A Modern Technique of Encryption Using The Integral Sadik Transform With The Taylor Series

Emad A.Kuffi[1*] and Nada Sabeeh Mohammed[2]
[1] Department of Mathematics, College of Basic Education, Mustansiriyah University, Baghdad, Iraq
[2] Department of Bioinformatics, College of Biomedical Informatics, Information Technology and Communications of University, Baghdad, Iraq

Abstract. This paper presented a new technique for encrypting original texts based on multiplying the coefficients defined in the Taylor series of the logarithmic function by its equivalent index. As for decryption, a Sadik integral transform and its inverse were applied. Through this new technique, new mathematical techniques for encryption and decryption were discovered. This paper includes a practical example in order to demonstrate the efficiency of this technique.

1- Introduction

One of the most important goals that can be achieved by using encryption methods is to protect the information that people transmit to each other through communication channels in a way that makes the process of decoding and understanding the transmitted information difficult for attackers. Therefore, encryption methods are built with several strategic steps to encrypt the original information. In contrast to these methods, In contrast to these methods, there are other methods used for decryption.In [1], the original text represented by a matrix is encrypted by inverting this array. In addition, the original text cannot be decrypted if the matrix of keys cannot be inverted.In [2], the Laplace transform is used to encrypt the information, and to decrypt the information the inverse Laplace transform is usedIn 2013, the hyperbolic function resulting from the Laplace transform is used to encrypt the original text, to return the encrypted text to the original the inverse Laplace transform is used [3].In [4], the security provided by systems based on the Laplace transform was tested using a large-scale attack using a technique that can pass the password without using the systems' secret key.In 2021, a new approach to encryption was devised by Elzaki by incorporating the Laplace transform developed by J. S. Shivaji, et al[5].Kuffi et al used SEE transform to encode and decode color images[6]. In 2023, the complex Sadik transform is used in the encryption of the original text and decryption[7].In this paper, we present a new encryption technique by encrypting the original text by applying the Sadik integral technique and then returning the encrypted text to the original text using the inverse of the Sadik integral technique. We present for the first time the mathematical steps involved in the encryption and decryption processes, in addition to the algorithm for the working technique.

1- Basic concepts and characteristics of the integral Sadik technique

Integral transformations have proven their ability to solve many problems in various fields of technology, science, and engineering[8,9].The Sadik integral technique has many properties used in many fields such as control theory and dynamic systems. In addition, it has been shown that integral transformations similar to the Laplace transform are a special case of the Sadik technique [10,11].

In this paper, we show the importance of applying the Sadik integral technique in encrypting information

The Sadik technique is defined[12]:

* Corresponding author: emad.kuffi@uomustansiriyah.edu.iq

1. If g(x) is piecewise continuous on the interval 0≤ x ≤B for any B>0.
2. If $|g(x)| \leq Z.e^{vx}$ when x ≥ N, for any real constant a. and some positive constant Z and N.

So, the Sadik technique of the function g(x) is expressed by:

$$M(f^{\delta},\gamma) = S\{g(x)\} = \frac{1}{f^{\delta}}\int_0^{\infty} e^{-xf^{\delta}}\, g(x)dx \qquad (1)$$

Where,

f is a complex variable,

δ is any nonzero real numerals, and

γ is any real numeral.

While the inverse of the Sadik integral technique is the following:

$$S^{-1}\{g(x)\} = M(f^{\delta},\gamma)$$

Theorem: The linear transform of the Sadik technique is:

$$S\{g_1(x)\} = M_1(f^{\delta},\gamma), S\{g_2(x)\} = M_2(f^{\delta},\gamma), \dots, S\{g_m(x)\} = M_m(f^{\delta},\gamma)$$

Then

$$S\{\omega_1 g_1(x)+\omega_2 g_2(x) + \cdots + \omega_m g_m(x)\} = \omega_1 M_1(f^{\delta},\gamma) + \omega_2 M_2(f^{\delta},\gamma) + \cdots + \omega_m M_m(f^{\delta},\gamma)$$

where $\omega_1, \omega_2, \dots \omega_m$ are constants

2- Major Outcomes

This part presents an idea of encryption the original text in a new way based on the Taylor series

3.1 Encryption

Now, suppose the Taylor expansion as the following:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Applying integration on both sides of the series from 0 to t to obtain:

$$\int_0^t \frac{1}{1-x}dx = \int_0^t (1 + x + x^2 + x^3 + x^4 + \cdots)dx$$

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

$$-t^2\ln(1-t) = t^3 + \frac{t^4}{2} + \frac{t^5}{3} + \frac{t^6}{4} + \cdots = \sum_{j=0}^{\infty} \frac{t^{3+j}}{j+1} \qquad (2)$$

