Utilizing Dinesh Verma Transformation (DVT) and Differential Equations in a Cryptography Model

Dr. Noor Kadhim Meftin
Computer Science and Information System Department, Al-Mansour University College, Iraq.
E-mail: noor.kadhim@muc.edu.iq

Received September 16, 2021; Accepted December 15, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19210

Abstract

The ever-expanding area of cryptography fostered the development of numerous cryptographic models utilizing a variety of mathematical and logical methodologies, and integral transformations were no exception. This paper proposes a cryptographic model based on the application of the Dinesh Verma integral Transformation (DVT) to the series produced by the production of a general polynomial P(t) of degree n with the Taylor series to increase the complexity of the resulting ciphertext, and in which key elements required for encryption and decryption are transmitted over channels of various security measurements to complicate the attacker's work in gathering the required information.

Keywords

Dinesh Verma integral Transformation (DVT), Nonhomogeneous Differential Equation, Cryptography, Taylor Series, Polynomials.

Introduction

The high applicability of integral transforms in solving numerous problems in different scientific fields (Verma 2020) (Rahul Gupta 2020) raised the cryptography scientists' interest in utilizing them in the highly growing field of cryptography.

Many integral transforms have been deployed in the cryptography field. The methods of cryptography that depend on using integral transforms, encoding the plaintext letters into some form of coefficients, that could be the numeric equivalent of the letters in their alphabet or their ASCII code or any other encoding scheme, then use them to create some form of a finite series (Briones 2019)(Rohit Gupta 2020). However, Roberto P. Briones in (M T Gençoğlu 2016) suggested using the positive integer coefficients generated from the plaintext letters into the polynomial of degree n in the function $P(t)e^{kt}$. This suggestion seized the opportunity of using the nonhomogeneous differential equation, where the

plaintext letters coefficients acted as the unique solution to this nonhomogeneous differential equation (M Tuncay Gençoğlu 2017).

This work proposed a new cryptographical model that utilized Dinesh Verma Transformation (DVT) with the particular solution of the nonhomogeneous differential equation function (Jadhav Shaila Shivaji 2021). The applicability of the suggested model has been tested via an example that discussed the encryption of actual plaintext then decrypting the resulting ciphertext back into its originated message (Kuffi et al. 2020).

Dinesh Verma Transformation (DVT) [1]

In 2020, Dinesh Verma produced a transformation under his name called the "Dinesh Verma Transform," DVT for shortening.

For the function $f(x)$ of real number $t \geq 0$, the DVT for $f(t)$ denoted by the operator D is defined as: $D\{f(x)\} = v^5 \int_{x=0}^{\infty} e^{-vx} f(x)dx = F(v)$.

Where, v could be real or complex parameter, and the integral is convergent.

DVT and Inverse DVT of t^n (M Tuncay Gençoğlu 2017)

1. $D\{t^n\} = \frac{n!}{v^{n-4}}$, n is a positive integer number,

if n=0, then $D\{1\} = v^4$.

2. $D^{-1}\left\{\frac{1}{v^{n-4}}\right\} = \frac{t^n}{n!}$.

Applying DVT on Taylor Series $(t^a + t^b)e^{kt}$

If a and b are positive integer numbers, and $b > a$, then DVT of Taylor series $(t^a + t^b)e^{kt}$would be causing terms expansion with coefficients of positive numbers.

Proof:

As a prove to this theorem, it is sufficient to prove the coefficients of $D\{(t^a + t^b)e^{kt}\}$ are positive integers, thus for:

$(t^a + t^b)e^{kt} = t^b e^{kt} + t^a e^{kt}$,
$= \sum_{n=0}^{\infty} \frac{k^n t^{n+b}}{n!} + \sum_{n=0}^{\infty} \frac{k^n t^{n+a}}{n!}$,

$= \sum_{n=b-a}^{\infty} \frac{k^{n-b+a}}{(n-b+a)!} t^{n+a} + \sum_{n=0}^{\infty} \frac{k^n t^{n+a}}{n!}$,

$= \sum_{n=0}^{b-a-1} \frac{k^n t^{n+a}}{n!} + \sum_{n=b-a}^{\infty} \left(\frac{k^{n-b+a} t^{n+a}}{(n-b+a)!} + \frac{k^n t^{n+a}}{n!} \right)$,

$= \sum_{n=0}^{b-a-1} \frac{k^n t^{n+a}}{n!} + \sum_{n=b-a}^{\infty} \left[1 + \frac{k^{b-a}}{P_{b-a}^n} \right] \frac{k^{n-b+a} t^{n+a}}{(n-b+a)!}$,

