APPLICATION OF LAPLACE-MAHGOUB TRANSFORM IN CRYPTOGRAPHY

Dr. C. Devi Shyamala Mary[1], B.Pavithra[2],

[1]Assistant Professor, PG and Research Department of Mathematics, St. Joseph's College of Arts and Science (Autonomous), cuddalore-1.

[2]PG Student, PG and Research Department of Mathematics, St. Joseph's College of Arts and Science, (Autonomous), Cuddalore-1.

ABSTRACT

Cryptography is a study of secret messages in which mathematics plays a vital role to encrypt and decrypt data. This paper aim is to encrypt and decrypt a message by a new mathematical method Laplace-Mahgoub transform.

KEYWORDS: Cryptography, Encryption, Decryption, Laplace transform, Mahgoub transform.

1. INTRODUCTION:

Cryptography is an art of secure transfer of messages in the presence of third party. The name cryptography was arise from the Greek "kryptos" meaning "hidden" and "graphein" meaning "to write". Julius Caesar was the first known use of modern cipher (100BC to 44BC) to communicate with his governors and officers. He created the system in which each character in his message was replaced by a character of three positions ahead in Roman alphabet. Cryptography plays a major role in transfer of sensitive information and has proved success in war and business. In our country, we are facing various types of crimes. So, it is very important to secure

- Internet
- Computer passwords
- Mobile communications
- Transfer of important files
- Security of ATM cards etc.

There are three types of cryptographic technique used in general

- Symmetric-key cryptography
- Asymmetric-key cryptography
- Hash functions

In symmetric key cryptography the sender and the receiver uses the same key.

In asymmetric key cryptography two keys are used public and private key. Public key known to everyone while the private key is kept secret.

No key is used in hash function algorithm. It is used in many operating systems to encrypt passwords.

In this paper, we introduced a new mathematical method of Laplace-Mahgoub transform. Thus for encrypting the message or plaintext we used Laplace-Mahgoub transform and inverse Laplace-Mahgoub transform for decryption.

2. DEFINITION:

2.1 LAPLACE TRANSFORM A function $f(t)$ is defined for all positive values of t, then the Laplace transform $f(t)$ is given by,

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt \qquad (1.1)$$

The parameter "s" is real or complex number.

2.2 MAHGOUB TRANSFORM The Mahgoub transform is given by the integral

$$M[f(m)] = H(v) = v\int_0^\infty e^{-vm} f(m)dm, \text{ where } m \geq 0 \qquad (1.2)$$

2.3 SOME RESULTS FOR LAPLACE AND MAHGOUB TRANSFORM

- $L[t^n] = \frac{n!}{s^{n+1}}$ $\qquad L^{-1}\left[\frac{n!}{s^{n+1}}\right] = t^n$
- $M[m^2] = \frac{2!}{v^2}$ $\qquad M^{-1}\left[\frac{2!}{v^2}\right] = m^2$

3. MAIN RESULT:

3.1 SYMMETRIC-KEY CRYPTOGRAPHY:

3.1.1 ENCRYPTION:

We consider the expansion

$$\sinh rt = rt + \frac{(rt)^3}{3!} + \frac{(rt)^5}{5!} + \ldots\ldots\ldots$$

$$= \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{(2i+1)!}$$

We allocate the values 'a to z' as '0-25' and space=26. Suppose that "mail me" is the given message, convert it into code as

C_0 =m=12 C_1=a=0 C_2 =i=8
C_3 =l=11 C_4 =space=26 C_5 =m=12 C_6 =e=14

Take the function, $f(t,m) = C_i m^2 \sinh rt = \sum_{i=0}^{\infty} C_i m^2 \frac{(rt)^{2i+1}}{(2i+1)!}$

Taking Laplace-Mahgoub transform both sides,

$$LM[F(t,m)] = F(s,v) = v\int_0^\infty\int_0^\infty e^{-(st+vm)} f(t,m)dtdm$$

$$F(s,v) = v\int_0^\infty\int_0^\infty e^{-(st+vm)} \sum_{i=0}^{\infty} C_i m^2 \frac{(rt)^{2i+1}}{(2i+1)!}dtdm$$

$$F(s,v) = \int_0^\infty e^{-st} \sum_{i=0}^{\infty} C_i \frac{(rt)^{2i+1}}{(2i+1)!}dt.v\int_0^\infty e^{-vm} m^2 dm$$

Take r=4

$$F(s,v) = L\left\{\sum_{i=0}^{\infty} C_i \frac{(rt)^{2i+1}}{(2i+1)!}\right\}.\frac{2!}{v^2}$$

Thus,

H_0=96 H_4=13631488 H_1=0
H_5=100663296 H_2=16384
H_6=1879048192 H_3=360448

The above series quotient and remainder term is given by q_n and $C_n{}'$ for n=0,1,2,….

$$H_n=27q_n+C_n{}'$$

q_0=3 q_4=504869 q_1=0
q_5=3728270 q_2=606
q_6=69594377 q_3=13349

So, the code changes to

C_0=15 C_4=25 C_1=0
C_5=6 C_2=22 C_6=13
C_3=25

Put the values calculated

$$F(s,v) = \frac{1}{v^2}\left[\frac{15}{s^2} + \frac{0}{s^4} + \frac{22}{s^6} + \frac{25}{s^8} + \frac{25}{s^{10}} + \frac{6}{s^{12}} + \frac{13}{s^{14}}\right]$$

Hence the message “mail me” is converted into “pawzzgn”.

