MATHEMATICAL APPROACH TO MODERN ENCRYPTION AND DECRYPTION USING LAPLACE TRANSFORM

Article · March 2019

CITATIONS
0

READS
347

4 authors:

Varun Kodathala
Orbitshifters Inc
7 PUBLICATIONS **17** CITATIONS
SEE PROFILE

Kandagadla Ashok Kumar
GITAM University
5 PUBLICATIONS **17** CITATIONS
SEE PROFILE

Guddam Sulthan Mohiddin Basha
GITAM University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Rakesh Chowdary Vunnam
GITAM University
5 PUBLICATIONS **17** CITATIONS
SEE PROFILE

MATHEMATICAL APPROACH TO MODERN ENCRYPTION AND DECRYPTION USING LAPLACE TRANSFORM

[1]Kodathala Sai Varun, [2]Kandagadla Ashok Kumar, [3]Guddam Sulthan Mohiddin Basha, [4]Vunnam Rakesh Chowdary

[1]Student, [2]Student, [3]Student, [4]Student

[1]Department of Electronics and Communication,

[1]Gitam School of Technology, Bengaluru, India

***Abstract*:** In this paper we investigated the mathematical analysis for modern cryptography by using suitable expansion and transform. Cryptography is a branch which deals with information detection and protection this is usually done using cryptography techniques known as cryptography algorithm. Laplace transform can be keenly adopted for cryptography. The same Laplace transform is used for encryption and its inverse is used for decryption. Apart from Laplace Z-Transforms can be adopted. By adoption of this technique the main propaganda of cryptography i.e. protected transmission of information is achieved.

***Index Terms*: Information, Information transmission, Laplace transform, Cryptography, Encryption, Decryption, Plain text, Cipher text.**

I. Introduction:

The present scenario indicates the excessive usage of Computers and Network system which insists the clients or the users to be aware of cracking of information because these networks are usually open who can access from anywhere this proves the requirement of some mechanism which can protect the data from being exploitation. The technique is named as Cryptography [1]. This Cryptography adopted everywhere like defense sector, Institutions, Hospitals, Etc. The adverse effects if we neglect cryptography can not be imagine this leads to misusage of information by unwanted parties [2].

Block diagram:

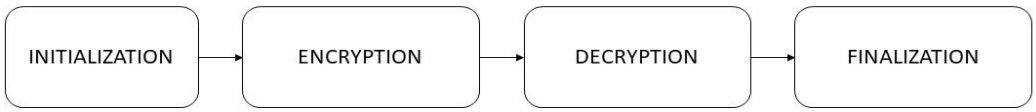

Fig (1): Block Diagram

Cryptography includes four sub categories namely:

1. Initialization
2. Encryption
3. Decryption
4. Finalization

Initialization phase includes the intake of information or message to be protected or encrypted [3]. This message is converted to corresponding numerical value according to the values assigned to it [4]. Encryption is a phase where the input signal message is encoded into protected from [5]. The initialization and encryption stages correspond to transmission stage [6].

Decryption phase decodes the encrypted or decrypted message by adopting the proposed technique. The final phase is transmission of decrypted message to client. These two phases are executed at receiving end [7].

The Laplace transform is transform applied for the conversion of time domain to complex frequency domain. This method is adopted in our proposal in order to encrypt and decrypt the data by making use of usual Mathematics [8]. The Laplace transform is given by

$$L\{f(t)\} = \int_{-\infty}^{\infty} f(t)e^{-st}dt$$

The proposed method is expected and found to be better topology then usual techniques and mentioned in various papers [9]. The proposal method uses series expansion so for different information or the importance or the priority of message the series can be varied for better encryption and the same is evaluated for decryption [10].