$= \sum_{n=0}^{b-a-1} \frac{k^n t^{n+a}}{n!} + \sum_{n=b-a}^{\infty} \frac{(P_{b-a}^n + k^{b-a})}{P_{b-a}^n} . \frac{k^{n-b+a} t^{n+a}}{(n-b+a)!}$, taking DVT to this infinite expression gives:

$D \left\{ \sum_{n=0}^{b-a-1} \frac{k^n t^{n+a}}{n!} + \sum_{n=b-a}^{\infty} \frac{(P_{b-a}^n + k^{b-a})}{P_{b-a}^n} . \frac{k^{n-b+a} t^{n+a}}{(n-b+a)!} \right\} = \sum_{n=0}^{b-a-1} \frac{k^n}{n!} . \frac{(n+a)!}{v^{n+a-4}} +$

$\sum_{n=b-a}^{\infty} \frac{(P_{b-a}^n + k^{b-a})}{P_{b-a}^n} . \frac{k^{n-b+a} (n+a)!}{(n-b+a)! v^{n+a-4}}$,

$= \sum_{n=0}^{b-a-1} \frac{P_a^{n+a} k^n}{v^{n+a-4}} + \sum_{n=b-a}^{\infty} \frac{(P_{b-a}^n + k^{b-a})}{P_{b-a}^n} . \frac{k^{n-b+a} P_a^{n+a}}{v^{n+a-4}}$,

$= \sum_{n=0}^{b-a-1} \frac{P_a^{n+a} k^n}{v^{n+a-4}} + \sum_{n=b-a}^{\infty} (P_{b-a}^n + k^{b-a}) \frac{k^{n-b+a} P_a^{n+a}}{v^{n+a-4}}$.

By observing the resulting two finite series, the coefficients are all positive integers, which concludes the proof.

The Algorithm of the Proposed Cryptography Model

To enhance the clarity and comprehension of the proposed cryptography model, each procedural step of the encryption and decryption algorithms will be accompanied by a practical example (Kuffi11, Abbas, and Maktoof n.d.).

Encryption Algorithm

The plaintext that required to be encrypted at the sender side is "SECRET."

The encryption steps would be as follows:

a. The encryption algorithm starts with coding the plaintext letters into their numeric equivalent in the alphabet.

The numeric equivalent in the alphabet to the plaintext “SECRET” letters are: 18, 4, 2, 17, 4, 19. And a plaintext vector could be written as: $\vec{P} = \langle 18, 4, 2, 17, 4, 19 \rangle$.

b. For the nonhomogeneous differential equation: $y''(\mathrm{t}) - 3y'(\mathrm{t}) + 2y(t) = (2t + 5)e^{3t}$, it is possible to determine the particular solution to the nonhomogeneous part

of the differential equation from applying the undetermined coefficients method to be (Kumar and Vasuki 2018): $y_p\ (t) = (t\ +\ 1)e^{3t}$.

c. Taylor expansion of $y_p\ (t) = (t\ +\ 1)e^{3t}$ series could be found, as:

$$(t\ +\ 1)e^{3t} = \sum_0^\infty \frac{3^n}{n!}t^{n+1} + \sum_0^\infty \frac{3^n}{n!}t^n\ ,$$
$$= 1 + \sum_0^\infty \frac{3^n}{n!}t^{n+1} + \sum_1^\infty \frac{3^n}{n!}t^n\ ,$$
$$= 1 + \sum_1^\infty \frac{3^{n-1}}{(n-1)!}t^n + \sum_1^\infty \frac{3^n}{n!}t^n,$$
$$= 1 + \sum_1^\infty \left(1 + \frac{3}{n}\right)\frac{3^{n-1}}{(n-1)!}t^n\ ,$$
$$= 1 + \sum_1^\infty \left(\frac{n+3}{n}\right)\frac{3^{n-1}}{(n-1)!}t^n.$$

DVT is applied on the Taylor expansion of $y_p\ (t)$ as:

$$D\{(t\ +\ 1)e^{3t}\} = D\left\{1 + \sum_{n=1}^\infty \left(\frac{n+3}{n}\right)\frac{3^{n-1}}{(n-1)!}t^n\right\},$$
$$= D\{1\} + D\left\{\sum_{n=1}^\infty \left(\frac{n+3}{n}\right)\frac{3^{n-1}}{(n-1)!}t^n\right\},$$
$$= v^4 + \sum_{n=1}^\infty \frac{n+3}{n}\cdot\frac{3^{n-1}}{(n-1)!}\cdot\frac{n!}{v^{n-4}},$$
$$= v^4 + \sum_{n=1}^\infty \frac{(n+3)3^{n-1}}{v^{n-4}}.$$

An infinite series of coefficients has been produced from applying DVT on the Taylor expansion series that is corresponded to the indexes n=0,1,2,3,… as follows:

Index:	0	1	2	3	4	5	6	Etc.
Coefficient:	1	4	15	54	189	648	2187	

d. Due to the number of letters in the given plaintext (6 letters), six random indexes and their coefficients are chosen from the infinite series concluded in step (c).

