International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-2, March, 2019

An Application of Tarig Transform in Cryptography

P.S. Shwethaa
Department of Information Technology
SNS College of Technology
Coimbatore, Tamil Nadu, India
E-mail: selvisekaran73@gmail.com

P. Senthil Kumar
Department of Mathematics
SNS College of Technology
Coimbatore, Tamil Nadu, India
E-mail: psenthil3@gmail.com

Abstract: Cryptography is the science of using mathematics to encrypt and decrypt data. It is the study of secret messages. Cryptography plays an important role when we deal with network security. Not only writing the message in a secret form but it is the intention of keeping the data secret. There were several algorithms to achieve cryptography. This paper aims to encrypt and decrypt a message by using an integral transform - Tarig transform and Congruence modulo operator.

Keywords: Caesar Cipher, Encryption, Decryption, Tarig transform

I. INTRODUCTION

Cryptography involves creating written or generated codes that allow information to be kept secret. 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 reverse process is called decryption. In this paper, our research concept to encrypt and decrypt a message by using a new integral transform Tarig transform [11]. Tarig 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], Aboodh [3], Mohand [12], Kamal [13], and Mahgoub [2] transforms. Based on the mathematical simplicity of this transform and its fundamental properties, we have to apply encryption and decryption algorithm 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 EL-zaki transform. Abdelilah Hassan Sedeeg, et.al [5] proposed a method by using Aboodh transform in cryptography. P. Senthil Kumar et. Al [8,9,10] proposed a method by using various integral transforms like Mahgoub, Mohand and Kamal in cryptography.

II. METHODOLOGY

One of the earliest ciphers is called Ceaser 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, $t \leq 26$, the integer in the set {1, 2, 3….26} with p (t) = (t+k) mod 26. This is the forward process. Whereas, in the reverse process we use the function p (t) = (t - k) mod 26. Finally we get the original text message from the sequence of numbers.

In this paper, our aims to encrypt and decrypt a message by using a new integral transforms Tarig transform.

III. TARIG TRANSFORM

Tarig M. ELzaki introduced a new transform and named as Tarig transform, which is defined by the following formula.

$$E_1(u) = T\left[f(t)\right] = \frac{1}{u}\int_0^{\infty} f(t)e^{\frac{t}{u^2}}, u \neq 0 \quad (1)$$

A. *Some Standard Functions*

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

(i) f (t) = 1 then G [1] =u
(ii) f (t) = t then G [t] =u^3
(iii) f (t) = t^2 then G [t^2] =2! . u^5
(iv) In general case, if n>0, then G[t^n] = n! . u^{2n+1}

B. *Inverse Tarig Transform*

(v) $G^{-1}[u] = 1$
(vi) $G^{-1}[u^3] = t$
(vii) $G^{-1}[u^5] = t^2/2!$
(viii) $G^{-1}[u^7] = t^3/3!$ and so on.

IV. 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 message is organized as a finite sequence of numbers based on the above conversion.

(III) Now replace each of the numbers *t* by
p (t) = (t+k) mod 26
(IV) Apply Tarig transform of polynomial p (t).

(V) Find r_i such that $q_i \equiv r_i \ mod\ 26$ for each i, $1 \le i \le n$
(VI) Consider a new finite sequence $r_1, r_2, r_3, \ldots r_n$
(VII) The output text message is in cipher text.

V. DECRYPTION ALGORITHM

(I) Convert the cipher text in to corresponding finite sequences of numbers $r_1, r_2, r_3, \ldots r_n$
(II) Take the inverse Tarig transform
(III) The coefficient of a polynomial p (t) as a finite sequence
(IV) Now replace each of the numbers by $p^{-1}(t) = (t-k) \bmod 26$
(V) Translate the number of the finite sequence to alphabets. We get the original text message.

VI. PROPOSED METHODOLOGY

Consider the plain text message **"ABSTRACT"**.

A. Encryption Procedure

Now the finite sequence is 1, 2, 19, 20, 18, 1, 3, 20. The number of terms in the sequence is 8 . That is n=8. 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 7.

