International Journal of Advanced and Innovative Research (2278-7844) /
Volume 7 Issue 9

Application of 'Mohand' Transform in Cryptography

P. Senthil Kumar[1], V. Sandhya [2], S. Sindhuja [3], A. Viswanathan[4]
[1,4] Professor, Department of Mathematics, SNS College of Technology
[2,3]Assistant Professor, Department of Mathematics, SNS College of Technology
Coimbatore, Tamil Nadu, India
Email: psenthil3@gmail.com, deansandh@snsct.org

Abstract*— *Cryptography involves creating written or generated codes that allow information to be kept secret. It is the science of using mathematics to encrypt and decrypt data (message).This paper aims to encrypt and decrypt a message by using a new integral transform "Mohand" transform and congruence modulo operator.

***Keywords*— Caesar Cipher, Mohand transform**

I. Introduction

Cryptography is the study of secret messages. An encryption or cipher is the process of translating plain text into something that appears to be random and meaningless (cipher text).Decryption is the process of converting cipher text back to plain text. 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 [2] 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 five, then the plain text A would be replaced by the cipher text F, the next letter B would be replaced by G 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, $t \leq 26$, 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 Mohand transform [5]. Mohand 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 [8], Mahgoub [4] 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 [7] and Uttam Dattu Kharde [9] proposed a method to encrypt and decrypt a plain text message by using Elzaki transform. Abdelilah K. Hassan Sedeeg, et.al [1] proposed a method by using Aboodh transform. P. Senthil Kumar and S. Vasuki [6] proposed an encryption and decryption procedure by using Mahgoub transform.

II. MOHAND TRANSFORM

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

$$A = \{ f(t) = \exists M \ , k_1, k_2 > 0. | \ f(t) | < Me^{\frac{|t|}{k_j}} , if \ t \ \varepsilon \ (-1)^j \times [0, \infty) \} .$$

where the constant M must be finite number, k_1, k_2 may be finite or infinite. The Mohand transform denoted by the operator M $(\bullet)$ defined by the integral equation

$$M[f(t)] = R(v) = v^2 \int_0^\infty f(t) \, e^{-v(t)} dt, t \geq o, k_1 \leq v \leq k_2 \quad \cdots \quad (1)$$

A. *Some Standard Functions*

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

(i) Let f (t) = 1 then M [1] = v
(ii) Let f(t) = t then M [t] = 1

(iii) Let f (t) = t^2 then $M(t^2) = \frac{2!}{v}$

(iv) In general case, if n > 0, then $M(t^n) = \frac{n!}{v^{n-1}}$

B. Inverse Mohand Transform

(v) $M^{-1}(v) = 1$

(vi) $M^{-1}(1) = t$

(vii) $M^{-1}\left(\frac{1}{v}\right) = \frac{t^2}{2!}$

(viii) $M^{-1}\left(\frac{1}{v^2}\right) = \frac{t^3}{3!}$ and so on.

III. 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 Mohand transform of polynomial p(t)

(VI) Find r_i such that $q_i \equiv r_i$ mod 26 for each i,0 ≤ i ≤ n

(VII) Consider a new finite sequence $r_0, r_1, \ldots . r_n$

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

IV. DECRYPTION ALGORITHM

(I) convert the cipher text in to corresponding finite sequence of numbers $r_0, r_1, \ldots . r_n$

(II) Let $q_i = 26c_i + r_i \ , \forall i = 0,1,2, \ldots . n$

(III) Let $p(t) = \sum_{i=0}^{n} \frac{q_i}{v^{i-1}}$

(IV) Take the inverse Mohand transform

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

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

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

V. PROPOSED METHODOLOGY

A. *EXAMPLE (1)*

Consider the plain text message is **"TRANSFORM"**

1) *Encryption Procedure*

Now the corresponding finite sequence is 20, 18, 1, 14, 19, 6, 15, 18, 13.The number of terms in the sequence is 9. That is

n=9.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 8. The above finite sequence shift by k letters (k = 3), this is 23, 21, 4, 17, 22, 9, 18, 21, 16

Now consider

$$p(t) = 23 + 21t + 4t^2 + 17t^3 + 22t^4 + 9t^5 + 18t^6 + 21t^7 + 16t^8$$

Take Mohand transform on both sides

$$M[p(t)] = M\{23 + 21 \cdot t + 4 \cdot t^2 + 17 \cdot t^3 + 22 \cdot t^4 + 9 \cdot t^5 + 18 \cdot t^6 + 21 \cdot t^7 + 16 \cdot t^8\}$$

$$= M[23] + M[21.t] + M[4.t^2] + M[17.t^3] + M[22.t^4] + M[9.t^5] + M[18.t^6] + M[21.t^7] + M[16.t^8]$$

$$= 23M[1] + 21M[t] + 4M[t^2] + 17M[t^3] + 22M[t^4] + 9M[t^5] + 18M[t^6] + 21M[t^7] + 16M[t^8]$$