Let the random indexes be: $\vec{G}_{\text{index}} = \langle 2, 5, 9, 10, 13, 17\rangle$ then, their corresponding coefficients are: $\vec{G}_{\text{coefficient}} = \langle 15, 648, 78732, 255879, 8503056, 860934420\rangle$.

The corresponding coefficients are multiplied by the numerical plaintext equivalents as:

$$\vec{G}_{\text{coefficient}} * \vec{P} = \langle 270, 2592, 157464, 4349943, 34012224, 16357753980\rangle = \vec{R}.$$

Modular arithmetic is used on the results from the multiplication operation as: $\vec{R} = 26(\vec{Q}) + \vec{C}$

$270 = 26\ (10) + 10,$
$2592 = 26(99) + 18,$
$157464 = 26(6056) + 8,$
$4349943 = 26(167305) + 13,$
$34012224 = 26(1308162) + 12,$
$16357753980 = 26(629144383) + 22.$

Where:

$\vec{Q}$ is the quotient key, $\vec{Q} = \langle 10, 99, 6056, 167305, 1308162, 629144383 \rangle$.
$\vec{C}$ is the numerical equivalents of the ciphertext letters, therefor, $\vec{C} = \langle 10, 18, 8, 13, 12, 22 \rangle$ is the ciphertext "KSINMW", to the plaintext "SECRET".

The proposed model assumes that there are two transmission channels (secured and unsecured), a specific information is sent via each channel.

- The ciphertext "KSINMW" and the differential expression $y''(\mathrm{t}) - 3y'(\mathrm{t}) + 2y(t)$ are transmitted over the unsecured channel.
- The key function $(2t\ +\ 5)e^{3t}$, the random indexes $\vec{G}_{\text{coefficient}}$ and the quotient key $\vec{Q}$ are transmitted over the secured channel. The information transmits via the unsecured channel is vital for the decryption purpose.

Decryption Algorithm

If the receiving end received the following information:

Through the unsecured channel, the ciphertext "KSINMW" and differential expression $y''(\mathrm{t}) - 3y'(\mathrm{t}) + 2y(t)$ have been received.

And through the secured channel, the key function $(2t\ +\ 5)e^{3t}$, the random indexes $\vec{G}_{\text{index}} = \langle 2, 5, 9, 10, 13, 17 \rangle$, and quotient key $\vec{Q} = \langle 10, 99, 6056, 167305, 1308162, 629144383 \rangle$ have been received.

The decryption algorithm would follow the following steps:

a. The usage of undetermined coefficients method (Sedeeg, Abdelrahim Mahgoub, and Saif Saeed 2016) would produce the unique particular solution $(t\ +\ 1)e^{3t}$ to the differential expression $y''(\mathrm{t}) - 3y'(\mathrm{t}) + 2y(t)$.

b. Applying DVT to $(t\ +\ 1)e^{3t}$ would give:

$$D\{(t\ +\ 1)e^{3t}\} = D\{1\} + D\left\{\sum_{n=1}^{\infty}\left(\frac{n+3}{n}\right)\frac{3^{n-1}}{(n-1)!}t^n\right\} = v^4 + \sum_{n=1}^{\infty}\frac{n+3}{n}\cdot\frac{3^{n-1}}{(n-1)!}\cdot\frac{n!}{v^{n-4}}$$
$$= v^4 + \sum_{n=1}^{\infty}\frac{(n+3)3^{n-1}}{v^{n-4}}$$

c. Substituting the index key sequence $\vec{G}_{\text{index}} = \langle 2, 5, 9, 10, 13, 17\rangle$ as (n)s' in the concluded sequence from step (c) is producing an infinite series of coefficients that correspond to the indexes $\vec{G}$ as follows:

$\vec{G}_{\text{index}}$:	2	5	9	10	13	17
$\vec{G}_{\text{coefficient}}$:	15	648	78732	255879	8503056	a860934420

d. It is possible to calculate the numerical equivalent of the plaintext letters $\vec{P}$ from using the numerical representation of the ciphertext "KSINMW" letters $\vec{C} = \langle 10, 18, 8, 13, 12, 22\rangle$ and the quotient key $\vec{Q}$ in the relation: $\vec{R} = 26(\vec{Q}) + \vec{C}$, where $\vec{R} = \vec{G}_{\text{coefficient}} * \vec{P}$ as follows:

$26\ (10) + 10 = 270 \Longrightarrow 15\mathrm{P}_1 = 270 \Longrightarrow P_1 = 18,$
$26(99) + 18 = 2592 \Longrightarrow 648\mathrm{P}_2 = 2592 \Longrightarrow P_2 = 4,$
$26(6056) + 8 = 157464 \Longrightarrow 78732\mathrm{P}_3 = 157464 \Longrightarrow P_3 = 2,$
$26(167305) + 13 = 4349943 \Longrightarrow 255879\mathrm{P}_4 = 4349943 \Longrightarrow P_4 = 17,$
$26(1308162) + 12 = 34012224 \Longrightarrow 8503056\mathrm{P}_5 = 34012224 \Longrightarrow P_5 = 4,$
$26(629144383) + 22 = 16357753980 \Longrightarrow 860934420\mathrm{P}_6 = 16357753980 \Longrightarrow P_6 = 19.$

The sequence that results from the decryption algorithm $\vec{P} = \langle 18, 4, 2, 17, 4, 19\rangle$ represents the numerical equivalent of the plaintext letters. Its alphabetic letter equivalent is the original plaintext transmitted by the sender, which is the word "SECRET".

Discussion and Conclusions

This work has suggested a straightforward cryptography model based on nonhomogeneous differential equations and the Dinesh Verma Transformation (DVT).

The proposed cryptographic model applies DVT to a nonhomogeneous differential equation of degree n general polynomial to increase the model complexity in its preliminary stages. A series of coefficients are produced from the application of DVT to the differential equation. Additional simple processing steps on the generated coefficients would deliver the final ciphertext that could be transmitted over an unsecured channel. The model uses separate channels (secured and unsecured) to transmit two sets of data. A secure channel is used to send the key function (the nonhomogeneous portion of the differential equation) and two other sequences (the index key and the quotient key). In contrast, the unsecured channel is used to transmit the differential expression and the ciphertext (Verma 2020). The partitioning of the data required to perform the cryptographical scheme gave the attacker a more challenging task of grasping all the necessary components to encrypt and decrypt the transmitted ciphertext.

References

Briones, R.P. (2019). On the Application of Nonhomogeneous Differential Equations to a Laplace Transform-based Cryptographic Process. *Journal of Mathematics and Statistical Science, 5*(11), 302-307.

Gençoğlu, M.T. (2016). Use of integral transform in cryptology. *Science and Engineering. Journal of Fırat University, 28*(2), 217-220.

Gençoğlu, M. T. (2017). Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions. *Communications in Mathematics and Applications, 8*(2), 183-189.

Gupta, R. (2020). Propounding a New Integral Transform: Gupta Transform with Applications in Science and Engineering. *International Journal of Scientific Research in Multidisciplinary Studies, 6*(3), 14-19.

Gupta, R. (2020). On novel integral transform: Rohit Transform and its application to boundary value problems. *ASIO Journal of Chemistry, Physics, Mathematics and Applied Sciences (ASIO-JCPMAS), 4*(1), 08-13.

Jadhav Shaila Shivaji, H.A. (2021). New Method for Cryptography using Laplace-Elzaki Transform. *Psychology and Education Journal, 58*(5), 1-6.

Kuffi, E.A., Mohammed, A.H., Majde, A.Q., & Abbas, E.S. (2020). Applying al-zughair transform on nuclear physics. *International Journal of Engineering & Technology, 9*(1), 9-11.

Kuffi, E., Abbas, E.S., & Maktoof, S.F. (2019). Solving The Beam Deflection Problem Using Al-Tememe Transforms. *Journal of Mechanics of Continua and Mathematical Science, 14*(4), 519-527.

Kumar, P.S., & Vasuki, S. (2018). An Application of Mahgoub Transform in Cryptography. *Advances in Theoretical and Applied Mathematics, 13*(2), 91-99.

Sedeeg, A.K.H., Abdelrahim Mahgoub, M.M., & SaifSaeed, M.A. (2016). An Application of the New Integral "Aboodh Transform" in Cryptography. *Pure and Applied Mathematics Journal, 5*(5), 151-154.

Verma, D. (2020). Putting Forward a Novel Integral Transform: Dinesh Verma Transform (DVT) and its Applications. *International Journal of Scientific Research in Mathematical and Statistical Sciences, 7*(2), 139-145.