IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

APPLICATION OF TARIG TRANSFORM IN CRYPTOGRAPHY

[1]Dr. K. Bhuvaneswari, [2]Dr. R. Bhuvaneswari

[1]Assistant Professor, [2]Assistant Professor

[1]Postgraduate Department of Mathematics,

[1]BMS College for Women, Bengaluru, India.

Abstract: Cryptography is the study of techniques in secured communication. Cryptanalysis is the art of breaking encoded data. Mathematical techniques are used to encrypt and decrypt data. In recent research various integral transform based cryptographic techniques were studied. In this paper, we give an encryption and decryption algorithm based on Tarig transformation and congruence modulo. Affine cipher technique is used in the proposed algorithm.

Index Terms **- Tarig Transform, Cryptography, Cryptanalysis, Encryption, Decryption, Affine cipher.**

I. INTRODUCTION

Cryptography is the science of secret communications. The data security has become an important and critical issue. Cryptography provides mathematical techniques to secure data [3],[4],[6]. Encryption is the process of converting the original message (known as plain text) into unreadable message (called as cipher text). Decryption is the process of converting cipher text into plain text. Modern cryptography uses mathematical algorithms and secret keys to encrypt and decrypt data.

Integral transforms plays an important role in applied mathematics. In recent research new cryptographic techniques based on integral transforms were introduced [1], [5], [7]. Tarig transform was introduced by Tarig.M.Elzaki and properties of Tarig transform was studied [7].

In this paper we give a new cryptographic technique based on Tarig transform, affine cipher and congruence modulo.

II. PRELIMINARIES

Definition (Affine Cipher)

Affine cipher is a substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. Each letter is encrypted using the formula

$$E(x) = ax + b \ \ (mod\ 26)$$

where a and b are keys of the cipher. The value a must be chosen such that a is coprime to 26. The decryption function is

$$D(y) = a^{-1}(x - b)\ (mod\ 26)$$

where a^{-1} is the modular multiplicative inverse of a modulo 26.

Definition (Tarig Transform)[7]

Consider the functions f in S where the set S is defined as

$$S = \{f(t): \exists\, M, k_1, k_2 > 0, |f(t)| < Me^{\frac{|t|}{k_j}}, t \in (-1)^j * [0, \infty)\}$$

For a given function in the set $M > 0$ must be finite number and k_1, k_2 may be finite or infinite.

For a given function $f \in S$, the Tarig transform of $f(t)$ is defined as

$$E(u) = T[f(t)] = \frac{1}{u}\int_0^\infty f(t)\ e^{-t/u^2} dt \quad , u \neq 0.$$

Tarig transform satisfies the linearity property [7].

Tarig transform & inverse Tarig transform of some elementary functions

Elementary functions include algebraic and transcendental functions.

1. $E(u) = T[1] = u$
2. $E(u) = T[t] = u^3, when\ f(t) = t$
3. In general, when $f(t) = t^n, E(u) = T[t^n] = n!\, u^{1+2n}$
4. $E^{-1}(u) = 1$
5. $E^{-1}\ (n!\, u^{(1+2n)}) = t^n$

III. MAIN RESULTS

The following algorithm provides an insight into the proposed cryptographic scheme. The sender converts the original message or plain text into cipher text using the following steps.

Encryption Algorithm

I. Every letter in the plain text message is converted as a number so $A = 0, B = 1, \dots\dots, Z = 25$.

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

For example let our text is "$FUNCTION$".

Then based on above step we get,

$$F = 5, U = 20, N = 13, C = 2, T = 19, I = 8, O = 14, N = 13.$$

Therefore our plain text finite sequence is 5,20,13,2,19,8,14,13.

III. We use affine cipher method. Take $a = 5$ and $b = 8$. Since $gcd(5,26) = 1$, a and 26 are co-prime.

Use the encryption function $E(x) = 5x + 8\ (mod\ 26)$, where x is an integer corresponding to the plain text letter.

The following table gives the encryption process.

Plain text	F	U	N	C	T	I	O	N
x	5	20	13	2	19	8	14	13
$5x + 8$	33	108	73	18	103	48	78	73
$(5x + 8) mod 26$	7	4	21	18	25	22	0	21

IV. Let $n + 1$ be the number of term in the sequence.

V. Consider a polynomial $p(t)$ of degree n with coefficient as the term of the given finite sequence.

In our example, finite sequence contains $7 + 1$ terms.