The above finite sequence shift by k letters (k=3), this results 4, 5, 22, 23,21,4,6,23. Now the polynomial p (t) is

$$p(t) = 4 + 5.t + 22.t^2 + 23.t^3 + 21.t^4 + 4.t^5 + 6.t^6 + 23.t^7$$

Take Tarig transform on both sides

$$T[p(t)] = G\{4 + 5.t + 22.t^2 + 23.t^3 + 21.t^4 + 4.t^5 + 6.t^6 + 23.t^7\}$$

$$= 4u + 5u^3 + 44u^5 + 138u^7 + 504u^9 + 480u^{11} + 4320u^{13} + 115920u^{15}$$

Where $q_1 = 4$, $q_2=5$, $q_3=44$, $q_4=138$, $q_5=504$, $q_6=480$, q7=4320, $q_{8=}115920$

Now find r_i such that $q_i \equiv r_i \ mod\ 26$

$q_1 = 4$,	$4 \equiv 4 \bmod 26$	=>	$r_1=4$
$q_2=5$,	$5 \equiv 5 \bmod 26$	=>	$r_2=5$
$q_3=44$,	$44 \equiv 44 \ mod\ 26$	=>	$r_3=44$
$q_4=138$,	$138 \equiv 8 \ mod\ 26$	=>	$r_4=8$
$q_5=504$,	$504 \equiv 10 \ mod\ 26$	=>	$r_5=10$
$q_6=480$,	$480 \equiv 12 \ mod\ 26$	=>	$r_6=12$
$q_7=4320$,	$4320 \equiv 4 \ mod\ 26$	=>	$r_7=4$
$q_8=115920$,	$115290 \equiv 44 \ mod 26$	=>	$r_8=44$

Now consider a new finite sequence is $r_1, r_2, r_3, \ldots r_8$
That is 4,5,44,8,10,12,4,12. The corresponding cipher text is **"DERHJLDL"**

B. 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 4, 5, 44, 8, 10, 12,4,12.

$$\text{Let } T[p(t)] = 4u + 5u^3 + 44u^5 + 138u^7 + 504u^9 + 480u^{11} + 4320u^{13} + 115920u^{15}$$

Take inverse Tarig transform on both sides

$$p(t) = G^{-1}\{4u + 5u^3 + 44u^5 + 138u^7 + 504u^9 + 480u^{11} + 4320u^{13} + 115920u^{15}\}$$

$$= 4 + 5 + 22t^2 + 23t^3 + 21t^4 + 4t^5 + 6t^6 + 23t^7$$

The coefficient of a polynomial p(t) as a finite sequence 4,5,22,23,21,4,6,23. Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (t-3) \bmod 26$. The corrected new finite sequence is 1, 2, 19, 20, 18, 1, 3, 20. Now by translating the number of alphabets we get the original plain text message **"ABSTRACT".**

VII. CONCLUSION

In this proposed work, a cryptographic scheme(Caesar cipher) with a new integral transform Tarig transform with congruence modulo operator is introduced and the results are verified. The algorithmic part is also simple. This procedure is allowed the plain text message in a more safety form. And thus the process of plain text security is strengthened as well as the process of decryption is simplified.

REFERENCES

[1] Tarig. M.Elzaki.,"The New Integral Transform El Zaki 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, 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] 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

[9] P. Senthil Kumar, V. Sandhya, S. Sindhuja and A. Viswanathan, "Application of Mohand transform in Cryptography", International Journal of Advanced and Innovative Research, Vol. 7, No.9, pp. 1 – 4, 2018.

[10] P. Senthil Kumar and S. Vasuki, " Application of Kamal transform in Cryptography", International journal of Interdisciplinary Research and Innovations, Vol. 6, No.3, pp. 182 – 189, 2018.

[11] Tarig M. Elzaki and Salih M. Elzaki, " On the relationship between Laplace transform and new integral transform Tarig transform", Elixir App. Math., Vol. 36, pp. 3230 – 3233, 2011

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

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

AUTHOR'S BIOGRAPHIES

Ms. Swethaa, P.S. is doing under graduate in B.Tech., Information Technology in SNS College of Technology, Coimbatore, Tamil Nadu, India. Her research interests are Database Management Systems, Operating Systems and Cryptography.

Dr. P. Senthil Kumar completed his graduation, post-graduation and Ph.D. from Bharathiar University. His research interests are wavelet transform, bio-medical signal processing, applied mathematics and cryptography. Now he is working as Professor and Head of Mathematics Department, SNS College of Technology, Coimbatore, Tamil Nadu, India. He has published more than 30 research articles in national / international journals and conferences.