Kamal Transformation based Cryptographic Technique in Network Security Involving ASCII Value

Ayush Mittal, Ravindra Gupta

Abstract: ***From old times, information security has been an essential part of human life. Day to day developing new technologies and increasing number of users share information with each other, securing information is becoming more important. For securing information, there are several techniques out of which most common is cryptography. Cryptography is a technique involving securing transmission of messages in presence of adversaries. The basic aim is to hide the information from unauthorized users. Cryptography includes to phases: encryption of plain message and decrypting encrypted message.***

The aim of this paper is to use new integral transform "Kamal transform" and congruence modulo operator involving ASCII value for encryption and decryption of message.

Key Words: Encryption, Decryption, ASCII, Plaintext, Ciphertext, Kamal Transform, Network Security, Cryptography.

I. INTRODUCTION

With growing utilization of computers and internet, the importance of data security has been more significant. For securing the data, it should be protected from unauthorized access. Hence, data security has become a very important as well as significant issue.

One of the widely used methods for data security is cryptography. Cryptography is the encryption (encoding) of information to create an encrypted message which can be transmitted over the network without having the possibility that information may be read by hackers. The Fundamental objective of cryptography is to enable two communication devices communicate over an open channel (Intruder can be present) without worrying that the information may be leaked to some other device. The need for secure communication is gaining importance as more and more devices keeps on adding in the network. Cryptography is the only technique which can provide information security in any domains of network be it communication between two computers, or transmission of data between robots, etc.

In terms of cryptography, the information which can we read by anyone without any special access is called plaintext. Cipher text is when plaintext is transformed into a different form so that actual contents can't be reveled without any special permissions and can only be read by recipient it is intended to.

The recipient of cipher text first decrypts the cipher text and then reads the actual contents.

In this paper, our research concept to encrypt and decrypt a message by using a new integral transform Kamal transform [1].

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 [14], Mahgoub [12] and Aboodh transforms [8]. Kamal transform is famous for it's simple mathematical model and we will use this model to get encrypted/decrypted text in simple way.

II. RELATED WORK

Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt data. Various techniques for cryptography are found in literature.

Various techniques for encryption and decryption of a message involving different Integral Transform have been established by Saha [13], Kumar [9, 10], Dhingra [3], Bodkhe [2], Hiwarekar [4, 5, 6, 7], Lakshmi [11] and others.

Subsequent them, in this paper we shall establish a new techniques for encryption and decryption of a message based on 'Kamal' Transform involving ASCII values.

III. KAMAL TRANSFORM

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

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

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

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

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

3.1 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] = $2v^3$ = $2!v^3$

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

3.2 Inverse Kamal transform:

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

(ii) $K^{-1}[v^2] = t$

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

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author

Mr.Ayush Mittal*, Pursuing PhD, Computer Science and Engineering, SRK University, Bhopal, MP, India.
Dr. Ravindra kumar Gupta, Associate Professor, Computer Science and Engineering, Department in RKDFIST,BHOPAL, M.P, India.

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

IV. PROPOSED METHOD:

In this paper a new cryptographic scheme is proposed using 'Kamal' Transform. 'Kamal' transform is used for encrypting the plain text and corresponding inverse 'Kamal' transform is used for decryption. The 'Kamal' transform is a widely used integral transform in mathematics and electrical engineering that transforms a function of time into a function of complex frequency. The inverse 'Kamal' transform takes a complex frequency domain function and yields a function defined in the time domain. Proposed algorithm provides as many transformations as per the requirements which are the most useful factor for changing key. Therefore it is very difficult for an eyedropper to trace the key by any attack.

4.1 ENCRYPTION ALGORITHM:

1. Select the message, M, to be sent, and convert into ASCII code. Let length of message be n.
2. The plain text message is organized as a finite sequence of numbers, based on the above conversion.
3. Writing these numbers as the coefficient in polynomial of degree n – 1.
4. Take 'Kamal' transform of a polynomial.
5. Find the remainders r_i such that $r_i = F_i \bmod 100$, where i = 1, 2, 3,..., n.
6. The ASCII values of remainders will be the Encrypted message.
7. Find the key k_i such that $k_i = (F_i – r_i)/100$, where i = 1, 2, 3,..., n.

Example:

1. Consider the plain text message is “NEHA”. Here the length of the message be 4. ASCII code of plain text is N = 78, E = 69, H = 72, A = 65.
2. The finite sequence corresponding to plain text message is 78, 69, 72, 65.
3. Now the polynomial p(t) is $p(t) = 78 + 69.t + 72.t^2 + 65.t^3$.
4. 'Kamal' transform of p(t) is
   $K[p(t)] = K[78 + 69.t + 72.t^2 + 65.t^3]$
   $= 78K[1] + 69K[t] + 72K[t^2] + 65K[t^3]$
   $= 78v + 69v^2 + 144v^3 + 390v^4$
   $K[p(t)] = \sum_{i=1}^{4} F_i\, v_i,$
   where $F_1 = 78$, $F_2 = 69$, $F_3 = 144$, $F_4 = 390$
5. Find the remainders r_i such that $r_i = F_i \bmod 100$, where i = 1, 2, 3,..., n.
   $r_1 = F_1 \bmod 100 = 78 \bmod 100 = 78$
   $r_2 = F_2 \bmod 100 = 69 \bmod 100 = 69$
   $r_3 = F_3 \bmod 100 = 144 \bmod 100 = 44$
   $r_4 = F_4 \bmod 100 = 390 \bmod 100 = 90$
6. Hence the message 'NEHA' is encrypted as "NE,Z".
7. Find the key k_i such that $k_i = (F_i – r_i)/100$, where i = 1, 2, 3,..., n.
   $k_1 = (F_1 – r_1)/100 = (78 – 78)/100 = 0$
   $k_2 = (F_2 – r_2)/100 = (69 – 69)/100 = 0$
   $k_3 = (F_3 – r_3)/100 = (144 – 44)/100 = 1$
   $k_4 = (F_4 – r_4)/100 = (390 – 90)/100 = 3$
   Thus the key is 0, 0, 1, 3.
   Hence the cipher text is NE,Z and key is 0, 0, 1, 3.

4.2 DECRYPTION ALGORITHM:

1. Consider the cipher text and key received from sender.
2. Convert the given cipher text to corresponding finite sequence of numbers in ASCII form and choose it C_i, where i = 1, 2, 3,..., n.
3. Using given key k_i for i = 1, 2, 3,..., n as k_1, k_2, k_3, k_4, …. and assuming $F_i = 100k_i + C_i$ for i = 1, 2, 3,..., n.
4. Now find the polynomial of degree n – 1 assuming F_i as a coefficient.
5. Next take Inverse 'Kamal' transform of a polynomial
6. Consider the coefficients of a polynomial f(t) as finite sequence
7. Now, translating the numbers of above finite sequence to alphabets (ASCII values), original plain text is obtained

Example:

1. In the above example cipher text is "NE,Z" and key is 0, 0, 1, 3.
2. Convert "NE,Z" to corresponding finite sequence of numbers in ASCII form i.e. 78, 69, 44, 90.
   Let $C_1 = 78$, $C_2 = 69$, $C_3 = 144$, $C_4 = 90$.
3. Let $k_1 = 0$, $k_2 = 0$, $k_3 = 1$, $k_4 = 3$. Now calculate $F_i = 100k_i + C_i$ for i = 1, 2, 3, 4. Therefore,
   $F_1 = 100k_1 + C_1 = 100×0 + 78 = 78$
   $F_2 = 100k_2 + C_2 = 100×0 + 69 = 69$
   $F_3 = 100k_3 + C_3 = 100×1 + 44 = 144$
   $F_4 = 100k_4 + C_4 = 100×3 + 90 = 390$
4. Now find the polynomial of degree 3 assuming $F_1 = 78$, $F_2 = 69$, $F_3 = 144$, $F_4 = 390$ as a coefficient. i.e.
   $K[p(t)] = \sum_{i=1}^{4} F_i\, v_i = 78v + 69v^2 + 144v^3 + 390v^4$
5. Now take Inverse 'Kamal' transform of the polynomial i.e.
   $p(t) = K^{-1}[78v + 69v^2 + 144v^3 + 390v^4]$
   $= 78 + 69t + 72t^2 + 65t^3$
6. The coefficients of a polynomial p(t) as finite sequence is 78, 69, 72, 65.
7. Now, translating the numbers of above finite sequence to alphabets (ASCII values), we get the original plain text is 'NEHA'.

V. APPLICATIONS

1. A symmetric key cryptographic framework named as DSWLT. This system is fast, reasonable for encryption of immense records. DSWLT think about the plain content (i.e. the info record) as paired string with constrained number of bits. The information string changed over to DNA nucleotides utilizing DNA coding and afterward the DNA codes are changed over to positive whole numbers. "KAMAL" transform is connected viewing these numbers as the coefficients of the extension. To give staggered security the resultant coefficients are changed over to their binary comparable and another dimension of encryption with total XOR is performed and individual MSBs found at each cycle are taken to build the encrypted text. Decoding is performed in the opposite way.

2. Mobile adhoc network is assortment of autonomous nodes that are of times moving while not the centralized management. Mobile adhoc networks are multi hop wireless networks while not mounted infrastructure. Node of times amendment topology, thanks to this kind of behavior transformation of data from one node to a different node is additional difficult task. Decentralized nature of mobile adhoc network is additional liable to attack like denial of service (DOS) that consumes additional information measure and resources. Security is major concern in adhoc network, therefore "KAMAL" transform and inverse "KAMAL" transform to reinforce secure communication for Edouard Manet.
3. The proposed technique can be used in Message Passing (Coding Theory) in which the exchange of messages is administered in a confidential and more secured way having a wide application in Military operations, Banking Transactions etc.