II. Methodology:

The proposed Cryptography algorithm is as follows

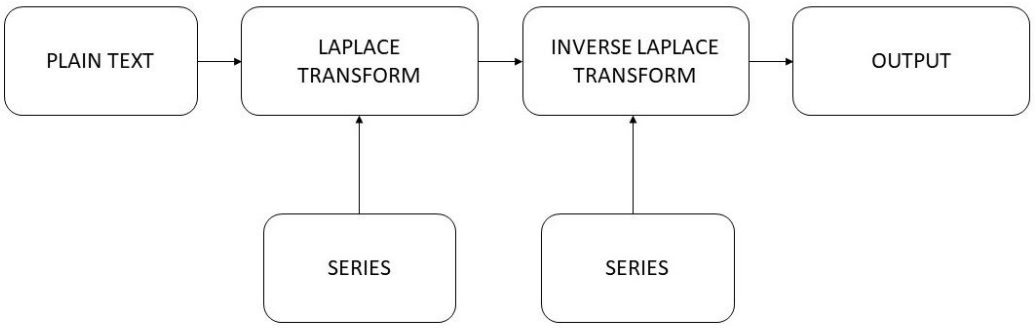

Fig (2): Cryptography Algorithm

The basic terminology is mentioned in below table

Table (1): Parameters specification

Sl. No.	Parameter	Significance
1	Plain text	The raw message required to be encrypted
2	Cipher text	The encoded text
3	Decrypted text	The decoded text
4	$G_{i,0}$	The numerical equivalent of message text
5	T	The coefficients of mathematical operated equation
6	M	Modulated coefficients
7	K	Key of the transmission
8	D	The decryption mathematical equation
9	Q	Coefficients used for decryption

Some standard formulas of Laplace Transform:

1. $L\{te^t\} = \frac{1}{(S-1)^2}$
2. $L\{t^n\} = \frac{n!}{S^{n+1}}$
3. $L^{-1}\left\{\frac{1}{S^n}\right\} = \frac{1}{(n-1)!}t^{n-1}$

The numerical assignment for alphabets according to our convenience is as follows:

Table (2): Numerical assignment of letters

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

III. Encryption:

The proposed model is explained using an illustration: **GITAMUNIV**. The corresponding numerical assignment for given illustration is **6-8-9-0-12-20-13-8-21.** The series explored to solve this problem is e^x.

The series is given as:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} + \frac{x^7}{7!} + \frac{x^8}{8!}$$

Neglected higher order terms as per the requirement. The plain text obtained from message or source information is

$G_{0,0} = 6$, $G_{1,0} = 8$, $G_{2,0} = 9$, $G_{3,0} = 0$, $G_{4,0} = 12$, $G_{5,0} = 20$, $G_{6,0} = 13$, $G_{7,0} = 8$, $G_{8,0} = 21$.

The coefficients multiplied with the series is given as

$$G_{i,o}e^x = G_{0,0}(1) + \frac{G_{1,0}x}{1!} + \frac{G_{2,0}x^2}{2!} + \frac{G_{3,0}x^3}{3!} + \frac{G_{4,0}x^4}{4!} + \frac{G_{5,0}x^5}{5!} + \frac{G_{6,0}x^6}{6!} + \frac{G_{7,0}x^7}{7!} + \frac{G_{8,0}x^8}{8!}$$

The above equation is multiplied with x to avoid x^0. Equation is rewritten as

$$G_{i,o}e^x(x) = G_{0,0}(x) + \frac{G_{1,0}x^2}{1!} + \frac{G_{2,0}x^3}{2!} + \frac{G_{3,0}x^4}{3!} + \frac{G_{4,0}x^5}{4!} + \frac{G_{5,0}x^6}{5!} + \frac{G_{6,0}x^7}{6!} + \frac{G_{7,0}x^8}{7!} + \frac{G_{8,0}x^9}{8!}$$

Substituting the plain-text coefficients in above equation is expressed as

$$G_{i,o}e^x(x) = 6x + \frac{8*x^2}{1!} + \frac{19*x^3}{2!} + \frac{0*x^4}{3!} + \frac{12*x^5}{4!} + \frac{20*x^6}{5!} + \frac{13*x^7}{6!} + \frac{8*x^8}{7!} + \frac{21*x^9}{8!}$$

