ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 9, No. 4, November 2021, pp.892-897

Mathematical modeling for cryptography using Jafari transformation method

Eman A. Mansour [1], Noor Kadhim Meftin [2]
[1]Department of Electrical Technologies, Southern Technical University/Technical Institute Nasiriyah
[2] Computer Sciense and Information System Department, Al-Mansour University College

ABSTRACT

Data protection is representing a huge trade in the modern era; the vast communication development gave this field increased attention from all sorts of parties (friends and foes); integral transforms have played a decent role in many methods that are proposed to be used in the cryptography field.
In this work, the Jafari integral transform has been used as a part of a symmetric key system, by implementing a practical example in encryption and decryption; Jafari integral transform has proven its capability to be invested in cryptography and in the data security field in general.

Keywords: Jafari integral transform, Cryptosystem, Encryption, Decryption, Symmetric key system, Asymmetric key system, Private key, Public key.

Corresponding Author:

Eman A. Mansour
Department of Electrical Technologies
Southern Technical University/Technical Institute Nasiriyah
Iraq
E-mail: iman.am73@stu.edu.iq

1. Introduction

Securing the data is representing the protection of data from the unauthorized parties to compromised that data in any possible form (corrupting, changing, unauthorized access), many measures have been taken to secure data during their transfer from one location into another, the most effective way to protect the information is by transforming the transmitted information from its comprehensible form, that could be read and understood by any party (authorized or unauthorized) into an illegible form that could be understood by the corresponding parties only, this process is called cryptography.
The cryptosystems represent the infrastructure that would allow the cryptographic techniques to be implemented; figure 1 represents the fundamental structure of the cryptosystem [1].

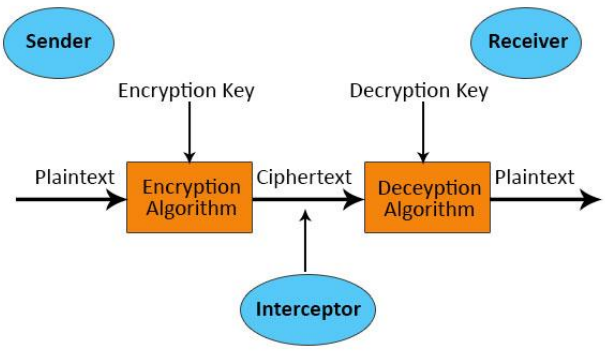

Figure 1. Fundamental structure of cryptosystems

In the cryptosystem, the party that would transmit the information (the sender), should encrypt the information using an encryption algorithm and encryption key[2]; the resulted information that would be transmitted through an unsecured channel is cryptic, the receiving party of the encrypted information (receiver), should decrypt the information using a decryption algorithm and decryption key. The encryption and decryption keys could be secret or public depending on the used cryptographic technique, cryptosystems could be classified into [1]:

- Symmetric key encryption (secret key systems): this system is used in the classical and some modern methods, where the same key that is known only to the engaged parties, is used for encryption and decryption.
- Asymmetric key encryption (public key systems): this system is used in the most recent methods, where different keys are used for encryption and decryption, modern systems often employ a combination of both systems.

Integral transforms have been deployed in many scientific fields [3]. Data security is one of the fields that exploited integral transforms, many cryptographic methods that are relied on integral transforms have been proposed [4]. However, the novelty of Jafari transform has prevented it from being used in such an important field, even though Jafari integral transform represents an excellent tool to be used in the cryptography field due to its generalization format [5].
In this work, a new secret system cryptographic method, that is based on the usage of Jafari integral transform, has been proposed and discussed through practical example, which shown the possibility of using such promising new transform in the all-growing field of data security.

2. Jafari transform

The Jafari transform of the function $f(t), t \geq 0$, $h(s) \neq 0$ and $g(s)$ being positive real functions, is given by [1]:

$J\{f(t)\} = h(s) \int_{t=0}^{\infty} f(t) e^{-g(s)t} dt = R\big(h(s), g(s)\big)$.

