"Science Stays True Here"
Journal of Mathematics and Statistical Science (ISSN 2411-2518), Vol.5, 302-307 | Science Signpost Publishing

# On the Application of Nonhomogeneous Differential Equations to a Laplace Transform-based Cryptographic Process

Roberto P. Briones
*School of Mathematical and Computer Sciences, Heriot-Watt University Malaysia, 62200, Putrajaya, Malaysia*

## Abstract

Hiwarekar [4] introduced a cryptographic scheme which made use of the Laplace transform of the Taylor series of a $C^{\infty}$ function $t^n f(kt)$, in the most general sense. However, the functional form more commonly used in literature is $t^n e^{kt}$ mainly due to computational convenience. To transmit an encoded message, the parameters *n, k,* and *f(t)* are specified in advance and sent securely. This paper extends the encoding to functions of the form $P(t)e^{kt}$, where *P(t)* is an nth degree polynomial with positive integral coefficients, and recognizes the role this function takes as a unique solution to a nonhomogeneous differential equation. Consequently, the representation of all the parameters through a single differential equation and the additional complexity it brings strengthens the security of the ciphertext.

*Keywords: Taylor series, non-homogeneous differential equation, particular solution, plaintext, ciphertext*

## Introduction

A new encryption algorithm has been forwarded based on imbedding the numerical codes of plaintext into the coefficients of the Laplace transform of the Taylor series of a function. Hiwarekar [4] first showed this in 2012, under the assumption that a plaintext of length *n* will also make use of the coefficients of the first *n* terms of the infinite series. Gupta and Mishra [2] showed that for a single-iteration of the algorithm, the use of modular arithmetic and elimination of invalid cryptic possibilities can decode the ciphertext. To address this issue, Briones [1] altered the formulation of the encryption process by using the coefficients of *n randomly* selected terms from the infinite series for the plaintext of length *n*. Consequently, this gave rise to a two-password system, and made the security of the coded message stronger.

In this paper I give a variation of the Hiwarekar scheme by generalizing the more commonly-used function $t^n e^{kt}$ into $P(t)e^{kt}$, where *P(t)* is a polynomial of degree *n* with positive integral coefficients, and recognizing the latter as the unique *particular* solution to a nonhomogeneous differential equation. The codification will entail specifying a nonhomogeneous differential equation to which $P(t)e^{kt}$ is a particular solution, and this in turn will become the basis for the Taylor series from whose coefficients will give rise the encrypted message. As a result, the differential equation itself becomes a vital part of the cryptographic process.

## The extension to $\boldsymbol{P(t)e^{kt}}$

In Hiwarekar (2012), as well as in other literature in treatment, the series from which the coefficients were taken was based on the product of the monomial $t^n$ and the Taylor expansion of $e^{kt}$. In this paper the monomial $t^n$ is replaced by the general polynomial *P(t)* of degree n. To be able to do this, it has to be shown that the Laplace transform of the resulting Taylor expansion of $P(t)e^{kt}$ will yield positive integral coefficients.

**Theorem.** Let *a* and *c* be positive integers, and assume *c* > *a*. Then the Laplace transform of the Taylor expansion of $(t^c + t^a)e^{kt}$ will result in a series of terms with positive integral coefficients.

**Proof.** It is enough to show that the coefficients of the Laplace transform of $(t^c + t^a)e^{kt}$ will yield positive integral coefficients.

Thus,

$$(t^c + t^a)e^{kt}$$

$$= t^c e^{kt} + t^a e^{kt}$$

$$= \sum_0^\infty \frac{k^n}{n!} t^{n+c} + \sum_0^\infty \frac{k^n}{n!} t^{n+a}$$

$$= \sum_{c-a}^\infty \frac{k^{n-c+a}}{(n-c+a)!} t^{n+a} + \sum_0^\infty \frac{k^n}{n!} t^{n+a}$$

$$= \sum_0^{c-a-1} \frac{k^n}{n!} t^{n+a} + \sum_{c-a}^\infty \frac{k^{n-c+a}}{(n-c+a)!} t^{n+a} + \sum_{c-a}^\infty \frac{k^n}{n!} t^{n+a}$$

