Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 2, pp. 311-319
DOI : 10.47974/JDMSC-1856

Application of a new integral "KAJ transform" technique in cryptography

Jinan A. Jasim *
Department of Mathematics
College of Education
Mustansiriyah University
Baghdad 10052
Iraq

Maysam Rahi Ali †
Department of Mathematics
College of Engineering
Al-Qadisiyah University
Al-Qadisiyah 58002
Iraq

Emad A. Kuffi §
College of Basic Education
Mustansiriyah University
Baghdad 10052
Iraq

Abstract

This work introduces the Kuffi- Abbas- Jawad transform, also known as the KAJ-integral transformation. We discuss key KAJ- transition properties and their cryptographic

* *ORCID-ID:* **0000-0002-5128-1522**
† *ORCID-ID:* **0000-0002-4406-8731**
§ *ORCID-ID:* **0000-0002-5905-5319**

* *E-mail:* **jinanadel78@uomus.tansiriyah.edu.iq (Corresponding Author)**
† *E-mail:* **maysamrahi7@gmail.com**
§ *E-mail:* **emad.kuffi@uomustansiriyah.edu.iq**

applications. An application is presented to demonstrate how to encrypt a plaintext and decrypt it using the KAJ- transform technique and inverse KAJ- transform, respectively.

Subject Classification: *34M25.*

Keywords: *KAJ-transform technique, The KAJ transform's inverse, ASCII Code, Decrypting, Encrypting.*

1. Introduction

Integral transformations have shown to be a highly effective tool in applied mathematics and engineering science over the past 200 years. Due to their popularity, integral transformations are widely recognized for their part in the solution of integral, difference equations, and other scientific issues [1-8]. The presentation of our article uses a KAJ- integral transform technique as a security way for encrypting and decrypting a message in coding theory. The common Laplace integral is where the KAJ-transformation is derived from [9]. Due to this change's core characteristics and mathematical simplicity, the procedures of encrypting prime texts and decrypting texts to give the message is simple. complex transforms Laplace, Elzaki, Sumudu, Aboodh, Kamal, and Mahgoub serve as models for this one. In the course of outlining our methods, a novel cryptographic method utilizing the KAJ- transform is presented. The inverse KAJ-technique is applied to decrypt plaintext, whereas this method is used to encrypt plaintext. By substituting every letter with its appropriate American Standard Code for Information Interchange (ASCII) value [10-15], this technique encrypts data [16-25].

2. Definition and important properties [9]:

2.1 *KAJ- integral transformation*

The most recent integral transformation As an improvement on the SEE integral transform technique, the KAJ- integral technique (denoted as S_m) is described by follows:

$$S_m\{h(t)\} = K(v) = \frac{1}{v^n}\int_{t=0}^{\infty} \quad f\left(\frac{t}{v}\right)e^{-t}dt,$$

2.2. *KAJ-integral transformation for a few basic functions*

- $S_m\{\beta\} = \frac{\beta}{v^{n+1}}, \beta \in R.$
- $S_m\{t\} = \frac{1}{v^{n+1}}.$
- $S_m\{t^m\} = \frac{m!}{v^{n+m}}, m \in N.$
- $S_m\{e^{\alpha t}\} = \frac{v}{v^n(v-\alpha)}, \alpha \in R.$

- $S_m\{sin\ (\alpha t)\ \} = \frac{\alpha}{v^{n-1}(v^2+\alpha^2)}$.
- $S_m\{cos\ (\alpha t)\ \} = \frac{1}{v^{m-2}(v^2+\alpha^2)}$.
- $S_m\{\ sinh\ (\alpha t)\ \} = \frac{\alpha}{v^{n-1}(v^2-\alpha^2)}$.
- $S_m\{cosh\ (\alpha t)\ \} = \frac{1}{v^{m-2}(v^2-\alpha^2)}$.

2.3. *The KAJ-transform technique's inverse*

If $S_m\{(t)\ \} = K(v)$ is the KAJ- transformation, then $(t) = S_m^{-1}\{K(v)\}$ represents an inverse of KAJ-transformation.