Hence consider a polynomial $p(t)$ of degree 7.

$$p(t) = 7 + 4t^1 + 21t^2 + 18t^3 + 25t^4 + 22t^5 + 0t^6 + 21t^7$$

VI. Take Tarig transform $E(u)$ of the polynomial $p(t)$ and write

$$E(u) = \sum_{i=0}^{n} q_i u^{2i+1}$$

Therefore,

$$E(u) = T[p(t)] = E[7 + 4t^1 + 21t^2 + 18t^3 + 25t^4 + 22t^5 + 0t^6 + 21t^7]$$
$$= 7u + 4u^3 + 21(2!)u^5 + 18(3!)u^7 + 25(4!)u^9 + 22(5!)u^{11} + 0(6!)u^{13} + 21(7!)u^{15}$$
$$= 7u + 4u^3 + 42u^5 + 108u^7 + 600u^9 + 2640u^{11} + 0u^{13} + 105840u^{15}$$
$$= \sum_{i=0}^{7} q_i u^{2i+1}$$

VII. Next we find r_i such that $q_i \equiv r_i \pmod{26}$ for each i, $0 \le i \le n$.

Therefore, we get $q_0 = 7 \equiv 7 \pmod{26}$, $q_1 = 4 \equiv 4 \pmod{26}$,

$q_2 = 42 \equiv 16 \pmod{26}$, $q_3 = 108 \equiv 4 \pmod{26}$,

$q_4 = 600 \equiv 2 \pmod{26}$, $q_5 = 2640 \equiv 14 \pmod{26}$,

$q_6 = 0 \equiv 0 \pmod{26}$, $q_7 = 105840 \equiv 20 \pmod{26}$

VIII. Write $q_i = 26k_i + r_i$. Thus we get a key k_i for i=0,1,2,3 $\dots\dots n$.

$$\therefore k_0 = 0, k_1 = 0, k_2 = 1, k_3 = 4, k_4 = 23, k_5 = 101, k_6 = 0, k_7 = 4070$$

IX. Now consider a new finite sequence $r_0, r_1, \dots\dots, r_n$

That is 7,4,16,4,2,14,0,20

X. Convert the numbers into alphabets, we get the cipher text.

Thus the corresponding cipher text is "HEQECOAU"

Decryption algorithm

This algorithm converts the cipher text into plain text. We assume that the receiver knows the affine cipher keys a and b. The multiplicative inverse of a under modulo 26 is denoted by a^{-1}.

In our above example, a=5 and b=8 and so $a^{-1} = 21$.

I. Consider the cipher text and key received from sender.

In above example cipher text is "HEQECOAU" and key is 0, 0,1,4,23,101,0,4070

II. Convert the given cipher text to corresponding finite sequence of numbers $r_0, r_1, \dots\dots r_n$

That is 7, 4,16,4,2,14,0,20.

III. Let $q_i = 26k_i + r_i, \forall i = 0,1, \dots\dots n$

Therefore, $q_0 = 26(0) + 7 = 7$, $q_1 = 26(0) + 4 = 4$,

$q_2 = 26(1) + 16 = 42$, $q_3 = 26(4) + 4 = 108$,

$q_4 = 26(23) + 2 = 600$, $q_5 = 26(101) + 14 = 2640$,

$q_6 = 26(0) + 0 = 0$, $q_7 = 26(4070) + 20 = 105840$

IV. Let $E(u) = \sum_{i=0}^{7} q_i u^{2i+1}$

Therefore,

$$E(u) = 7u + 4u^3 + 42u^5 + 108u^7 + 600u^9 + 2640u^{11} + 0u^{13} + 105840u^{15}$$
$$= 7u + 4u^3 + 21(2!)u^5 + 18(3!)u^7 + 25(4!)u^9 + 22(5!)u^{11} + 0(6!)u^{13} + 21(7!)u^{15}$$

V. Take the inverse Tarig transform of $E(u)$ and get the polynomial $p(t)$.

In the above example, we get

$$p(t) = 7 + 4t^1 + 21t^2 + 18t^3 + 25t^4 + 22t^5 + 0t^6 + 21t^7$$

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

That is 7,4,21,18,25,22,0,21

VII. For each number y in the number sequence, use decryption function

$$D(y) = a^{-1}(y - b)(mod\ 26)$$

Where a & b are affine cipher keys.

For our example,

y	7	4	21	18	25	22	0	21
$21(y-8)$	-21	-84	273	210	357	294	-168	273
$D(y)$	5	20	13	2	19	8	14	13
Plain text	F	U	N	C	T	I	O	N

IV. Conclusion

We provided an encryption and decryption algorithm based on Tarig transform and affine cipher. The results are verified. As an extension of this work, we can use different types of ciphers available in the literature instead of affine cipher.

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] Abdelilah K.Hassan Sedeeg, Mohand M.Abdelrahim Mahgoub, Muneer A.Saif Saeed,"An application of the new integral Aboodh Transform in cryptography", Pure and Applied Mathematics Journal, 2016; 5(5):151-154.

[3] T.H. Barr, "Invitation to Cryptography", Prentice Hall, (2002).

[4] Blakeley G.R. ,Twenty years of Cryptography in the open literature, Security and Privacy 1999,Proceedings of the IEEE Symposium, 9-12, (May 1999).

[5] R. Bhuvaneswari, K. Bhuvaneswari, "Application of Yang Transform in Cryptography", International Journal of Engineering, Science and Mathematics, Vol.9, Issue 3, March 2020.

[6] Johanees A.Buchmann, Introduction to Cryptography, Fourth Edn.,Indian Reprint, Springer,(2009).

[7] Shrinath Manjarekar, A.P.Bhadane, "Applications of Tarig Transformation To New Fractional Derivatives With Non Singular Kernel",Journal of Fractional Calculus and Applications,Vol.9(1) Jan.2018, pp.160-166.