Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 1889–1895
DOI : 10.47974/JDMSC-1680

A new approach of cryptography using Taylor series of logarithm function

Bashar Ahmed Sharba *
Roaa Razaq Al-Khalidy †
Department of Mathematics
Faculty of Computer Science and Mathematics
University of Kufa
Iraq

Raghad I. Hussein §
Department of Pharmacognosy and Medicinal Plants
Faculty of Pharmacy
University of Kufa
Najaf
Iraq

Abstract

This study investigated a novel cryptographic approach involving the encryption of plaintext using the coefficients of a Taylor series for the logarithm function multiplied by its corresponding index. The decryption process utilized the Laplace transform of the logarithm function and its inverse. Through this methodology, several innovative mathematical encryptions and decryption formulas were derived. The study also includes a practical example to demonstrate the broader implications of the findings.

Subject Classification: *Primary 15A80, Secondary 94A60.*

Keywords: *Cryptography, Taylor series, Laplace transformation, The inverse of laplace transformation.*

* *E-mail:* **bashara.hamod@uokufa.edu.iq (Corresponding Author)**
† *E-mail:* **Ragadi.alfarhani@uokufa.edu.iq**
§ *E-mail:* **rowar.alkhalidy@uokufa.edu.iq**

1. Introduction

The main goal of cryptography is to make it feasible for two people to communicate via a risky channel in a way that makes it difficult for an adversary to decipher what they are saying. Through the use of encryption, information is made difficult to read without the right tools. This strategy involves making our communication unsecured to prevent it from being intercepted. The unencrypted data version is called cypher text, and the original data is known as plain text. Cryptographers use cyphers to perform encryption (and the opposite, decryption) in a set of clearly defined steps that can be carried out as a method. In 2011, Dhanorkar and Hiwarekar inverted the key matrix needed to encrypt the plaintext. However, the encrypted text cannot be decoded if the key matrix is not invertible [1]. In 2012, Hiwarekar introduced a novel method of cryptography in which the plaintext was encrypted using the Laplace transform and decrypted using the inverse Laplace transform[2]. In 2013, Hiwarekar created a new cryptographic algorithm in which the plain text was encrypted using the hyperbolic function Laplace transforms, and the decryption process used the inverse Laplace transform [3]. In 2017, Gençoğlu examined Laplace Transform-based cryptosystems' security using a broad attack that was put out. The proposed technique described in the referenced work was able to bypass password security without requiring access to the secret key [4]. Elzaki incorporated the Laplace transformation developed by Jadhav Shaila Shivaji and Hiwarekar A.P. in 2021 to devise a new cryptographic approach [5]. In this study, we introduce a novel cryptographic technique that leverages the Laplace transformation of the logarithm function. This technique allows the encryption of plaintext using private keys. The ciphertext can then be decrypted using the inverse of the Laplace transformation. We present precise mathematical expressions for the encryption and decryption processes for the first time. Additionally, an algorithm is provided as an illustrative example of our methodology in action.

2. Some Basic Concepts and Notations

The Laplace transformation finds applications in various fields of study, including mechanics, electrical circuits, heat conduction, beam problems, wave equations, transmission lines, control systems, signals and systems, communication systems, hydrodynamics, and solar systems [4,8]. In this work, we specifically focus on its relevance and application in the field of cryptography.

The Laplace transform: The Laplace Transform is defined as a function that has a definition for all positive values of as

$$\mathcal{L}\{f(t)\} = \mathcal{F}(p) = \int_0^\infty e^{-pt} f(t)dt \tag{1}$$

assuming that the integral is present. A real or complex number is used here as the argument. The related inverse Laplace transform is.

Then $\mathcal{F}(p)\} = f(t)$

Theorem: The linear transform of Laplace transform is

$$\mathcal{L}\{\mathbb{f}_1(t)\} = \mathcal{F}_1(p). \quad \mathcal{L}\{\mathbb{f}_2(t)\} = \mathcal{F}_2(p). \cdots \mathcal{L}\{\mathbb{f}_n(t)\} = \mathcal{F}_n(p)$$

Then

$$\mathcal{L}\{\mu_1\mathbb{f}_1(t) + \mu_2\mathbb{f}_2(t) + \cdots \mu_n\mathbb{f}_n(t)\} = \mu_1\mathcal{F}_1(p) + \mu_2\mathcal{F}_2(p) + \cdots + \mu_n\mathcal{F}_n(p).$$

where $\mu_1.\mu_2.\cdots.\mu_n$ are constants

3. Main Results

This section introduces a new approach to encrypting plain text using the Tayler series of logarithm functions and gives a new formula for encryption and deception.