$$= \sum_0^{c-a-1} \frac{k^n}{n!} t^{n+a} + \sum_{c-a}^\infty \left( \frac{k^{n-c+a} t^{n+a}}{(n-c+a)!} + \frac{k^n t^{n+a}}{n!} \right)$$

$$= \sum_0^{c-a-1} \frac{k^n}{n!} t^{n+a} + \sum_{c-a}^\infty \left( 1 + \frac{k^{c-a}}{P_{c-a}^n} \right) \frac{k^{n-c+a} t^{n+a}}{(n-c+a)!}$$

$$= \sum_0^{c-a-1} \frac{k^n}{n!} t^{n+a} + \sum_{c-a}^\infty \frac{(P_{c-a}^n + k^{c-a})}{P_{c-a}^n} \cdot \frac{k^{n-c+a} t^{n+a}}{(n-c+a)!}$$

Taking the Laplace transform of this infinite series, we get

$$L\left\{ \sum_0^{c-a-1} \frac{k^n}{n!} t^{n+a} + \sum_{c-a}^{\infty} \frac{(P_{c-a}^n + k^{c-a})}{P_{c-a}^n} \cdot \frac{k^{n-c+a} t^{n+a}}{(n-c+a)!} \right\}$$

$$= \sum_0^{c-a-1} \frac{k^n}{n!} \cdot \frac{(n+a)!}{s^{n+a+1}} + \sum_{c-a}^\infty \frac{(P_{c-a}^n + k^{c-a})}{P_{c-a}^n} \cdot \frac{k^{n-c+a}}{(n-c+a)!} \cdot \frac{(n+a)!}{s^{n+a+1}}$$

$$= \sum_0^{c-a-1} \frac{P_a^{n+a} k^n}{s^{n+a+1}} + \sum_{c-a}^\infty \frac{(P_{c-a}^n + k^{c-a})}{P_{c-a}^n} \cdot \frac{P_c^{n+a} k^{n-c+a}}{s^{n+a+1}}$$

$$= \quad \sum_0^{c-a-1} \frac{P_a^{n+a} k^n}{s^{n+a+1}} + \sum_{c-a}^{\infty} (P_{c-a}^n + k^{c-a}) \cdot \frac{P_a^{n+a} k^{n-c+a}}{s^{n+a+1}}.$$

Observing that the coefficients of both series (the first finite, the second infinite) are all positive integers, this concludes the proof. ■

This enables us to codify the message by first passing through the solution of a nonhomogeneous differential equation. The Laplace transform of the Taylor series of the solution function $P(t)e^{kt}$ , whose randomly chosen coefficients are to be multiplied with the numerical codes of the letters of the message, will complete the encryption process.

The formulation hinges on the solution of a differential equation to determine the function $P(t)e^{kt}$ that will be used in encoding the message. Here $P(t)$ is a polynomial function with positive integral coefficients, and *k* is a positive integer. We give a demonstration of the procedure as follows.

## An encoding example

Encode the word SECRET using this modified cryptographic scheme.

**Step 1.** The corresponding numerical codes for the letters in the words are 18, 4, 2, 17, 4, 19. The plaintext vector is thus $\vec{P} = \langle 18, 4, 2, 17, 4, 19 \rangle$

**Step 2.** Now consider the nonhomogeneous differential equation $y'' - 3y' + 2y = (2t + 5)e^{3t}$, where $y = y(t)$. By using the method of undetermined coefficients, the *unique* particular solution is found to be $y_p(t) = (t + 1)e^{3t}$ [5]. We then encode our message using the Laplace transform of the Taylor expansion of $y_p(t) = (t + 1)e^{3t}$.