We allocated 0 to A, 1 to B,…, and Z to 25

Let us assume that the location of the first letter of any message is indicated by Γ_0, the location of the second letter is indicated by Γ_1, the location of the third letter is indicated by Γ_2,..., and the location of the mth letter is indicated by Γ_{m-1} such that $\Gamma_m = 0$, $m \geq k$, so k is the length of the message, and thus the values of Γ_j become $j = 0,1,2,\dots,k-1$ by the coefficients of the series in(2), we get:

$$Z(t) = -\Gamma t^2\, ln(1-t) = \Gamma_0 t^3 + \frac{\Gamma_1 t^4}{2} + \frac{\Gamma_2 t^5}{3} + \frac{\Gamma_3 t^6}{4} + \cdots + \frac{\Gamma_{k-1} t^{k+2}}{k} = \sum_{j=0}^{\infty} \frac{\Gamma_j t^{3+j}}{j+1}$$

Now, on the above equation, apply the Sadik integral technique on both sides

$$S\{Z(t)\} = S\{\Gamma_0 t^3 + \tfrac{\Gamma_1 t^4}{2} + \tfrac{\Gamma_2 t^5}{3} + \tfrac{\Gamma_3 t^6}{4} + \cdots + \tfrac{\Gamma_{k-1} t^{k+2}}{k}\} \qquad (3)$$

$$S\{Z(t)\} = \{\frac{\Gamma_0 3!}{f^{4\delta+(\delta+\gamma)}} + \frac{\Gamma_1 4!}{2f^{5\delta+(\delta+\gamma)}} + \frac{\Gamma_2 5!}{3f^{6\delta+(\delta+\gamma)}} + \frac{\Gamma_3 6!}{4f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{\Gamma_{k-1}(k+2)!}{kf^{(k+3)\delta+(\delta+\gamma)}}\}$$

Let $O_j = \frac{\Gamma_j (j+3)!}{J+1}$, $j = 0,1,2,\dots,k-1$

$$S\{Z(t)\} = \{\frac{O_0}{f^{4\delta+(\delta+\gamma)}} + \frac{O_1}{f^{5\delta+(\delta+\gamma)}} + \frac{O_2}{f^{6\delta+(\delta+\gamma)}} + \frac{O_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{O_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

Now select the invertible key, $P = [0:25]$, where the gcd {26,1}=1

Multiply P_j by O_j, $j = 0,1,2,\dots,k-1$

$$S\{PZ(t)\} = \{\frac{P_0 O_0}{f^{4\delta+(\delta+\gamma)}} + \frac{P_1 O_1}{f^{5\delta+(\delta+\gamma)}} + \frac{P_2 O_2}{f^{6\delta+(\delta+\gamma)}} + \frac{P_3 O_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{P_{k-1} O_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

To simplify the above step, suppose that $Q_j = P_j \cdot O_j$, $j = 0,1,2,\dots,k-1$

$$S\{PZ(t)\} = \{\frac{Q_0}{f^{4\delta+(\delta+\gamma)}} + \frac{Q_1}{f^{5\delta+(\delta+\gamma)}} + \frac{Q_2}{f^{6\delta+(\delta+\gamma)}} + \frac{Q_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{Q_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

Remark 3.1: The presented original text in terms of Γ_j underneath the Sadik technique to the Taylor series of the function $Z(t)$, (that is, after writing them as coefficients of equation (3), and then applying the Sadik technique), and utilizing the invertible key P_j can be transformed to cipher text in terms of $\emptyset_j$, $j = 0,1,2,\dots,k-1$ for instance

$Q_j = \emptyset_j \bmod 26$ or $\emptyset_j = Q_j - 26\varphi_j$, $j = 0,1,2,\dots,k-1$

3.2 Decryption

The message we acquired is a cipher text in terms of $\emptyset_j$, $j = 0,1,2,\dots k-1$ which is rewarded to Q_j, $j = 0,1,2,\dots,k-1$ for instance

$$Q_j = \emptyset_j + 26\varphi_j \qquad (4)$$

Where

$$S\{PZ(t)\} = \{\frac{Q_0}{f^{4\delta+(\delta+\gamma)}} + \frac{Q_1}{f^{5\delta+(\delta+\gamma)}} + \frac{Q_2}{f^{6\delta+(\delta+\gamma)}} + \frac{Q_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{Q_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

