

To recover the original message encrypted by Caesar cipher, the inverse p^{-1} is used. For that, take the finite sequence corresponding to the cipher text is 7,23,14,20,0,4,24

Let $q_i = 26\, c_i + r_i\,, \forall\, i\,, i = 1,2,3\,, \ldots n$

$q_1 = 26 \times 0 + 7 = 7$

$q_2 = 26 \times 0 + 23 = 23$

$q_3 = 26 \times 1 + 14 = 40$

$q_4 = 26 \times 5 + 20 = 150$

$q_5 = 26 \times 12 + 0 = 312$

$q_6 = 26 \times 46 + 4 = 1440$

$q_7 = 26 \times 636 + 24 = 16560$

Let $K[p(t)] = \sum_{i=1}^{7} q_i \, v^i$

$= 7v + 23\, v^2 + 40\, v^3 + 150\, v^4 + 312\, v^5 + 1200\, v^6 + 16560\, v^7$

Take inverse Kamal transform on both sides, we get

$p(t) = K^{-1}\{ 7v + 23\, v^2 + 40\, v^3 + 150\, v^4 + 312\, v^5 + 1200\, v^6 + 16560\, v^7 \}$

$\boldsymbol{p(t) = 7 + 23t + 20t^2 + 25t^3 + 13t^4 + 10t^5 + 23t^6}$

The coefficient of a polynomial p(t) as a finite sequence 7,23,20,25,13,10,23. Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (t - 5) mod\ 26$. The corrected new finite sequence is 2,18,15,20,8,5,18. Now translating the numbers to alphabets. We get the original plain text message **" BROTHER "**

6. CONCLUSION

In this proposed work, a cryptographic scheme (Caesar cipher) with a new integral transform Kamal transform with congruence modulo operator is introduced. Two examples with different text messages are given and the results are verified.

REFERENCES

[1] Tarig. M.Elzaki., "The New Integral Transform ELzaki Transform", Global Journal of Pure and Applied Mathematics, Vol. 7, No.1, pp. 57 – 64, 2011

[2] Mohand M. Abdelrahim Mahgoub., "The New Integral Transform Mahgoub Transform", Advances in Theoretical and Applied Mathematics, Vol. 11, No.4, pp. 391 – 398, 2016

[3] Khalid Suliman Aboodh., " The New Integral Transform Aboodh Transform", Global Journal of Pure and Applied Mathematics, Vol.9, No.1, pp. 35 – 43, 2013

[4] Shaikh Jamir Salim., and Mundhe Ganesh Ashruji., " Application of El-zaki Transform in Cryptography", Inter. Journal of Modern Sciences and Engineering Technology, Vol.3, No.3, pp. 46 – 48, 2016

[5] Abdelilah K. Hassan Sedeeg., Mohand M. Abdelrahim Mahgoub, and Muneer A.Saif Saeed., "An Application of the New Integral Aboodh Transform in Cryptography", Pure and Applied Mathematics Journal, Vol.5, No.5, pp. 151 – 154, 2016

[6] Kenneth H. Rosan., Discrete Mathematics and Its Applications, Mcgraw Hill, Chapter 4, 2012

[7] Uttam Dattu Kharde., " An Application of the Elzaki Transform in Cryptography", Journal for Advanced Research in Applied Sciences, Vol.4, No.5, pp. 86 – 89, 2017

[8] Abdelilah Kamal H. Sedeeg,"The New Integral Transform "Kamal Transform" ", Advances in Theoretical and Applied Mathematics, Vol.11, No.4, pp. 451 – 458, 2016

[9] P. Senthil Kumar and S.Vasuki, " An Application of MAHGOUB Transform in Cryptography", Advances in Theoretical and Applied Mathematics, Vol.13, No.2, pp. 91-99, 2018