3.1 *Encryption*

We consider Tayler's expansion

$$\frac{1}{1-t} = 1 + t + t^2 + t^3 + \cdots$$

Integrate both sides of the geometric series from 0 to $\mathcal{X}$ to get:

$$\int_0^{\mathcal{X}} \frac{1}{1-t}dt = \int_0^{\mathcal{X}} (1 + t + t^2 + t^3 + \cdots)dt$$

$$-\ln(1-\mathcal{X}) = \mathcal{X} + \frac{\mathcal{X}^2}{2} + \frac{\mathcal{X}^3}{3} + \frac{\mathcal{X}^4}{4} + \cdots = \sum_{i=0}^{\infty} \frac{\mathcal{X}^{i+1}}{i+1}$$

$$-\mathcal{X}^2\ln(1-x) = \left(\mathcal{X}^3 + \frac{\mathcal{X}^4}{2} + \frac{\mathcal{X}^5}{3} + \frac{\mathcal{X}^5}{4} + \cdots\right) = \sum_{i=0}^{\infty} \frac{\mathcal{X}^{3+i}}{i+1} \qquad (2)$$

We assigned 0 for A, 1 for B, and Z would be 25

Let given any message called plaintext; we refer to the locate of the first letter of the massage by ζ_0 , the locate of the second letter by ζ_1 , the locate of the third letter by ζ_2,…, and the locate of an nth letter by ζ_{n-1} such that $\zeta_n = 0.n \geqslant \ell$ where ℓ is the length of the massage, now we product the values of $\zeta_i.i = 0.1.2.\ldots.\ell - 1$ by the coefficients of the series in (2.2), we have

$$H(x) = -\zeta\mathcal{X}^2\ln(1-x)$$

$$= \left(\zeta_0\,\mathcal{X}^3 + \frac{\zeta_1\mathcal{X}^4}{2} + \frac{\zeta_2\mathcal{X}^5}{3} + \frac{\zeta_3\mathcal{X}^6}{4} + \cdots + \frac{\zeta_{\ell-1}\mathcal{X}^{\ell+2}}{\ell} + \cdots\right)$$

$$= \sum_{i=0}^{\infty} \frac{\zeta_i\mathcal{X}^{3+i}}{i+1}$$

By taking Laplace transform to both sides, we get

$$\mathcal{L}H(x) = \mathcal{L}\left(\zeta_0\,\mathcal{X}^3 + \frac{\zeta_1\mathcal{X}^4}{2} + \frac{\zeta_2\mathcal{X}^5}{3} + \frac{\zeta_3\mathcal{X}^6}{4} + \cdots + \frac{\zeta_{\ell-1}\mathcal{X}^{\ell+2}}{\ell}\right) \qquad (3)$$

$$\mathcal{L}H(x) = \frac{\zeta_0 3!}{p^4} + \frac{\zeta_1 4!}{2p^5} + \frac{\zeta_2 5!}{3p^6} + \frac{\zeta_3 6!}{4p^7} + \cdots \frac{\zeta_{\ell-1}(\ell+2)!}{\ell p^{\ell+3}}$$

Now let $\phi_i = \frac{\zeta_i(i+3)!}{i+1}$ $.i = 0.1.2.\ldots\ell - 1$

$$\mathcal{L}H(x) = \frac{\phi_0}{p^4} + \frac{\phi_1}{p^5} + \frac{\phi_2}{p^6} + \frac{\phi_3}{p^7} + \cdots \frac{\phi_{\ell-1}}{p^{\ell+3}}$$

Choosing invertible key, k ={0,….,25} ,such that gcd (26,k)=1

Now multiply k_i by $\phi_i \,.i = 0.1.2. \ldots \ell - 1$

$$\mathcal{L}\, k\, H(x) = \frac{k_0\phi_0}{p^4} + \frac{k_1\phi_1}{p^5} + \frac{k_2\phi_2}{p^6} + \frac{k_3\phi_3}{p^7} + \cdots \frac{k_{\ell-1}\phi_{\ell-1}}{p^{\ell+3}}$$