$$= 23v + 21.1 + 4.\frac{2}{v} + 17\frac{6}{v^2} + 22.\frac{24}{v^3} + 9.\frac{120}{v^4} + 18.\frac{720}{v^5} + 21.\frac{5040}{v^6} + 16.\frac{40320}{v^7}$$

$$= \frac{23}{v^{-1}} + \frac{21}{v^0} + \frac{8}{v^1} + \frac{102}{v^2} + \frac{528}{v^3} + \frac{1080}{v^4} + \frac{12960}{v^5} + \frac{105840}{v^6} + \frac{645120}{v^7}$$

$$M[p(t)] = \sum_{i=0}^{8} \frac{q_i}{v^{i-1}}$$

$where\, q_0 = 23, q_1 = 21, q_2 = 8, q_3 = 102, q_4 = 528, q_5 = 1080, q_6 = 12960, q_7 = 105840, q_8 = 645120$

Find

$$r_i \ such that\, q_i \ = r_i \bmod 26 \ for\ each\, i, 0 < i < 8$$

q_0 = 23, 23 ≡ 23 mod 26 ⇒ r_0 = 23

q_1 = 21, 21≡ 21 mod 26 ⇒ r_1 = 21

q_2 = 8, 8 ≡ 8 mod 26 ⇒ r_2 = 8

q_3 = 102,102 ≡ 24 mod 26 ⇒ r_3 = 24

q_4 = 528,528 ≡ 20 mod 26 ⇒ r_4 = 20

q_5 = 1080, 1080 ≡ 14 mod 26⇒ r_5 = 14

q_6 = 12960, 12960 ≡12 mod 26⇒ r_6 = 12

q_7 = 105840, 105840 $\equiv$20 mod 26 $\Rightarrow$ r_7 = 20

q_8 = 645120, 645120 $\equiv$ 8 mod 26 $\Rightarrow$ r_8 = 8

Now consider a new finite sequence is $r_0, r_1, \ldots, r_8$. That is 23, 21,8,24,20,14,12,20,8 and the key (c_i) is

0 , 0 , 0 , 3 , 20 , 41 , 498 , 4070 , 24812 . The corresponding cipher text is ”**WUHXTNLTH”.**

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 23, 21, 8, 24, 20, 14, 12, 20, 8. Let $q_i = 26c_i + r_i \ ,\forall i, i = 0,1,2,\ldots.n$

q_0 = 26 × 0 + 23 = 23

q_1 = 26 × 0 + 21= 21

q_2 = 26 × 0 + 8 = 8

q_3 = 26 × 3 + 24 = 102

q_4 = 26 × 20 + 8 = 528

q_5 = 26 × 41 + 14 = 1080

q_6 = 26 × 498 + 12 = 12960

q_7 = 26 × 4070 + 20 = 105840

q_8 = 26 × 24812 + 8 = 645120

$$Let\ M[p(t)] = \sum_{i=0}^{8} \frac{q_i}{v^{i-1}}$$

$$= \frac{23}{v^{-1}} + \frac{21}{v^0} + \frac{8}{v^1} + \frac{102}{v^2} + \frac{528}{v^3} + \frac{1080}{v^4} + \frac{12960}{v^5} + \frac{105840}{v^6} + \frac{645120}{v^7}$$
$$= M^{-1}\left[\frac{23}{v^{-1}} + \frac{21}{v^0} + \frac{8}{v^1} + \frac{102}{v^2} + \frac{528}{v^3} + \frac{1080}{v^4} + \frac{12960}{v^5} + \frac{105840}{v^6} + \frac{645120}{v^7}\right]$$
$$= 23M^{-1}(v) + 21M^{-1}(1) + 8M^{-1}\left(\frac{1}{v}\right) + 102M^{-1}\left(\frac{1}{v^2}\right) + 528M^{-1}\left(\frac{1}{v^3}\right) + 1080M^{-1}\left(\frac{1}{v^4}\right)$$
$$+ 12960M^{-1}\left(\frac{1}{v^5}\right) + 105840M^{-1}\left(\frac{1}{v^6}\right) + 645120M^{-1}\left(\frac{1}{v^7}\right)$$
$$= 23.1 + 21.t + 8.\frac{t^2}{2!}. + 102.\frac{t^3}{3!} + 528.\frac{t^4}{4!} + 1080.\frac{t^5}{5!} + 12960.\frac{t^6}{6!} + 105840.\frac{t^7}{7!} + 645120.\frac{t^8}{8!}$$
$$= 23 + 21t + 4t^2 + 17t^3 + 22t^4 + 9t^5 + 18t^6 + 21t^7 + 16t^8$$