VI. CONCLUSION

1. Cryptography is one of the first lines of defense against hackers and crackers in today's world. Thus, the importance of cryptography will stay for long period of time.
2. Many sectors such as banking and other financial institutions are adopting e-services and improving their internet services. But, e-services are also vulnerable to frauds. Internet banking fraud is one of the most serious and famous electronic crimes. Banking sectors are investing huge amount of money for securing data of users.
3. In the proposed work, we develop a new method for encryption/decryption of messages using "KAMAL" transform. The proposed algorithm is strong approach yet it is simple and straight forward. The new algorithm provides same or sometimes betters result in very less time.
4. A new approach for generation of key is developed in this papers and it may be used for a fraud prevention mechanism. This algorithm provides as many transformations as per the requirements which are the most useful factor for changing key. Therefore it is very difficult for an hackers to trace the key by any attack.
5. The similar results can be obtained by using "KAMAL" transform of other suitable function. Hence extension of this work is possible.
6. Encryption and Decryption time with respect to different input sizes has been calculated. It has been analyzed that as input size increases, encryption and decryption time increases. Also, encryption time is more compared to decryption time.

REFERENCES

1. Abdelilah Kamal H. Sedeeg: “The New Integral Transform “Kamal Transform” ”, Advances in Theoretical and Applied Mathematics, Vol.11, No.4, pp. 451 – 458, 2016.
2. Bodkhe D. S., Panchal S. K.: Use of Sumudu transform in cryptography, Bulletin of the Marathwada Mathematical Society 16 (2) (2015), pp. 1 – 6.
3. Dhingra Swati, Savalgi Archana A., Jain Swati: Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications (0975 – 8887), Volume 136, No.7, February 2016, pp. 6-10.
4. Hiwarekar A. P.: A new method of cryptography using Laplace transform, International Journal of Mathematical, Archive 3 (3) (2012), pp. 1193 – 1197.
5. Hiwarekar A. P.: A new method of cryptography using Laplace transform of Hyperbolic functions, International Journal of Mathematical, Archive 4 (2) (2013), pp. 208 – 213.
6. Hiwarekar A. P.: Application of Laplace Transform for Cryptography, April 2015, Vol-5, Issue-4, pp. 129-135.
7. Hiwarekar A. P.: Application of Laplace Transform For Cryptographic Scheme, Proceedings of the World Congress on Engineering 2013, Vol I, July 3 - 5, 2013, London, U.K., pp. 1-6.
8. Khalid Suliman Aboodh., “ The New Integral Transform Aboodh Transform”, Global Journal of Pure and Applied Mathematics, Vol.9, No.1, pp. 35 – 43, 2013.
9. Kumar P. Senthil, Vasuki S.: An Application of MAHGOUB Transform in Cryptography, Advances in Theoretical and Applied Mathematics, ISSN 0973-4554, Volume 13, Number 2 (2018), pp. 91-99.
10. Kumar P. Senthil, Vasuki S.: Application of "Kamal" Transform in Cryptography, International Journal of Interdisciplinary Research and Innovations, Vol. 6, Issue 3, Month: July - September 2018, pp. 182-186.
11. Lakshmi G. Naga, Kumar B. Ravi, Chandrasekhar A.: A cryptographic scheme of Laplace transforms, International Journal of Mathematical, Archive 2 (12) (2011), pp. 2515 – 2519.
12. Mohand M. Abdelrahim Mahgoub., “The New Integral Transform Mahgoub Transform”, Advances in Theoretical and Applied Mathematics, Vol. 11, No.4, pp. 391 – 398, 2016.
13. Saha Mampi: Application of Laplace - Mellin Transform for Cryptography, Rai Journal of Technology Research & Innovation, January 2017, Vol. V, Issue I, pp. 12-17.
14. Tarig. M.Elzaki., “The New Integral Transform ELzaki Transform”, Global Journal of Pure and Applied Mathematics, Vol. 7, No.1, pp. 57 – 64, 2011.

AUTHORS PROFILE

 First Author	**Mr.Ayush Mittal** did his post-graduation in M.Tech(Master of Technology) in Computer Science and Engineering from Indian Institute of Information Technology and Management(IIITM),Gwalior, MP in 2015. He has also received gold medal in post-graduation degree. Currently, he is pursuing his Phd in Computer Science and Engineering from SRK university, Bhopal, MP. His area of interest includes robotics, cryptography and embedded systems. He has published 2 research papers in International Journals.
 Second Author	**Dr. Ravindra kumar Gupta** received his M.Tech (Master of Technology) degree in Computer Science & Engineering from Sri Satya Sai Institute Of Science & Technology, RGPV Bhopal, In 2010 M.P., Ph.D in Computer Science & Enginnering From Barkatullah University Bhopal India. Presently he is Associate Professor Of Computer Science and Engineering Department in RKDFIST,BHOPAL,M.P. India. He is having 12 Yrs of teaching experience .He has published 54 papers in referred International/National Journal & conference also a Member of Easy Chair Conference System.