For simplicity, assume that $S_i = k_i * \phi_i \,.i = 0.1.2. \ldots \ell - 1$

$$\mathcal{L}\, k\, H(x) = \frac{S_0}{p^4} + \frac{S_1}{p^5} + \frac{S_2}{p^6} + \frac{S_3}{p^7} + \cdots \frac{S_{\ell-1}}{p^{\ell+3}}$$

Remark 3.1: The given plain text in terms of $\zeta_i.i = 0.1.2. \ldots \ell - 1$ under Laplace transform to the Taylor series of the function $H(x)$, (that is by writing them as coefficients of (3), and then taking the Laplace transform), and using invertible key k_i can be converted to cypher text in terms of $\psi_i \,.i = 0.1.2. \ldots \ell - 1$ such that

$$S_i = \psi_i \, mod\, 26 \text{ or } \psi_i = S_i - 26k_i \qquad .i = 0.1.2. \ldots \ell - 1$$

3.2 *Decryption*

We have received the massage as a cypher text in terms of $\psi_i.i = 0.1.2. \ldots . \ell - 1$ which is equivalent to $S_i \,.i = 0.1.2. \ldots . \ell - 1$ such that

$$S_i = \psi_i + 26k_i \tag{4}$$

Where $\mathcal{L}\, k\, H(x) = \frac{S_0}{p^4} + \frac{S_1}{p^5} + \frac{S_2}{p^6} + \frac{S_3}{p^7} + \cdots \frac{S_{\ell-1}}{p^{\ell+3}}$

By multiply k_i^{-1} by $S_i \,.i = 0.1.2. \ldots . \ell - 1$, we have

$$\mathcal{L}\, k\, k^{-1}\, H(x) = \frac{k_0^{-1}S_0}{p^4} + \frac{k_1^{-1}S_1}{p^5} + \frac{k_2^{-1}S_2}{p^6} + \frac{k_3^{-1}S_3}{p^7} + \cdots \frac{k_{\ell-1}^{-1}S_{\ell-1}}{p^{\ell+3}}$$

$$\mathcal{L}H(x) = \frac{\phi_0}{p^4} + \frac{\phi_1}{p^5} + \frac{\phi_2}{p^6} + \frac{\phi_3}{p^7} + \cdots \frac{\phi_{\ell-1}}{p^{\ell+3}}$$

By taking the inverse of Laplace transform to both sides, we have

$$\mathcal{L}^{-1}\mathcal{L}\, H(x) = \mathcal{L}^{-1}[\frac{\phi_0}{p^4} + \frac{\phi_1}{p^5} + \frac{\phi_2}{p^6} + \frac{\phi_3}{p^7} + \cdots \frac{\phi_{\ell-1}}{p^{\ell+3}}]$$

$$H(x) = \left(\begin{array}{c} \phi_0\, 3!\, X^3 + \phi_1 4!\, X^4 + \phi_2 5!\, X^5 + \phi_3 6!\, X^6 \\ + \cdots + \phi_{\ell-1}(\ell+2)!\, X^{\ell+2} \end{array} \right)$$

We can have the values of plain text by using the formula.

$$\zeta_i = \frac{\phi_i(i+1)}{(i+3)!}. \qquad i = 0.1.2. \ldots \ell - 1$$

Remark 3.2: The provided text phrase of the cypher $\psi_i.i = 0.1.2. \ldots . \ell - 1$, with given key $k_i \,.i = 0.1.2. \ldots \ell - 1$. It can be converted to plain text $\zeta_i.i = 0.1.2. \ldots . \ell - 1.$ under the inverse of Laplace transform of (3) such that $\zeta_i = \frac{\phi_i(i+1)}{(i+3)!}$, $i = 0.1.2. \ldots . \ell - 1$

Where $\psi_i = S_i - 26k_i.$ $i = 0.1.2. \ldots . \ell - 1$

Example 4.1: let us have the massage called the plain text "Roaa Razak" find the inscription and decryption of the previous message

*Encryption***:** The plain text "Roaa Razak" is equivalent to:17 14 0 0 17 0 25 0 10

Where $\ell = 9$ the length of the massage. Now, Assume that

$\zeta_0 = 17.$ $\zeta_1 = 14.$ $\zeta_2 = 0.$ $\zeta_3 = 0.$ $\zeta_4 = 17.$

$\zeta_5 = 0.$ $\zeta_6 = 25.$ $\zeta_7 = 0.$ $\zeta_8 = 10.$ $\zeta_n = 0. n \geqslant 9$

Making use of those numbers as coefficients of $-\mathcal{X}^2 \ln(1-\mathcal{X})$ and assuming