Now multiply P_j^{-1} by Q_j , $j = 0,1,2,\dots k-1$, we get

$$S\{P^{-1}PZ(t)\} = \{\frac{P_0^{-1}Q_0}{f^{4\delta+(\delta+\gamma)}} + \frac{P_1^{-1}Q_1}{f^{5\delta+(\delta+\gamma)}} + \frac{P_2^{-1}Q_2}{f^{6\delta+(\delta+\gamma)}} + \frac{Q_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{Q_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

$$S\{Z(t)\} = \{\frac{O_0}{f^{4\delta+(\delta+\gamma)}} + \frac{O_1}{f^{5\delta+(\delta+\gamma)}} + \frac{O_2}{f^{6\delta+(\delta+\gamma)}} + \frac{O_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{O_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

Now use the inverse of the Sadik technique on the above equation's two sides, to obtain:

$$S^{-1}S\{Z(t)\} = S^{-1}\{\frac{O_0}{f^{4\delta+(\delta+\gamma)}} + \frac{O_1}{f^{5\delta+(\delta+\gamma)}} + \frac{O_2}{f^{6\delta+(\delta+\gamma)}} + \frac{O_3}{f^{7\delta+(\delta+\gamma)}} + \cdots + \frac{O_{k-1}}{f^{(k+3)\delta+(\delta+\gamma)}}\}$$

$$S\{Z(t)\} = \{O_0 3!\, t^3 + O_1 4!\, t^4 + O_2 5!\, t^5 + O_3 6!\, t^6 + \cdots + O_{k-1}[k+2]!\, t^{k+2}\}$$

Thus, we can obtain the original text by applying the following formula:

$$\Gamma_j = \frac{O_j(j+1)}{(J+3)!}\ , j = 0,1,2,\dots,k-1$$

Remark 3.2: The supplied text expression of the cipher $\emptyset_j$, $j = 0,1,2,\dots,k-1$ and use the given key P_j, $j = 0,1,2,\dots,k-1$ It can be transformed into original text Γ_j , $j = 0,1,2,\dots,k-1$ underneath the inverse of the Sadik technique for (3) so that

$$\Gamma_j = \frac{O_j(j+1)}{(J+3)!}\ , j = 0,1,2,\dots,k-1$$

Where $Q_j = \emptyset_j - 26\varphi_j \qquad , j = 0,1,2,\dots,k-1$

Example 4.1: Suppose we have the message (Roaa Razak), representing the original text, we find the encrypt and decrypt the previous message.

Encryption: Converting the original text into equivalent numbers: 17, 14, 0, 0, 17, 0, 25, 0, 10
If k=9 represents the length of the message. Assume this

$\Gamma_0 = 17,\quad \Gamma_1 = 14,\quad \Gamma_2 = 0,\quad \Gamma_3 = 0,\quad \Gamma_4 = 17,\quad \Gamma_5 = 0,\quad \Gamma_6 = 25,\quad \Gamma_7 = 0,\quad \Gamma_8 = 10,\quad \Gamma_n = 0,\quad n \geq 9$

To use these numbers as coefficients for $-t^2\ln(1-t)$, we assume
, we obtain:$Z(t) = -\Gamma t^2\ln(1-t)$

$$Z(t) = -\Gamma t^2\ln(1-t) = \Gamma_0 t^3 + \frac{\Gamma_1 t^4}{2} + \frac{\Gamma_2 t^5}{3} + \frac{\Gamma_3 t^6}{4} + \cdots + \frac{\Gamma_8 t^{k11}}{9}$$

$$Z(t) = -\Gamma t^2\ln(1-t) = 17t^3 + \frac{14t^4}{2} + \frac{t^7}{5} + \frac{25t^9}{7} + \cdots + \frac{10t^{k11}}{9}$$

Apply the Sadik technique on two sides:

$$S\{g(x)\} = M(f^{\delta}, \gamma)$$

$$g(x) = S\{Z(t)\} = \{17\frac{3!}{f^{4\delta+(\delta+\gamma)}} + 14\frac{4!}{2f^{5\delta+(\delta+\gamma)}} + 17\frac{7!}{5f^{8\delta+(\delta+\gamma)}} + 25\frac{9!}{7f^{10\delta+(\delta+\gamma)}} + 10\frac{11!}{9f^{12\delta+(\delta+\gamma)}}\}$$

$$g(x) = S\{Z(t)\} = \{\frac{120}{f^{4\delta+(\delta+\gamma)}} + \frac{168}{f^{5\delta+(\delta+\gamma)}} + \frac{17136}{f^{8\delta+(\delta+\gamma)}} + \frac{1296000}{f^{10\delta+(\delta+\gamma)}} + \frac{44352000}{f^{12\delta+(\delta+\gamma)}}\}$$