Where the integral exists for some $g(s)$. It must be noted that Jafari transform for those $f(t)$, which are not continuously differentiable, contains terms with negative or functional power of $g(s)$.

Supposing that for all $t \geq 0$, the function $f(t)$ is a piecewise continuous, and satisfying $|f(t)| \leq Me^{\mu t}$, then $R\big(h(s), g(s)\big)$ exists $\forall\, g(s) > \mu$.

Since,

$\left|\left|R\big(h(s), g(s)\big)\right|\right| = \left|h(s) \int_{t=0}^{\infty} f(t) e^{-g(s)t} dt\right| \leq h(s) \int_{t=0}^{\infty} |f(t)| e^{-g(s)t} dt \leq h(s) \int_{t=0}^{\infty} Me^{\mu t} e^{-g(s)t} dt \leq \frac{M\, h(s)}{\mu - g(s)}$, the statement is valid.

The correspondence inverse Jafari transform is:

$J^{-1}\{R\big(h(s), g(s)\big)\} = f(t)$.

Here, $f(t)$ and $R\big(h(s), g(s)\big)$ are called a combination of Jafari transform.

2.1. Jafari transform linearity property

The Jafari transformation is a linear transformation, the linearity property of the transformation can be stated as [4]:

If $J\{f_1(t)\} = R_1\big(h_1(s), g_1(s)\big)$, $J\{f_2(t)\} = R_2\big(h_2(s), g_2(s)\big)$, then

$J\{K_1 f_1(t) + K_2 f_2(t)\} = K_1 J\{f_1(t)\} + K_2\, J\{f_2(t)\} = K_1 R_1 + K_2 R_2$ ...

Where K_1 and K_2 are constants.

2.2. Jafari transform for some basic functions

For this work, it is going to be assumed that all the elementary functions (algebraic and transcendental) and their Jafari transforms exist [2].

1) $J\{t^n\} = \frac{\Gamma(n+1)\, h(s)}{[g(s)]^{n+1}}$, $n > 0$.
2) $J\{1\} = \frac{h(s)}{g(s)}$.
3) $J\{e^{\lambda t}\} = \frac{h(s)}{g(s)-\lambda}$, $g(s) > \lambda$.
4) $J\{\sin(Kt)\} = \frac{Kh(s)}{[g(s)]^2+K^2}$.
5) $J\{\cos(Kt)\} = \frac{g(s)h(s)}{[g(s)]^2+K^2}$.
6) $J\{\sinh(Kt)\} = \frac{Kh(s)}{[g(s)]^2-K^2}$.
7) $J\{\cosh(Kt)\} = \frac{g(s)h(s)}{[g(s)]^2-K^2}$.
8) $J\{f^{(n)}(t)\} = [g(s)]^m J\{f(t)\} - h(s)\sum_{i=0}^{n-1}[g(s)]^{n-i-1} f^{(i)}(0)$.
9) $J\{t^m f(t)\} = \left(\frac{-d}{ds}\right)^m R\big(h(s), g(s)\big)$ and $J^{-1}\left\{\left(\frac{-d}{ds}\right)^m R\big(h(s), g(s)\big)\right\} = t^m f(t)$.
10) $J\{t^m e^{Kt}\} = \frac{n!h(s)}{(g(s)-K)^{m+1}}$.

3. The proposed cryptographic methodology

The proposed cryptographic methodology includes the following:

- The proposed method is belonged to the secret key systems, in which the encryption and decryption keys are known only to the sender and the receiver[6].
- The data that is processed in the proposed method is encoded in the extended ASCII code, where the total number of symbols are 256 [7].
- Jafari integral transform has been used at the sender side as a part of the encryption algorithm, and inverse Jafari integral transform is used at the receiving side as a part of decryption algorithm.