Applying Laplace transform for above equation is given as

$$L\{G_{i,0}e^x(x)\} = \frac{6}{S^2} + \frac{8*2!}{S^3} + \frac{19*3!}{2!*S^4} + \frac{0*4!}{3!*S^5} + \frac{12*5!}{4!*S^6} + \frac{20*6!}{5!*S^7} + \frac{13*7!}{6!*S^8} + \frac{8*8!}{7!*S^9} + \frac{21*9!}{8!*S^{10}}$$

By solving coefficients are given as

$T_0 = 6$, $T_1 = 16$, $T_2 = 57$, $T_3 = 0$, $T_4 = 60$, $T_5 = 120$, $T_6 = 91$, $T_7 = 64$, $T_8 = 189$

These coefficients cannot be expressed as alphabets so these coefficients are divided with 26 and the remainders are expressed as alphabets this message is sent to receiver. This can be achieved by mod operator.

$M_0 = 6 \bmod 26 = 6$, $M_1 = 16 \bmod 26 = 16$, $M_2 = 57 \bmod 26 = 5$, $M_3 = 0 \bmod 26 = 0$, $M_4 = 60 \bmod 26 = 8$, $M_5 = 120 \bmod 26 = 16$, $M_6 = 91 \bmod 26 = 13$, $M_7 = 64 \bmod 26 = 12$, $M_8 = 189 \bmod 26 = 7$

The word formed using these modulated coefficients is **GQFAIQNHM.** The encrypted message of GITAMUNIV is GWFAIQNHM. By this way encryption process is done using Laplace transform.

The one more important parameter required to determined for transmission of this encrypted data is **KEY (K_i).** This can be done using normal division rule,

If d represents divisor, D represents divider, Q represents Quotient, and R represents remainder then the equation is given as d * R + Q = K.

For considered example, d = 26 (Total number of alphabets), R = M_i (Modulated values), then key is generated as follows

$K_0 = 0$, $K_1 = 0$, $K_2 = 2$, $K_3 = 0$, $K_4 = 2$, $K_5 = 4$, $K_6 = 3$, $K_7 = 2$, $K_8 = 7$.

The required elements to be transmitted are: Modulated message (GQFAIQNMH), KEY (K_i) Series (xe^x).

IV. Decryption:

The decryption process is done at receiver end with the help of these parameters mentioned before. The received modulated message **GQFAIQNMH** is converted to corresponding numerical equivalent **6-16-5-0-8-16-13-12-7** then it is converted to Q form with the help of equation,

$Q_{i,o} = G_{i,o} + 26K_{i.}$

The obtained results are as follows:

$Q_{0,0} = 6$, $Q_{1,0} = 16$, $Q_{2,0} = 57$, $Q_{3,0} = 0$, $Q_{4,0} = 60$, $Q_{5,0} = 120$, $Q_{6,0} = 91$, $Q_{7,0} = 64$, $Q_{8,0} = 189$.

From the given parameter (series) the Laplacian equation is determined as follows:

$$D = \frac{0!}{S^2} + \frac{1!}{S^3} + \frac{2!}{S^4} + \frac{3!}{S^5} + \frac{4!}{S^6} + \frac{5!}{S^7} + \frac{6!}{S^8} + \frac{7!}{S^9} + \frac{8!}{S^{10}}$$