$H(x) = -\zeta \mathcal{X}^2 \ln(1-\mathcal{X})$, we get

$$H(x) = -\zeta \mathcal{X}^2 \ln(1-\mathcal{X}) = \left(\zeta_0 \mathcal{X}^3 + \frac{\zeta_1 \mathcal{X}^4}{2} + \frac{\zeta_2 \mathcal{X}^5}{3} + \frac{\zeta_3 \mathcal{X}^6}{4} + \cdots + \frac{\zeta_8 \mathcal{X}^{11}}{9}\right)$$

$$H(x) = -\zeta \mathcal{X}^2 \ln(1-\mathcal{X}) = \left(17\, \mathcal{X}^3 + \frac{14\mathcal{X}^4}{2} + \frac{\mathcal{X}^7}{5} + \frac{25\mathcal{X}^9}{7} + \frac{10\mathcal{X}^{11}}{9}\right)$$

Laplace transform applied to both sides yields

$$\mathcal{L}\{f(t)\} = \mathcal{F}(p)$$

$$\mathcal{F}(p) = \mathcal{L}\, H(x) = 17\, \frac{3!}{p^4} + 14 \frac{4!}{2p^5} + 17 \frac{7!}{5p^8} + 25 \frac{9!}{7p^{10}} + 10 \frac{11!}{9p^{12}}$$

$$\mathcal{F}(p) = \mathcal{L}\, H(x) = \frac{102}{p^4} + \frac{168}{p^5} + \frac{17136}{p^8} + \frac{1296000}{p^{10}} + \frac{44352000}{p^{12}}$$

Adjusting the resultant values

$\phi_0 = 102.$ $\phi_1 = 168$ $\phi_2 = 0$ $\phi_3 = 0$ $\phi_4 = 17136$ $\phi_5 = 0$ $\phi_6 = 1296000$ $\phi_7 = 0$ $\phi_8 = 44352000$

Now choosing inventible key {3,5,7,11,13,17,19,23}, we find

$S_i = k_i * \phi_i \,. i = 0.1.2. \ldots \ell - 1$

$S_0 = 3 * 102 = 306.$ $S_1 = 5 * 168 = 840$ $S_2 = 7 * 0 = 0.$ $S_3 = 11 * 0 = 0$

$S_4 = 13 * 17136 = 222768.$ $S_5 = 17 * 0 = 0.$ $S_6 = 19 * 1296000 = 2451000.$ $S_7 = 23 * 0 = 0.$ $S_8 = 2 * 44352000 = 88704000$

mod 26 is

$306 = 20\ mod\ 26$ $840 = 8\ mod\ 26$ $0 = 0\ mod 26$ $0 = 0\ mod\ 26$

$222768 = 0\ mod\ 26$ $0 = 0\ mod\ 26$ $2451000 = 6\ mod 26$ $0 = 0 mod 26$ $88704000 = 8\ mod\ 26$

Now let

$\psi_0 = 20.$ $\psi_1 = 8.$ $\psi_2 = 0.$ $\psi_3 = 0.$ $\psi_4 = 0.$ $\psi_5 = 0.$ $\psi_6 = 6.$ $\psi_7 = 0.$ $\psi_8 = 8$

Then the cypher text 20 8 0 0 0 0 6 0 8

the plain text 'Roaa Razak' gets converted to 'Uiaa Aagai'.

decryption: if we have the cypher text 'Uiaa Aagai' is equivalent to

$$20 \quad 8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 6 \quad 0 \quad 8$$

Suppose that

$$\psi_0 = 20.\ \ \psi_1 = 8.\ \psi_2 = 0.\ \ \psi_3 = 0.\ \ \psi_4 = 0.$$
$$\psi_5 = 0.\ \ \psi_6 = 6.\ \ \psi_7 = 0.\ \psi_8 = 8$$

Using (4) and assuming $S_i = \psi_i + 26k_i$, and the values of $k_i . i = 0.1.2. \ldots 8$

$$11 \quad 32 \quad 0 \quad 0 \quad 8568 \quad 0 \quad 94269 \quad 0 \quad 3411692$$

We have $\mathcal{F}(p) = \mathcal{L}\, k\, H(x) = \frac{306}{p^4} + \frac{840}{p^5} + \frac{222768}{p^8} + \frac{2451000}{p^{10}} + \frac{88704000}{p^{12}}$