The coefficient of a polynomial p(t) as a finite sequence 23, 21,4,17,22,9,18,21,16.Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (t-3)\,\mathrm{mod}\,26.$ The corrected new finite sequence is 20, 18, 1, 14, 19, 6, 15, 18, 13. Now translating the numbers of alphabets .We get the original plain text message **“TRANSFORM”**

B. *EXAMPLE (2)*

Consider the plain text message is **“BIDMAS**”

1) *Encryption Procedure*

Now the corresponding finite sequence is 2, 9, 4, 13, 1 ,19. The number of terms in the sequence is 6 including the space. That is n=6. .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 5. The above finite sequence shift by k letters (k = 5), this is 7, 14, 9, 18, 6, 24

Now consider

$$p(t) = 7 + 14t + 9t^2 + 18t^3 + 6t^4 + 24t^5$$

Take Mohand transform on both sides

$$M(p(t)) = M\{7 + 14t + 9t^2 + 18t^3 + 6t^4 + 24t^5\}$$
$$= M[7] + M[14.t] + M[9.t^2] + M[18.t^3] + M[6.t^4] + M[24.t^5]$$
$$= 7M[1] + 14M[T] + 9M[t^2] + 18M[t^3] + 6M[t^4] + 24M[t^5]$$
$$= 7v + 14.1 + 9.\frac{2}{v} + 18\frac{6}{v^2} + 6.\frac{24}{v^3} + 24.\frac{120}{v^4}$$
$$= 7v + 14.1 + \frac{18}{v} + \frac{108}{v^2} + \frac{144}{v^3} + \frac{2880}{v^4}$$

$$M[p(t)] = \sum_{i=0}^{5} \frac{q_i}{v^{i-1}}$$

$$where\ q_0 = 7, q_1 = 14, q_2 = 18, q_3 = 108, q_4 = 144, q_5 = 2880$$

Find

$$r_i\ such that\ q_i \ = r_i\ \mathrm{mod}26\ \ for\ each\ i, 0 < i < 5$$

q_0 =7, 7$\equiv$7 mod 26 $\Rightarrow$ r_0 =7

q_1 =14, 14$\equiv$14mod 26 $\Rightarrow$ r_1 =14

q_2 =18, 18$\equiv$18 mod 26 $\Rightarrow$ r_2 =18

q_3 =108,108$\equiv$4 mod 26 $\Rightarrow$ r_3 =4

q_4 =144,144$\equiv$14 mod26 $\Rightarrow$ r_4 =14

q_5 =2880, 2880$\equiv$20 mod 26 $\Rightarrow$ r_5 =20

Now consider a new finite sequence is $r_0, r_1, \ldots, r_5$ that is 7,14,18,4,14,20 and the key (c_i) is 0, 0, 0, 4, 26, 110. The corresponding cipher text is **”GNRDNT”**

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 7, 14, 18, 4, 14, 20

Let

$$q_i = 26c_i + r_i \ , \forall i = 0,1,2,....n$$

q_0 =26×0+7=7

q_1 =26×0+14=14

q_2 =26×0+18=18

q_3 =26×4+4=108

q_4 =26×5+14=144

q_5 =26×110+20=2880

$$M[p(t)] = \sum_{i=0}^{5} \frac{q_i}{v^{i-1}}$$

$$= \frac{7}{v^{-1}} + \frac{14}{v^0} + \frac{18}{v^1} + \frac{102}{v^2} + \frac{108}{v^3} + \frac{144}{v^4} + \frac{2880}{v^5}$$

$$= M^{-1}\left[\frac{7}{v^{-1}} + \frac{14}{v^0} + \frac{18}{v^1} + \frac{102}{v^2} + \frac{108}{v^3} + \frac{144}{v^4} + \frac{2880}{v^5}\right]$$

$$= 7M^{-1}(v) + 14M^{-1}(1) + 18M^{-1}\left(\frac{1}{v}\right) + 108M^{-1}\left(\frac{1}{v^2}\right) + 144M^{-1}\left(\frac{1}{v^3}\right) + 2880M^{-1}\left(\frac{1}{v^4}\right)$$

$$= 23.1 + 14.t + 18.\frac{t^2}{2!}. + 108.\frac{t^3}{3!}t^3 + 144.\frac{t^4}{4!} + 2880.\frac{t^5}{5!}$$

$$= 7 + 14t + 9t^2 + 18t^3 + 6t^4 + 24t^5$$

The coefficient of a polynomial p(t) as a finite sequence 7,14,9,18,6,24. Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (t-5)\bmod 26$ the corrected new finite sequence is 2, 9, 4, 13, 1, 19. Now translating the numbers of alphabets .We get the original plain text message **“BIDMAS”**

VI. CONCLUSION

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

REFERENCES

[1] 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

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

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

[5] Mohand M. Abdelrahim Mahgoub, “The New Integral Transform “Mohand transform”, Advances in Theoretical and Applied Mathematics , Vol.12, No.2, pp. 113 – 120, 2017.

[6] 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

[7] 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

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

[9] 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