3.1. Encryption algorithm

The following steps should be performed at the sender side, to transform the plaintext from its readable form into illegible text (ciphertext). The resulting ciphertext is going to be transmitted throughout an unsecured channel.

Step (1): The letters of the plaintext of length (N), are encoded into their equivalent decimal numbers in the ASCII code.

Step (2): A finite sequence (G sequence) is generated from the ASCII code decimal encoding of the plaintext letters.

Step (3): The G sequence parameters are used as coefficients into the polynomial, that is generated from the mathematical formula: $t\cosh(rt) = t + \frac{r^2t^3}{2!} + \frac{r^3t^4}{4!} + \frac{r^6t^7}{6!} + \frac{r^8t^9}{8!} + \cdots + \frac{r^{2n}t^{2n+1}}{2n!} + \cdots = \sum_{n=0}^{\infty}\frac{r^{2n}t^{2n+1}}{(2n)!}$

Where, r is a random constant number $r \geq 1$, and must be agreed upon between the sender and the receiver previously.

The G sequence polynomial would be:

$f(t) = Gt\cosh(rt) = G_0 t + G_1\frac{r^2t^3}{2!} + G_2\frac{r^3t^4}{4!} + G_3\frac{r^6t^7}{6!} + G_4\frac{r^8t^9}{8!} + \cdots + G_{N-1}\frac{r^{2n}t^{2n+1}}{(2n)!} + \cdots = \sum_{n=0}^{N-1} G_n\frac{r^{2n}t^{2n+1}}{(2n)!}$.

Step (4): Jafari transform is applied to the generated polynomial, as: $J\{f(t)\} = J\{Gt\cosh(rt)\}$.

Step (5): Finding the decimal ASCII encoding of the ciphertext by applying the relation: $C_i = M_i \bmod 200$, $i = 0,1,2, \ldots, N-1$, where M_i is the polynomial coefficients from step (4).

The resulted decimal ASCII encoding of the ciphertext is returned back into their equivalent ASCII symbols, to be transmitted through the unsecured channel[8].

Step (6): Calculating the decryption key, that would be sent into the receiver party through a secure channel, using the formula: $k_i = \frac{(M_i - C_i)}{200}$, $i = 0,1,2, \dots, N-1$.

3.1.1. Encryption example

To clarify the encryption algorithm of the proposed cryptographic mathematical model, the following example is going to be considered.

Before starting the encryption algorithm, it is going to be assumed that the communicating parties, agreed upon using 2 as the random number required for encryption, decryption, and the generation of the decryption key; the random number and the decryption key are going to be transformed into the receiving party through a secured channel[9].

Step (1): Let the plaintext that is required to be sent throughout the unsecured channel is: ACADEMICS

The number of letters in the plaintext (plaintext length), $N = 9$.

The decimal ASCII codes encoding of the plaintext letters are:

$A = 65$, $C = 67$, $A = 65$, $D = 68$, $E = 69$, $M = 77$, $I = 73$, $C = 67$, $S = 83$.

Step (2): The plaintext finite sequence (G sequence) is:

$G_0 = 65$, $G_1 = 67$, $G_2 = 65$, $G_3 = 68$, $G_4 = 69$, $G_5 = 77$, $G_6 = 73$, $G_7 = 67$, $G_8 = 83$, $G_n = 0$ for $n \geq 9$.

Step (3): The G sequence parameters are going to be used as coefficients to the polynomial of $t\cosh(rt)$, as:

$$f(t) = Gt\cosh(rt) = \sum_{n=0}^{8} G_n \frac{r^{2n}t^{2n+1}}{(2n)!} = G_0 t + G_1 \frac{r^2t^3}{2!} + G_2 \frac{r^3t^4}{4!} + G_3 \frac{r^6t^7}{6!} + G_4 \frac{r^8t^9}{8!} + G_5 \frac{r^{10}t^{11}}{10!} + G_6 \frac{r^{12}t^{13}}{12!} + G_7 \frac{r^{14}t^{15}}{14!} + G_8 \frac{r^{16}t^{17}}{16!},$$

$$f(t) = 65t + 67\frac{r^2 2^3}{2!} + 65\frac{r^3 2^4}{4!} + 68\frac{r^6 2^7}{6!} + 69\frac{r^8 2^9}{8!} + 77\frac{r^{10} 2^{11}}{10!} + 73\frac{r^{12} 2^{13}}{12!} + 67\frac{r^{14} 2^{15}}{14!} + 83\frac{r^{16} 2^{17}}{16!}.$$

