Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

Mathematical Tools for Cryptography

Dr. Vasanthakumari T. N.*

Assistant Professor, Department of Mathematics, Government First Grade College, Tumakuru

Abstract – The Information protection has been an important part of human life from ancient time. In computer field, information security becomes more and more important for humanity and new emerging technologies are developing in recent days. Cryptography is one of the most important techniques used for securing transmission of messages and protection of data in the present days. Which includes e-commerce; electronic communications such as mobile communications, sending the emails; business transactions which can be cash transaction or cashless transactions; Pay-TV; transmitting financial information; security of ATM cards; computer passwords etc, which includes on many aspects of our daily lives. Cryptography provides privacy and security for the secret information by hiding it. This can be done through mathematical technique. Laplace transform has many applications in various fields one such application is the cryptography. This technique uses a new iterative method for cryptography, in which can be applied successive Laplace transform of suitable function for encrypting the plain text and apply corresponding inverse Laplace transform for decryption. Generalization of the results is also obtained. Encryption by Laplace Transform is resistance to nearly all types of attacks on symmetric encryption algorithms. There is flexibility in implementation of algorithms. One can implement the algorithms as per the application demands. Which can find many application of encryption by Laplace Transform in banking, Security, One time password generation (OTP).

----------X----------

INTRODUCTION

In present world, with increasing usage of computer networks and internet, the importance of network, computer and information security is must. For the purpose of securing the data or, information which has to be protected from unauthorized access. Hence, data security has become a critical and important issue. One of the widely used approaches for information security is Cryptography. Cryptography, the mathematic of encryption, plays a vital role in many fields. The fundamental aim of cryptography is to enable two people, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. Encryption is the process of obscuring information to make it unreadable without special knowledge. A cipher is an algorithm for performing encryption (and on other hand, decryption) a series of well-defined steps that can be followed as a procedure. The original information is known as plain text, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it. Ciphers are usually parameterized by a piece of auxiliary information, called a key. The encrypting procedure is varied depending on the type of key which can changes the detailed operation of the algorithm. Without the key, the plaintext cannot be encrypted, or more importantly, to decryption varied depending on the key which changes the detailed operation of the algorithm.

ENCRYPTION:

This is based on theorems as mentioned below.

1. The given plane text in terms of $G_{i,o}$ i=1,2,3,……., under Laplace of $Gt^2\sinh 2r$ (that is by writing them as a coefficients of $t^2\sinh 2r$ and then taking the Laplace transform) can be converted to cipher text

$$G_{i,1} = 2^{2i+1}(2i+2)(2i+3)G_{i,0}, \text{ mod } 26 = q_{i,1}-26k_{i,1}, \text{ for } i=0,1,2,3,\ldots\ldots Z$$

Where

$$q_{i,1}=2^{2i+1}(2i+2)(2i+3)G_{i,0} \quad i=0,1,2,3\ldots\ldots$$

And key is

$$K_{i,1} = \frac{ki,1-Gi,1}{26} \quad \text{for } i=0,1,2,3,\ldots\ldots..$$

2. The given plan text in terms of $G_{i,0}$ i=0,1,2,3,……. Under Laplace transform of $G_{i,0}t^2\sinh 2t$, successively j times (that is writing them as a coefficients of $t^2\sinh 2t$ and then taking the Laplace transform

www.ignited.in

successively) can be converted to cipher text

$$G_{i,j} = G_{i,j-1}2^{2i+1}(2i+2)(2i+3) \bmod 26$$

$$=q_{i,j}-26k_{i,j} \quad i,j=0,1,2,3,\ldots\ldots$$

Where

$$q_{i,j} = G_{i,j-1}2^{2i+1}(2i+2)(2i+3)$$

i , j =0,1,2,3……

and a key is

$$k_{i,j} = \frac{qi,j-Gi,j}{26} \quad i,j=0,1,2,3,\ldots\ldots\ldots$$

Decryption:

1. The given cipher text in terms of $G_{i,1}$ i=0,1,2,3,4,……with a given key

$k_{i,0}$, i = 0,1,2,3,…..which can be converted to plain text $G_{i,0}$ under the inverse Laplace transform of

$$G\left(-\frac{d}{ds}\right)^2 \frac{2}{(s^2-2^2)} = \sum_{i=0}^{n} \frac{q_{i,0}}{s^{2i+4}},$$

Where

$$G_{i,0} = \frac{26k_{i,0}+G_{i,1}}{2^{2i+1}(2i+2)(2i+3)},$$

i = 01,2,3,…..

and

$q_{i.0} = 26k_{i,0} + G_{i\,1}$ i= 0,1,2,3,…..

2. The given cipher text in terms of $G_{i,j}$ i , j =1,2,3,4,…..with a given key

$k_{i,j-1}$ i ,j =1,2,3,4,……can be converted to plain text

$G_{i,j-1}$ under the inverse Laplace transform of

$$G\left(-\frac{d}{ds}\right)^2 \frac{2}{(s^2-2^2)} = \sum_{i=0}^{n} \frac{q_{i,j-1}}{s^{2i+4}},$$

Where

$$G_{i,j-1} = \frac{26k_{i,j-1}+G_{i,j}}{2^{2i+1}(2i+2)(2i+3)},$$

i, j = 1,2,3,4,…… and $q_{i,j}$ =$26k_{i,j}$ + $G_{i,j}$ i , j =1,2,3,4,…….

CONCLUSION:

Many sectors such as banking and other financial institutions are adopting e-services and improving their Internet services. However, the e-service requirements are also opening up new opportunity to commit financial fraud. Internet banking fraud is one of the most serious electronic crimes and mostly committed by unauthorized users. The new method of key generation scheme developed in this paper may be used for a fraud prevention mechanism

For computer network security random number generation is a prime important task and also it is very essential in constructing keys for cryptographic algorithm. Method used in this review paper can be useful for random number generation

BIBLIOGRAPHY:

[1] Alexander Stanoyevitch (2002). Introduction to cryptography with mathematical foundations and computer implementations, CRC Press.

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

[3] Blakley G.R. (1999). Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium.

[4] Dhanorkar G.A. and Hiwarekar A.P. (2011). A generalized Hill cipher using matrix transformation, International J. of Math. Sci. & Engg. Appls,Vol.5 No. IV, pp. 19-23.

[5] Eric C., Ronald K., James W.C. (2009). Netwark Security Bible Second edn.,Wiley India pub.

[6] Erwin Kreyszing (1999). Advanced Engineering Mathematics, John Wiley and Sons Inc.

REFERENCES:

[1] G.Naga Lakshmi, B.Ravi Kumar and A.ChandraSekhar, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2515-2519, (2011).

[2] Grewal B.S., Higher Engineering Mathematics, Khanna Pub., Delhi, (2005).

[3] Gupta P., Mishra P. R., Cryptanalysis of "A New Method of Cryptography Using Laplace Transform, Proceedings of the Third International Conference on Soft Computing for Problem Solving Advances

in Intelligent Systems and Computing Vol.258, 2014, 539-546

[4] Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), 1193-1197, (2012).

[5] Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive, 4(2), 208-213, (2013).

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

[7] Lokenath Debnath, Dambaru Bhatta (2010). Integrl Transforms and Their Applications, Chapman and Hall/CRC, First Indian edn.

[8] Overbey J., Traves W.and Wojdylo J. (2005). On the Keyspace of the Hill Cipher, Cryptologia, 29, pp. 59-72.

[9] Ramana B.V. (2007). Higher Engineering Mathematics, Tata McGraw-Hills.

Corresponding Author

Dr. Vasanthakumari T. N.*

Assistant Professor, Department of Mathematics, Government First Grade College, Tumakuru