Now, recasting the resulting values

$O_0 = 102,\quad O_1 = 168,\quad O_2 = 0,\quad O_3 = 0,\quad O_4 = 17136,\quad O_5 = 0,\quad O_6 = 1296000,\quad O_7 = 0,\quad O_8 = 44352000$

Now selecting an inventible key

$$Q_j = P_j \cdot O_j, \quad j = 0,1,2,\dots,k-1$$

$$Q_0 = 3 \cdot 102 = 306, \quad Q_1 = 5 \cdot 168 = 840, \quad Q_2 = 7 \cdot 0 = 0, \quad Q_3 = 11 \cdot 0 = 0, \quad Q_4 = 13 \cdot 17136 = 222768, \quad Q_5 = 17 \cdot 0 = 0, \quad Q_6 = 19 \cdot 1296000 = 2451000, \quad Q_7 = 23 \cdot 0 = 0, \quad Q_8 = 2 \cdot 44352000 = 88704000$$

mod 26 is
$306 = 20 \bmod 26$, $840 = 8 \bmod 26$, $0 = 0 \bmod 26$, $0 = 0 \bmod 26$, $222768 = 0 \bmod 26$, $0 = 0 \bmod 26$, $2451000 = 6 \bmod 26$, $0 = 0 \bmod 26$, $88704000 = 8 \bmod 26$

Now let
$\emptyset_0 = 20, \quad \emptyset_1 = 8, \quad \emptyset_2 = 0, \quad \emptyset_3 = 0, \quad \emptyset_4 = 0, \quad \emptyset_5 = 0, \quad \emptyset_6 = 6, \quad \emptyset_7 = 0, \quad \emptyset_8 = 8$

So the ciphertext is as follows:

20, 8, 0, 0, 0, 0, 6, 0, 8

the original text {Roaa Razak} obtains transformed to {Uiaa Aagai}.

Decryption:: If encrypted text{Uiaa Aagai} is equivalent to

20, 8, 0, 0, 0, 0, 6, 0, 8

Assume that the

$$\emptyset_0 = 20, \quad \emptyset_1 = 8, \quad \emptyset_2 = 0, \quad \emptyset_3 = 0, \quad \emptyset_4 = 0, \quad \emptyset_5 = 0, \quad \emptyset_6 = 6, \quad \emptyset_7 = 0, \quad \emptyset_8 = 8$$

Utilizing {4} and Suppose the $\emptyset_j = Q_j + 26\varphi_j \quad , \varphi_j, j = 0,1,2,\dots,8$

11, 32, 0, 0, 8568, 0, 94269, 0, 3411692

We have $g(x) = S\{PZ(t)\} = \{\frac{306}{f^{4\delta+(\delta+\gamma)}} + \frac{840}{f^{5\delta+(\delta+\gamma)}} + \frac{222768}{f^{8\delta+(\delta+\gamma)}} + \frac{2451000}{f^{10\delta+(\delta+\gamma)}} + \frac{88704000}{f^{12\delta+(\delta+\gamma)}}\}$

Now multiply P_j^{-1} by $Q_j, \quad j = 0,1,2,\dots,k-1$ we get:

$$g(x) = \{\frac{102}{f^{4\delta+(\delta+\gamma)}} + \frac{168}{f^{5\delta+(\delta+\gamma)}} + \frac{17136}{f^{8\delta+(\delta+\gamma)}} + \frac{1296000}{f^{10\delta+(\delta+\gamma)}} + \frac{44352000}{f^{12\delta+(\delta+\gamma)}}\}$$

Apply the inverse of the Sadik technique on two sides:

$$S^{-1}g(x) = S^{-1}\{\frac{102}{f^{4\delta+(\delta+\gamma)}} + \frac{168}{f^{5\delta+(\delta+\gamma)}} + \frac{17136}{f^{8\delta+(\delta+\gamma)}} + \frac{1296000}{f^{10\delta+(\delta+\gamma)}} + \frac{44352000}{f^{12\delta+(\delta+\gamma)}}\}$$

$$M(f^{\delta}, \gamma) = \{[3!] \cdot 102t^3 + [4!] \cdot 168t^4 + [7!] \cdot 17136t^7 + [9!] \cdot 1296000t^9 + [11!] \cdot 44352000t^{11}\}$$