Step (4): Applying Jafari transform on both sides of the polynomial from the previous step, as:

$$J\{f(t)\} = J\{65t\} + J\left\{67\frac{r^2 2^3}{2!}\right\} + J\left\{65\frac{r^3 2^4}{4!}\right\} + J\left\{68\frac{r^6 2^7}{6!}\right\} + J\left\{69\frac{r^8 2^9}{8!}\right\} + J\left\{77\frac{r^{10} 2^{11}}{10!}\right\} + J\left\{73\frac{r^{12} 2^{13}}{12!}\right\} + J\left\{67\frac{r^{14} 2^{15}}{14!}\right\} + J\left\{83\frac{r^{16} 2^{17}}{16!}\right\},$$

$$J\{f(t)\} = \frac{65\,h(s)}{[g(s)]^2} + \frac{804\,h(s)}{[g(s)]^4} + \frac{5200\,h(s)}{[g(s)]^6} + \frac{30464\,h(s)}{[g(s)]^8} + \frac{158976\,h(s)}{[g(s)]^{10}} + \frac{867328\,h(s)}{[g(s)]^{12}} + \frac{3887104\,h(s)}{[g(s)]^{14}} + \frac{16465920\,h(s)}{[g(s)]^{16}} + \frac{92471296\,h(s)}{[g(s)]^{18}}.$$

Step (5): Finding the required ciphertext from: $C_i = M_i \bmod 200$, such as:

$C_0 = 65 \bmod 200 = 65$.

$C_1 = 804 \bmod 200 = 4$.

$C_2 = 5200 \bmod 200 = 0$.

$C_3 = 30464 \bmod 200 = 64$.

$C_4 = 148976 \bmod 200 = 176$.

$C_5 = 867328 \bmod 200 = 128$.

$C_6 = 3887104 \bmod 200 = 104$.

$C_7 = 16465920 \bmod 200 = 120$.

$C_8 = 92471296 \bmod 200 = 96$.

The ASCII symbols that are equivalent to the resulted ciphertext decimal encoding from step (5) are: A♦@ÇhxŸ.

Step (6): The decryption key for the taken example can be obtained as:

$k_i = \frac{(M_i - C_i)}{200} \Rightarrow k_0 = 0, k_1 = 4, k_2 = 26, k_3 = 152, k_4 = 794, k_5 = 4336, k_6 = 19435, k_7 = 82329, k_8 = 462356$.

3.2. Decryption algorithm

The following steps should be performed at the receiving side to transform back the received illegible ciphertext into its original readable plaintext[10].

Step (1): The decryption key k_i, and the random number r are delivered to the receiving end through a secured channel, while the ASCII symbols of the ciphertext are delivered through an unsecured channel.

Step (2): Encoding the received ASCII symbols, of length N, into a finite sequence of their equivalent decimal ASCII codes (C_i').

Step (3): The received decryption key is used to generate a sequence of coefficients for the polynomial that would be used in the inverse Jafari transform.

The formula for generating the polynomial that would be used in the inverse Jafari transform is: $G\left\{\frac{-d}{ds}\right\}\frac{g(s)h(s)}{[g(s)]^2-2^2} = \sum_{n=0}^{N-1}\frac{M_n\, h(s)}{[g(s)]^{2n+2}}$, where the coefficients M_i could be found by: $M_i = 200k_i + C_i'$.