By multiply k_i^{-1} by $S_i\ .i = 0.1.2. \ldots . \ell - 1$, we have

$$\mathcal{F}(p) = \left(\frac{102}{p^4} + \frac{168}{p^5} + \frac{17136}{p^8} + \frac{1296000}{p^{10}} + \frac{44352000}{p^{12}}\right)$$

By taking Laplace inverse to both sides, we get

$$\mathcal{L}^{-1}\mathcal{F}(p) = \mathcal{L}^{-1}\left(\frac{102}{p^4} + \frac{168}{p^5} + \frac{17136}{p^8} + \frac{1296000}{p^{10}} + \frac{44352000}{p^{12}}\right)$$

$$\mathfrak{f}(\mathcal{X}) = \begin{pmatrix}(3!)102\,\mathcal{X}^3 + (4!)168\,\mathcal{X}^4 + (7!)17136\,\mathcal{X}^7 \\ +(9!)1296000\mathcal{X}^9 + (11!)44352000\mathcal{X}^{11}\end{pmatrix}$$

We can find the values of plain text by using the following formula

$$\zeta_i = \frac{\phi_i(i+1)}{(i+3)!} . i = 0.1.2. \ldots . 8$$

$$\zeta_0 = 17. \quad \zeta_1 = 14. \quad \zeta_2 = 0. \quad \zeta_3 = 0. \quad \zeta_4 = 17.$$
$$\zeta_5 = 0. \quad \zeta_6 = 25. \quad \zeta_7 = 0. \quad \zeta_8 = 10. \quad \zeta_n = 0. n \geqslant 9$$

Here 17 14 0 0 17 0 25 0 10 is equivalent to 'Roaa Razak'

4. Algorithm

Encryption :

1- Convert the plain text to a decimal number.
2- Embedding the decimal number as a coefficient of the Taylor series.
3- Taking Laplace transformation to both sides of Taylor series.
4- The embedding coefficient of Laplace is $\phi_i = \frac{\zeta_i(i+3)!}{i+1}\ .i = 0.1.2. \ldots \ell - 1$
5- Choosing an invertible key that belongs to {0…25}, such that gcd (26,k)=1.
6- Multiply k_i by $\phi_i\ .i = 0.1.2. \ldots \ell - 1$, to obtained S_i .
7- Use the relation $\psi_i = S_i - 26k_i$, $i = 0.1.2. \ldots \ell - 1$, to obtain the cipher text.

Decryption:

1- Using the relation $S_i = \psi_i + 26k_i$, to obtained S_i , from the cypher text.
2- Multiply $k_i^{-1}{}_i$ by $S_i\ .i = 0.1.2. \ldots \ell - 1$, to obtained ϕ_i.

3- taking the inverse of Laplace transform to both sides of the Taylor series

4- Use the relation $\zeta_i = \frac{\phi_i(i+1)}{(i+3)!}.\ i = 0.1.2. \ldots \ell - 1$, to obtain the plain text.

5. Discussion and Conclusion

We have introduced a novel cryptographic scheme that utilizes Laplace transforms, with an invertible key that belongs to the set {0…25}, satisfying the condition gcd(26, k) = 1. Our method significantly increases an attacker's difficulty in tracing the key through any form of attack. The Taylor series of logarithmic functions are employed in this approach. Through various assault scenarios on the secret message, the results demonstrate the robust security provided by our proposed method and the challenge it poses in attempting to guess the key. Furthermore, exploring the Laplace transform of the inverse of trigonometric and hyperbolic functions enables us to obtain additional novel results.

References

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

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

[3] A. P. Hiwarekar, "A new Method of Cryptography using Laplace Transform of Hyperbolic Functions", *International Journal of Mathematical Archive*-4(2), pp.208-213 (2013).

[4] M.Tuncay Gençoğlu, "Cryptanalysis A Cryptographic Scheme of Laplace Transforms", Conference: ICPAM 2017.

[5] Jadhav Shaila Shivaji and Hiwarekar A.P, "New Method for Cryptography using Laplace-Elzaki Transform", Psychology and Education, 58(5), pp. 1-6 (2021).

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

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

[8] Shubham Sharma & Ahmed J. Obaid. Mathematical modelling, analysis and design of fuzzy logic controller for the control of ventilation systems using MATLAB fuzzy logic toolbox, *Journal of Interdisciplinary Mathematics,* 23:4, 843-849 (2020), DOI: 10.1080/09720502.2020.1727611.

Received October 2022