THEOREM 1.1:

The plaintext “C_n” for n=0,1,2,….. is transferred to cipher text “$C_n{}'$” with the keys q_n for n=0,1,2,…. By using Laplace-Mahgoub transform. The function which we take

$f(t,m) = C_n m^2 \sinh rt$ where $C_n=H_n-27q_n$ for n=0,1,2…. and $\frac{H_n - C_n}{27} = q_n$

3.1.2 DECRYPTION:

We received a message "pawzzgn" which is equivalent to

15 0 22 25 25 6 13

$$F(s,v)=\frac{1}{v^2}\sum_{n=0}^{\infty}\frac{H_n}{s^{2n+2}}$$

$$F(s,v)=\frac{1}{v^2}\left[\frac{96}{s^2}+\frac{0}{s^4}+\frac{16384}{s^6}+\frac{360448}{s^8}+\frac{13631488}{s^{10}}+\frac{100663296}{s^{12}}+\frac{1879048192}{s^{14}}\right]$$

Take inverse Laplace-Mahgoub transform then the above equation becomes

$$f(t,m)=C_i m^2\sinh rt=\sum_{i=0}^{\infty}C_i m^2\frac{(rt)^{2i+1}}{(2i+1)!}$$

Hence the message changes the cipher text "pawzzgn" to the plain text "mail me".

THEOREM 1.2:

The cipher text " C_n' " for n=0,1,2,…… is changed into the plaintext " C_n " with the keys H_n for n=0,1,2,….. by using inverse Laplace-Mahgoub transform.

$$f(s,v)=\frac{1}{v^2}\sum_{n=0}^{\infty}\frac{H_n}{s^{2n+2}}$$ where, $H_n=C_n+27q_n$ for n=0,1,2,3……

3.2 ASYMMETRIC-KEY CRYPTOGRAPHY: 3.2.1 ENCRYPTION:

From the above example, by applying Laplace-Mahgoub transform the plaintext "mail me" is converted into the cipher text "pawzzgn" with the key

q_0=3 q_4=504869 q_1=0
q_5=3728270 q_2=606
q_6=69594377 q_3=13349

in asymmetric key cryptography, now the sender changes this key into public key by

$$P_n=q_n+3$$

Thus the plaintext "mail me" is changed to the cipher text "pawzzgn" with the public key

P_0=7 P_4=504872 P_1=3
P_5=3728273 P_2=609 P_6=69594380
P_3=13352

3.2.2 DECRYPTION:

We received a cipher text "pawzzgn" and public key

P_0=7 P_4=504872 P_1=3
P_5=3728273 P_2=609 P_6=69594380
P_3=13352

Now the receiver uses the key

$$q_n=P_n-3$$

Thus, we have

q_0=3 q_4=504869 q_1=0
q_5=3728270 q_2=606
q_6=69594377 q_3=13349

By applying inverse Laplace-Mahgoub transform the cipher text is converted into the plaintext "mail me".

4. ILLUSTRATIVE EXAMPLES:

suppose that the original message is "mail me". Using the result we can convert it to

- 'va iqml' for r=2
- 'saaaaaa' for r=3
- 'maxlcvf' for r=5
- 'jaaaaaa' for r=6

5. CONCLUSION:

In today's world cryptography is one of major defense against hackers. In the proposed work, a new cryptography scheme was introduced using Laplace-Mahgoub transform and the number of multiples of mod 'n' is used as the key. Therefore, it is very difficult for an eyedropper to trace the key by any attack.

REFERENCES:

1. **Alexander Stanoyevitch,** Introduction to cryptography with mathematical foundations and computer implementations, CRC press, (2002).
2. **Barr T.H.** Invitation to cryptography, Prentice Hall. (2002).
3. **Blakley G.R.** Twenty years of cryptography in the open literature, Security and privacy 1999, Proceedings of the IEEE symposium, 9-12, (May 1999).
4. **Diffie. W. and Hellman. M. E.** New direction in cryptography. IEEE Transactions on information Theory. 22, 633-654,1976.
5. **G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar,** A cryptographic scheme of Laplace transforms, International Journal of mathematical Archive-2. 2515-2519,(2011).
6. **Hiwarekar A.P.** A new method of cryptography using Laplace transform. International Journal of Mathematical Archieve.3(3),1193-1197, (2012).
7. **Hiwarekar A.P.** A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archieve.4 (2), 208-213, (2013).

8. **Hiwarekar AP.** Application of Laplace transform for Cryptographic scheme. Proceeding of World Congress on Engineering 2013; II, LNCS, 95-100.
9. **Hiwarekar AP.** New Mathematical Modeling for Cryptography. Journal of Information Assurance and Security, MIR lab USA, 2014; 9:027-033.
10. **Johannes A. Buchmann,** Introduction to cryptography, Fourth Edn., Indian Reprint, Springer, (2009).
11. **Lokenath Debnath, Dambaru Bhatta,** Integral Transforms and Their Applications, Chapman and Hall/CRC, First Indian edn. (2010).
12. **Mohand M. Abdelrahim Mahgoub.,** The New Integral Transform Mahgoub Transform, Advances in Theoretical and Applied Mathematics, 11(4),pp.391-398,(2016).
13. **Mahdi FM.** Laplace transformation as a tool algorithm for the classical cryptography.IJSR: ISSN (2319-7064). 2016;(5):10.
14. **M.T. Gençoğlu,** Use of integral transform in cryptology, science and Eng. J of Firat Univ. 28 (2) (2016), 217-220.
15. **Murry R. Spiegel.,** A text book of Laplace Transforms, Schaum's outlines.
16. **Oded G.** Foundations of cryptography-A Primer. FnT-TCS. 2005;1(1):116.
17. **P. Senthil Kumar, S. Vasuki**, An application of MAHGOUB transform in cryptography, Advances in theoretical and applied mathematics, volume 2(2018),pp.
18. **Stallings W.,** Cryptography and Network Security, Fourth Edition, Prentice Hall,2005