By applying the following formula, we will obtain the equivalent values for the original text

$$\Gamma_j = \frac{O_j(j+1)}{(J+3)!} \quad , j = 0,1,2,\dots,8$$

$$\Gamma_0 = 17, \quad \Gamma_1 = 14, \quad \Gamma_2 = 0, \quad \Gamma_3 = 0, \quad \Gamma_4 = 17, \quad \Gamma_5 = 0, \quad \Gamma_6 = 25, \quad \Gamma_7 = 0, \quad \Gamma_8 = 10, \quad \Gamma_n = 0, \quad n \geq 9$$

So that: 17, 14, 0, 0, 17, 0, 25, 0, 10 is the {Roaa Razak}equivalent

3- Algorithm

Encryption:

1. Transform the original text to a decimal numeral.
2. include the decimal numeral as a coefficient of the Taylor series.
3. applying the Sadik technique on two sides of the Taylor series.
4. The including coefficient of the Sadik is $O_j = \frac{\Gamma_j (j+3)!}{J+1}$, $\mathrm{j} = 0,1,2, \dots, \mathrm{k}-1$.
5. Select an invertible key that belongs to [0:25], so that gcd (26,)=1.
6. Multiply $\mathrm{P_j}$ by $\mathrm{O_j}$, $\mathrm{j} = 0,1,2, \dots \mathrm{k}-1$ to get $\mathrm{Q_j}$
7. Applying the relation $\emptyset_{\mathrm{j}} = \mathrm{Q_j} - 26\varphi_{\mathrm{j}}$, $\mathrm{j} = 0,1,2, \dots, \mathrm{k}-1$ to get the encrypted text.

Decryption:

1- Applying the relation $\mathrm{Q}_j = \emptyset_j - 26\varphi_j$, $\mathrm{j} = 0,1,2, \dots, \mathrm{k}-1$, to get the $\emptyset_j$ from encrypted text.
2- Multiply P_j^{-1} by Q_j , $\mathrm{j} = 0,1,2, \dots, \mathrm{k}-1$, to get O_j.
3- Applying the inverse of Sadik technique to two sides of the Taylor series.
4- Applying the relation $\Gamma_j = \frac{O_j (j+1)}{(J+3)!}$, $\mathrm{j} = 0,1,2, \dots, \mathrm{k}-1$, to get the original text.

4- Conclusion

The encryption system applied in this paper is a new system that was built based on the Sadik integral technique with the key in the set [0:25], which is a key that has reversibility and at the same time satisfies the condition gcd(26, k) = 1. The technique used in this system provides high security In front of the attackers to know the decryption keys. In this work, we used the Taylor series, which is one of the logarithmic functions. The ability of the inverse of the Sadik technique inverse to inverse the trigonometric and hyperbolic functions helped in finding new conclusions.

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*, 2021, 58(5), pp. 1-6.
6 E.A.Kuffi, S. A. Mehdi, and E. A.Mansour, “Color Image Encryption Based on New Integral Transform SEE”, *Journal of Physics*, 2022, pp. 1-9.
7 N. S. Mohammed, and E. A. Kuffi, “Perform the CSI complex Sadik integral transform in cryptography, ”*Journal of Interdisciplinary Mathematics*, vol. (26), No. 6, 2023, pp. 303–1309.
8 N. S. Mohammed, and E. A. Kuffi, “The complex integral transform complex Sadik transform of error function, ”*Journal of Interdisciplinary Mathematics*, vol.(26), No. 6, 2023, pp. 1145–1157.
9 N. S. Mohammed, and E. A. Kuffi, “Implementation of the CST complex Sadik transform to treat population expansion and decay problems, ”*Journal of Interdisciplinary Mathematics*, vol. (26), No. 6, 2023, pp. 1261–1271.
10 S. L.Shaikh, “Sadik Transform in Control Theory, ” *International Journal of Innovative Science and Research Technology*, vol.(3), 2018 , pp. 396–398.

11 S. S. Redhwan, S. L. Shaikh, and M. S. Abdo, “SOME PROPERTIES OF SADIK TRANSFORM AND ITS APPLICATIONS OF FRACTIONAL-ORDER DYNAMICAL SYSTEMS IN CONTROL THEORY, ” *math.GM*, 2019, pp. 1–15.

12 S. L. Shaikh, “Introducing a New Integral Transform: Sadik Transform, ” *American International Journal of Research in Science, Technology, Engineering & Mathematics*, 2018, pp. 100–102.