Step (4): The inverse Jafari transform would be applied on the generated polynomial from step (3), to get the ASCII decimal codes of the plaintext.

The formula of applying inverse Jafari transform on the mentioned polynomial is: $f(t) = J^{-1}\left\{\sum_{n=0}^{N-1}\frac{M_n\, h(s)}{[g(s)]^{2n+2}}\right\}$.

Step (5): The concluded coefficients from $f(t)$ polynomial represented the ASCII decimal codes are encoded back into their ASCII symbols, in which they would represent the original plaintext.

3.2.1. Decryption example

To clarify the decryption algorithm of the proposed cryptographic mathematical model, the following example is going to be considered[11].

Step (1): The following random number and the decryption key have been received via secured channel: $r = 2$ and k_i for $i = 0,1,2,\ldots,8$ is 0,4,26,152,794,4336,19435,82329,462356.

And the following ciphertext received via unsecured channel is: A♦@ Çhx`.

Step (2): The finite sequence of the decimal ASCII encoding of the received ciphertext is: $C_0' = 65, C_1' = 4, C_2' = 0, C_3' = 64, C_4' = 176, C_5' = 128, C_6' = 104, C_7' = 120, C_8' = 96$.

Step (3): Using the given key (k_i) for $i = 0,1,2,\ldots,8$, the coefficients sequence is generated by:

$G\left\{\frac{-d}{ds}\right\}\frac{g(s)h(s)}{[g(s)]^2-2^2} = \sum_{n=0}^{N-1}\frac{M_n\, h(s)}{[g(s)]^{2n+2}}$, where: $M_i = 200k_i + C_i'$, for $i = o, 1,2,\ldots,8$,

$M_0 = 65$.
$M_1 = 804$.
$M_2 = 5200$.
$M_3 = 30464$.
$M_4 = 158976$.
$M_5 = 867328$.
$M_6 = 3887104$.
$M_7 = 16465920$.
$M_8 = 92471296$.

Then, $G\left\{\frac{-d}{ds}\right\}\frac{g(s)h(s)}{[g(s)]^2-2^2} = \sum_{n=0}^{N-1}\frac{M_n\, h(s)}{[g(s)]^{2n+2}} = \frac{65\, h(s)}{[g(s)]^2} + \frac{804\, h(s)}{[g(s)]^4} + \frac{5200\, h(s)}{[g(s)]^6} + \frac{30464\, h(s)}{[g(s)]^8} + \frac{158976\, h(s)}{[g(s)]^{10}} + \frac{867328\, h(s)}{[g(s)]^{12}} + \frac{3887104\, h(s)}{[g(s)]^{14}} + \frac{16465920\, h(s)}{[g(s)]^{16}} + \frac{92471296\, h(s)}{[g(s)]^{18}}$.

Step (4): Applying the inverse Jafari transform on the polynomial generated from the previous step as:

$f(t) = J^{-1}\left\{\sum_{n=0}^{N-1}\frac{M_n\, h(s)}{[g(s)]^{2n+2}}\right\} = J^{-1}\left\{\frac{65\, h(s)}{[g(s)]^2} + \frac{804\, h(s)}{[g(s)]^4} + \frac{5200\, h(s)}{[g(s)]^6} + \frac{30464\, h(s)}{[g(s)]^8} + \frac{158976\, h(s)}{[g(s)]^{10}} + \frac{867328\, h(s)}{[g(s)]^{12}} + \frac{3887104\, h(s)}{[g(s)]^{14}} + \frac{16465920\, h(s)}{[g(s)]^{16}} + \frac{92471296\, h(s)}{[g(s)]^{18}}\right\}$,

$f(t) = 65t + 67\frac{r^2 2^3}{2!} + 65\frac{r^3 2^4}{4!} + 68\frac{r^6 2^7}{6!} + 69\frac{r^8 2^9}{8!} + 77\frac{r^{10} 2^{11}}{10!} + 73\frac{r^{12} 2^{13}}{12!} + 67\frac{r^{14} 2^{15}}{14!} + 83\frac{r^{16} 2^{17}}{16!}$.

