ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 3, Dec 2022

Mohandtransform Based Cryptographic Technique

Dr. K. Bhuvaneswari[1],

[1]Assistant professor, PG department of Mathematics, BMS College for Women (Autonomous), Basavanagudi, Bangalore, India

Abstract

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

Keywords: Mohand Transform, Cryptography, Cryptanalysis, Encryption, Decryption.
MSC 2010 Subject classification: 11T71, 94A60

Introduction

Cryptography is the science of secret communications. The data security has become an important and critical issue. Cryptography provides mathematical techniques to securedata[3],[4],[5].

Encryption is the process of converting theoriginal message(known as plain text)intounreadable 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 anddecrypt data.

Integral transforms plays an important role inapplied mathematics.In recent research newcryptographic techniques based on integraltransforms were introduced[1],[7].

Mohand transform was introduced by Mohand M. Abdelrahim Mahgouband properties of Mohand transform was studied[7].

In this paper, our research gives a new cryptographic technique based on Mohand transform, affine cipher and congruence modulo.

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

IJFANS International Journal of Food And Nutritional Sciences Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11,S Iss 3, Dec 2022

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

where$a$ and b are keys of the cipher. The value a must be chosen such that a is co prime 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 (Mohand Transform)[7]

Consider the function$f$ in A where the set A is defined as

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

For a given function in the set A , the constant $M > 0$ must be finite number and k_1, k_2may be finite or infinite.

The Mohand transform denoted by the operator M(.) defined by the integral equations

$$R(v) = M[f(t)] = v^2 \int_0^\infty f(t)\, e^{-vt} dt \quad , t \geq 0, k_1 \leq v \leq k_2.$$

Mohan transform satisfies the linearity property[7]

Mohand transform & inverse Mohand transform of some elementary functions

Elementary functions include algebraic and transcendental functions.

1. $R(v) = M[1] = v$
2. $R(v) = M[t] = \ 1\ , when\ f(t) = t$
3. In general, when $f(t) = t^n, R(v) = M[t^n] = \frac{n!}{v^{n-1}}$
4. $R^{-1}(v) = 1$
5. $R^{-1}\left(\frac{n!}{v^{n-1}}\right) = t^n$

Main Result

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 $A = 0, B = 1, \ldots\ldots, Z = 25$.

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

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11,S Iss 3, Dec 2022

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
$(5x + 8)mod26$	7	4	21	18	25	22	0	21

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

V. Consider apolynomial $p(t)$ 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 $p(t)$ ofdegree 7.

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

VI. Take Mohand transform $R(v)$ of the polynomial $p(t)$ and write

$$R(v) = \sum_{i=0}^{n} q_i v^{-i+1}$$

Therefore,

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

$$= 7v + 4 + 21\frac{(2!)}{v} + 18\frac{(3!)}{v^2} + 25\frac{(4!)}{v^3} + 22\frac{(5!)}{v^4}$$

$$+0\frac{(6!)}{v^5} + 21\frac{(7!)}{v^6}$$

$$= 7u + 4 + \frac{42}{v} + \frac{108}{v^2} + \frac{600}{v^3} + \frac{2640}{v^4} + \frac{0}{v^5} + \frac{105840}{v^6}$$

$$= \sum_{i=0}^{7} q_i v^{-i+1}$$

VII. Next we find r_i such that $q_i \equiv r_i$ (mod26) for each i,$0 \leq i \leq n$.

Therefore, we get $q_0 = 7 \equiv 7$(mod 26),$q_1 = 4 \equiv 4$(mod 26),

$q_2 = 42 \equiv 16$ (mod 26), q_3=108 $\equiv 4$(mod 26),

$$q_4 = 600 \equiv 2(mod\ 26), q_5 = 2640 \equiv 14(mod\ 26),$$

IJFANS International Journal of Food And Nutritional Sciences
Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

Research paper © 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11,S Iss 3, Dec 2022

$$q_6 = 0 \equiv 0(\text{mod } 26), \qquad q_7 = 105840 \equiv 20 \ (\text{mod } 26)$$

VIII. Write $q_i = 26k_i + r_i$. Thus we get a key k_i for i=0,1,2,3 … … . . 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, $q_3 = 26(4) + 4 = 108$,

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

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

IV. Let R(v) $= \sum_{i=0}^{7} q_i \, u^{-i+1}$

Therefore,

$$R(v) = 7v + 4 + \frac{42}{v} + \frac{108}{v^2} + \frac{600}{v^3} + \frac{2640}{v^4} + \frac{0}{v^5} + \frac{105840}{v^6}$$
$$= 7v + 4 + 21\frac{(2!)}{v} + 18\frac{(3!)}{v^2} + 25\frac{(4!)}{v^3} + 22\frac{(5!)}{v^4} + 0\frac{(6!)}{v^5} + 21\frac{(7!)}{v^6}$$

V. Take the inverse Mohand 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

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 3, Dec 2022

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

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

Conclusion

We provided an encryption and decryption algorithm based on Mohand 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.

Reference

[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]Barr T.H., “Invitation to Cryptography”, Prentice Hall, (2002).

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

[5] K. Bhuvaneswari , R. Bhuvaneswari, “Application of Tarig transformation in cryptography”, International Journal of Creative Research Thoughts, Vol 8, issue 6 June 2020,pp 1878-1880.

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

[7] Mohand M. Abdelrahim Mahgoub, “The New Integral Transform “Mohand Transform”, Advances in Theoretical and Applied Mathematics ISSN 0973-4554 Volume 12, Number 2(2017), pp113-120.