The process is continued by multiplying the coefficients $Q_{i,0}$ The resultant equation is given as

$$DQ_{i,0} = \frac{Q_{0,0}0!}{S^2} + \frac{Q_{1,0}1!}{S^3} + \frac{Q_{2,0}2!}{S^4} + \frac{Q_{3,0}3!}{S^5} + \frac{Q_{4,0}4!}{S^6} + \frac{Q_{5,0}5!}{S^7} + \frac{Q_{6,0}6!}{S^8} + \frac{Q_{7,0}7!}{S^9} + \frac{Q_{8,0}8!}{S^{10}}$$

$$DQ_{i,0} = \frac{6*0!}{S^2} + \frac{16*1!}{S^3} + \frac{57*2!}{S^4} + \frac{0*3!}{S^5} + \frac{60*4!}{S^6} + \frac{120*5!}{S^7} + \frac{91*6!}{S^8} + \frac{64*7!}{S^9} + \frac{189*8!}{S^{10}}$$

Then Inverse Laplace transform is applied to above equation which reverts to original form as shown below

$$L^{-1}\{DQ_{i,0}\} = \frac{6*0!}{1!} + \frac{16*1!}{2!} + \frac{57*2!}{3!} + \frac{0*3!}{4!} + \frac{60*4!}{5!} + \frac{120*5!}{6!} + \frac{91*6!}{7!} + \frac{64*7!}{8!} + \frac{189*8!}{9!}$$

By taking coefficients of reverted message and converting it to alphabet manner the original message is retrieved. This process is adopted in different aspects for better results.

The reverted message is **GITAMUNIV (6-8-9-0-12-20-13-8-21).**

V. Comparative analysis:

Abdulaziz B.M. Hamed and Ibrahim O.A. Albudawe discussed the iterative method adopted for cryptography using the matrix background [11]. Here they adopted the technique of encrypting and decrypting using inverse matrix method this method involves complex nature and difficulty at receiver end. The proposed technique provides the encryption and decryption method which can be done with ease and protect the data as well. The protection is increased by complexing the series or the multiplier. The decryption can only to be done by the receiver who is capable to decrypt the algorithm with the key, the proposed method analyses suggests that key protection can be done in better manner rather than the text so this proposed method is expected to be efficient rather than all existing techniques.

VI. Discussions and Conclusions:

- The development is the cause for excess usage of technology, this leaded to excess use of computer applications and networks, most of the computer networks are open which exhibits the information open to everyone where there is a scope to modify the data or misuse the appropriate data which is not favorable case.
- The main fields which are affected are banking and financial sectors, defense sectors, personal blogs, personal profiles (like Social networking sites).
- The complete solution is achieved by adopting cryptography technique. Because the determination of key is difficult for any malware user.
- The trace of information can be determined that ease without proper information about the algorithm and the key.
- To decrease the risk of pirate of data the key is generated dynamically which helps the respected client to retrieve data safe.
- The same process can be represented using Z transforms which is used to solve for discrete values.

References:

[1] Invitation to Cryptography, Prentice Hall Barr TH , 2002.

[2] Methods for Protection of Key in Private Key Cryptography, International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-5, Issue-2, March 2017.

[3] A new method of cryptography using Laplace transform, P. Hiwarekar 13-03-12.

[4] Comparative study of Cryptography Algorithms, Manisha Vishwakarma, International Journal of Advanced Research in Computer Science, Volume 4, No. 3, March 2013.

[5] A cryptographic scheme of Laplace transforms G. Naga Lakshmi, Ravi Kumar B and Chandra Sekhar A 2011.

[7] Cryptography using Chebyshev polynomials G. J. Fee and M. B. Monagan V5A 1S6.

[8] A research Paper on Cryptography Encryption and Compression Techniques, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919.

[9] Incrementing visual cryptography using random grids Ran-ZanWang a Yung-ChingLana, 1 November 2010.

[10] Protection of Key in Private Key Cryptography, NehaTyagi, AshishAgarwal, AnuragKatiyar, ShubhamGarg, ShudhanshuYadav International Journal of Advanced Research, Volume 5, Issue 2, Feb 2017.

[11] Encrypt and Decrypt Messages Using Invertible Matrices Modulo 27, Abdulaziz B.M. Hamed and Ibrahim O.A. Albudawe, American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-6, Issue-6, pp-212-217