Step (5): $f(t)$ polynomial coefficients, which are:

$G_0 = 65 , G_1 = 67 , G_2 = 65 , G_3 = 68 , G_4 = 69 , G_5 = 77 , G_6 = 73 , G_7 = 67 , G_8 = 83 , G_n = 0$ for $n \geq 9$,
represent the ASCII decimal encoding of the plaintext, and by encoding them back into their ASCII symbols, the original plaintext (ACADEMICS) is generated back.

4. Discussion and conclusions

In the Jafari integral transform, the general functions (h(s) and g(s)), in which could obtain any type of functions (trigonometric, hyperbolic, exponential, etc.), gave the transform an immense value to be used in the fields that required functions diversity in them [12]. Cryptography represents one of the most prominent fields, where the ambiguity of the cryptographic methods to the adversary represents a substantial advantage for the engaged parties [13].

A new cryptographic methodology using Jafari integral transform has been proposed, the proposed method has a general nature, where it doesn't use specific functions for encryption and decryption. To recognize the applicability of the proposed methodology, a practical example that includes encrypting a plaintext using the proposed encryption algorithm, then decrypt the resulting ciphertext has been applied, the results from the application of the proposed cryptographical methodology proved the capability of using the novel Jafari integral transform in the cryptography field to secure data [14].

References

[1] A. I. El-Mesady, Y. S. Hamed, and A. M. Alsharif, "Jafari Transformation for Solving a System of Ordinary Differential Equations with Medical Application," *Fractal Fract.*, vol. 5, no. 3, p. 130, 2021.

[2] E. A. Mansour, S. Mehdi, and E. A. Kuffi, "The new integral transform and its applications," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 849–856, 2021.

[3] M. T. Gençoğlu, "Use of integral transform in cryptology," *Sci. Eng. J Fırat Univ*, vol. 28, no. 2, pp. 217–220, 2016.

[4] M. T. Gençoğlu, "Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions," *Commun. Math. Appl.*, vol. 8, no. 2, pp. 183–189, 2017.

[5] G. N. Lakshmi, B. R. Kumar, and A. C. Sekhar, "A cryptographic scheme of Laplace transforms," *Int. J. Math. Arch.*, vol. 2, no. 12, pp. 2515–2519, 2011.

[6] M. Mohand and A. Mahgoub, "The new integral transform 'Mohand Transform,'" *Adv. Theor. Appl. Math.*, vol. 12, no. 2, pp. 113–120, 2017.

[7] C. Jayanthi and V. Srinivas, "Mathematical modeling for cryptography," *Int. J. Math. Trends Technol.*, vol. 65, no. 2, pp. 10–15, 2019.

[8] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[9] A. Kahate, *Cryptography and network security*. Tata McGraw-Hill Education, 2013.

[10] A. Kamal and H. Sedeeg, "The New Integral Transform''Kamal Transform'','' *Adv. Theor. Appl. Math.*, vol. 11, no. 4, pp. 451–458, 2016.

[11] A. K. H. Sedeeg, M. M. AbdelrahimMahgoub, and M. A. SaifSaeed, "An Application of the New Integral 'Aboodh Transform' in Cryptography," *Pure Appl. Math. J.*, vol. 5, no. 5, pp. 151–154, 2016.

[12] A. Stanoyevitch, *Introduction to Cryptography with mathematical foundations and computer implementations*. CRC Press, 2010.

[13] P. S. Kumar and S. Vasuki, "An Application of MAHGOUB Transform in Cryptography," *Adv. Theor. Appl. Math.*, vol. 13, no. 2, pp. 91–99, 2018.

[14] W. Zhang, Y. Zhao, and S. Fan, "Cryptosystem Identification Scheme Based on ASCII Code Statistics," *Secur. Commun. Networks*, vol. 2020, 2020.