**Step 3.** $(t + 1)e^{3t}$

$$= \quad \sum_0^{\infty} \frac{3^n}{n!} t^{n+1} + \sum_0^{\infty} \frac{3^n}{n!} t^n$$

$$= \quad 1 + \sum_0^{\infty} \frac{3^n}{n!} t^{n+1} + \sum_1^{\infty} \frac{3^n}{n!} t^n$$

$$= \quad 1 + \sum_1^{\infty} \frac{3^{n-1}}{(n-1)!} t^n + \sum_1^{\infty} \frac{3^n}{n!} t^n$$

$$= \quad 1 + \sum_1^{\infty} \left(1 + \frac{3}{n}\right) \frac{3^{n-1}}{(n-1)!} t^n$$

$$= \quad 1 + \sum_1^{\infty} \left(\frac{n+3}{n}\right) \frac{3^{n-1} t^n}{(n-1)!}$$

This implies that

$$L\{(t+1)e^{3t}\} = L\left\{1 + \sum_1^{\infty} \left(\frac{n+3}{n}\right) \frac{3^{n-1} t^n}{(n-1)!}\right\} = \frac{1}{s} + \sum_1^{\infty} \frac{n+3}{n} \cdot \frac{3^{n-1}}{(n-1)!} \cdot \frac{n!}{s^{n+1}} = \frac{1}{s} + \sum_1^{\infty} \frac{(n+3)3^{n-1}}{s^{n+1}}.$$

(Note that the corresponding coefficients for the indexes (subscripts) *n* = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, etc., are 1, 4, 15, 54, 189, 648, 2187, 7290, 24057, 78732, etc.)

**Step 4.**

Now *randomly* choose six indexes from the infinite series of Laplace transforms from the preceding step. Select, for example, the indexes n = 2, 5, 9, 10, 13, and 17, and the corresponding coefficients, namely

15, 648, 78732, 255879, 8503056, and 860934420.

Multiply these with the numerical codes 18, 4, 2, 17, 4, 19 for the word SECRET. Thus, we get the numbers 270, 2592, 157464, 4349943, 34012224, and 16357753980.

Using modular arithmetic,

$$270 \equiv 26 \cdot 10 + 10$$
$$2592 \equiv 26 \cdot 99 + 18$$
$$157464 \equiv 26 \cdot 6056 + 8$$
$$4349943 \equiv 26 \cdot 167305 + 13$$
$$34012224 \equiv 26 \cdot 1308162 + 12$$
$$16357753980 \equiv 26 \cdot 629144383 + 22.$$

The residues 10, 18, 8, 13, 12, and 22 form the ciphertext vector $\vec{C} = \langle 10, 18, 8, 13, 12, 22 \rangle$, and represents the coded message KSINMW, the ciphertext for SECRET.

**Step 5.**

This is the transmission step. The sender transmits the following data to the receiver through a valid secure channel the following transmission:

i. The differential expression $y'' - 3y' + 2y$, and
ii. The ciphertext KSINMW

In a separate secure transmission, for the purpose of decryption, the sender transmits the following to the receiver.

i. The key function $(2t + 5)e^{3t}$ (the nonhomogeneous term of the DE)
ii. The index key $\vec{G} = \langle 2, 5, 9, 10, 13, 17 \rangle$, and
iii. The quotient key $\vec{Q} = \langle 10, 99, 6056, 167305, 1308162, 629144383 \rangle$.

## A decoding example

The ciphertext YAQCCOAASIE and the differential expression $(D - 1)^2 y = y'' - 2y' + y$ were received. In a prior communication the key function $2e^t$ was received, along with the index key $\vec{G} = \langle 0, 1, 3, 4, 7, 8, 10, 12, 15, 19, 22 \rangle$, and the quotient key

$$\vec{Q} = \langle 0, 0, 14, 8, 11, 41, 0, 133, 83, 32, 382 \rangle.$$

Now the differential equation $(D - 1)^2 y = y'' - 2y' + y = 2e^t$ will have the *unique* particular solution $t^2 e^t$, [5] by direct use of the method of undetermined coefficients. Then

$$L\{t^2e^t\} = L\left\{\sum_{n=0}^{\infty}\frac{t^{n+2}}{n!}\right\} = \sum_{n=0}^{\infty}\frac{L(t^{n+2})}{n!} = \sum_{n=0}^{\infty}\frac{(n+2)!}{n!}\cdot\frac{1}{s^{n+3}} = \sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{s^{n+3}}$$

Hence, the index $n$ gives rise to the coefficient defined by $(n+1)(n+2)$, and direct substitution of the entries of the index key $\vec{G} = \langle 0, 1, 3, 4, 7, 8, 10, 12, 15, 19, 22\rangle$ give the sequence of numbers

*2, 6, 20, 30, 72, 90, 132, 182, 272, 420, 552* .

The ciphertext YAQCCOAASIE is represented by the vector $\vec{C} = \langle 24, 0, 16, 2, 2, 14, 0, 0, 18, 8, 4\ \rangle$. The information from the quotient key $\vec{Q}$ and the ciphertext $\vec{C}$ yield the following values:

$$0 * 26\ +\ 24\ =\ 24 \Longrightarrow 2P_1 = 24 \Longrightarrow P_1 = 12$$

$$0 * 26\ +\ 0\ =\ 0\ \Longrightarrow 6P_2 = 0 \Longrightarrow P_2 = 0$$

$$14 * 26\ +\ 16 =\ 380 \Longrightarrow 20P_3 = 380\ \Longrightarrow P_3 = 19$$

$$8 * 26\ +\ 2\ =\ 210\ \Longrightarrow 30P_4 = 210 \Longrightarrow P_4 = 7$$

$$11 * 26\ +\ 2\ =\ 288\ \Longrightarrow 72P_5 = 288 \Longrightarrow P_5 = 4$$

$$41 * 26\ +\ 14\ =\ 1080\ \Longrightarrow 90P_6 = 1080\ \Longrightarrow P_6 = 12$$

$$0 * 26\ +\ 0\ =\ 0\ \Longrightarrow 132P_7 = 0\ \Longrightarrow P_7 = 0$$

$$133 * 26\ +\ 0\ =\ 3458\ \Longrightarrow 182P_8 = 3458 \Longrightarrow P_8 = 19$$

$$83 * 26\ +\ 18\ =\ 2176\ \Longrightarrow 272P_9 = 2176 \Longrightarrow P_9 = 8$$

$$32 * 26\ +\ 8\ =\ 840\ \Longrightarrow 420P_{10} = 840 \Longrightarrow P_{10} = 2$$

$$382 * 26\ +\ 4\ =\ 9936\ \Longrightarrow 552P_{11} = 9936\ \Longrightarrow P_{11} = 18$$

The plaintext vector is thus $\vec{P} = \langle 12, 0, 19, 7, 4, 12, 0, 19, 8, 2, 18\rangle$, which corresponds to the original plaintext MATHEMATICS.

## Conclusion

The original Hiwarekar cryptographic scheme makes use of the Laplace transform of the Maclaurin series of the function $t^n f(kt)$. In that cryptographic process [3, 4], the parameters $n$, $k$, and the function $f(t)$ itself would have to be specified by the sender in advance, and communicated to the receiver through supposedly secure medium. In this paper, nonhomogeneous differential equations are introduced in the early stage of the cryptographic process. The presence of the parameters $n$, $k$, and $f(t)$ are compactly ensured in the use of a single nonhomogeneous differential equation. In addition, the replacement of $t^n$ by $P(t)$ gives more complexity in the calculation of the coefficients that are to be used in the infinite series of Laplace transforms, and thus combined with the two-password system, adds strength to the security of the encoded message.

# References


[1] Briones, R.P. (2018). Modification of an Encryption Scheme Based on the Laplace Transform. International Journal of Current Research, vol. 10, no.7, pp. 71759 – 71763.

[2] Gupta, P., Mishra, P.R. (2014). Cryptanalysis of "A New Method of Cryptography Using Laplace Transform". In: Pant, M., Deep, K., Nagar, A., Bansal, J., (eds) Proceedings of the Third International Conference on Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing **258**, 539 – 546. Springer, New Delhi.

[3] Hiwarekar, A.P. (2015). Application of Laplace Transform for Cryptography. International Journal of Engineering & Science Research **5** (4), 129 – 135.

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

[5] Nagle, R. Kent, Saff, E.B., Snider, A.D. (2018). Fundamentals of Differential Equation. Ninth edition. Pearson, Boston, pp.174 – 180.