Then the KAJ-transformation's inverse is:

- $S_m^{-1} = \left\{\frac{1}{v^{n+1}}\right\} = 1$.
- $S_m^{-1}\left\{\frac{m!}{v^{n+m}}\right\} = t^m, m \in N$.
- $S_m^{-1}\left\{\frac{1}{v^{n-1}(v-\alpha)}\right\} = e^{\alpha t}, \alpha$ is a constant.
- $S_m^{-1}\left\{\frac{\alpha}{v^{n-1}(v^2+\alpha^2)}\right\} = sin\ (\alpha t)$.
- $S_m^{-1}\left\{\frac{1}{v^{m-2}(v^2+\alpha^2)}\right\} = cos\ (\alpha t)$.
- $S_m^{-1}\left\{\frac{\alpha}{v^{n-1}(v^2-\alpha^2)}\right\} = sinh\ (\alpha t)$.
- $S_m^{-1}\left\{\frac{1}{v^{m-2}(v^2-\alpha^2)}\right\} = cosh\ \ (\alpha t)$.

2.4. Linearity property of KAJ-transform technique

Let $S_m\{p(t)\} = K_1(v)$ and $S_m\{q(t)\} = K_2(v)$, then

$$S_m\{cp(t) \pm dq(t)\} = cS_m\{p(t)\} \pm dS_m\{q(t)\},$$

Where $c, d \in R$.

3. KAJ-technique in cryptography

3.1. Encryption algorithms procedure

- Each letter in plaintext messages should have an ASCII value assigned to it.
- The prime text is formatted such as a list of numbers established on the reducing described above.
- For transforming $h(t) = Ft^2e^{\beta t}$, use the KAJ-integral transform. Here, F represents the ASCII values of the plaintext message.
- Calculate $r_k$such that it equals M_k mod 500, $(1 \le k \le n)$. M_k represents the coefficients of $S_m\{h(t)\}$ for the previous equation.

- Determine a new finite series of remainders, $r_1, r_2, \cdots, r_n$, using the same technique.
- The key $Co_k, k \in N$ is a set of quotients, and the encrypted text is represented by the ASCII values $r_1, r_2, \cdots, r_n$.

3.2. *Decryption algorithms procedure*

- Use the Co_k specified, where k is any integer between 1 and n, to translate the given secret message back to plain text. Then applying the corresponding finite series of numbers, $r_1, r_2, \cdots, r_n$, prepare the encrypted text.
- To create the initial message, think about the congruence $M_k = Co_k + 500r_k$, as k could be any value between $(1, n)$.
- Find values of $M_1, M_2, \cdots$ and, M_n using the approach outlined above.
- Apply the inverse of the KAJ- technique to the $S_m\{h(t)\}$ function.
- The polynomial $h(t)$ coefficients should be arranged in a sequence. This series ought to end.
- Modify the number of the sequence to letters applying the ASCII values.
- The outcome of this procedure is that we now have the original communication in its unencrypted version.

4. Suggestive methodology

Let's begin with a plaintext with the word "ENVIRONMENT" in it.

4.1. *Process for encryption*

Give every letter in the prime text an appropriate value from the ASCII range using the first stage of encryption (see Tables 1 and 2).

Table 1

Letter	ASCII range	Letter	ASCII range
E	69	N	78
N	78	M	77
V	86	E	69
I	73	N	78
R	82	T	84
O	79		

The original text is arranged as a discrete series of ASCII values by the second phase of the encryption approach, such as:

Table 2

F's	***values***	***F's***	***values***
F_1	69	F_7	78
F_2	78	F_8	77
F_3	86	F_9	69
F_4	73	F_{10}	78
F_5	82	F_{11}	84
F_6	79		

There are eleven terms in all. As an example, examine the exponential's normal growth.

$$e^{\beta t} = 1 + \frac{\beta t}{1!} + \frac{\beta^2 t^2}{2!} + \cdots,$$

$$t^2 e^{\beta t} = 1 + \frac{\beta t^3}{1!} + \frac{\beta^2 t^4}{2!} + \cdots$$

Consider the polynomial in accordance with the 3^{rd}stage of the encryption procedure.

$$h(t) = Ft^2 e^{\beta t}, \beta = 2.$$

$$h(t) = 69t^2 + 78\frac{2t^3}{1!} + 86\frac{2^2 t^4}{2!} + 73\frac{2^3 t^5}{3!} + 82\frac{2^4 t^6}{4!} + 79\frac{2^5 t^7}{5!} + 78\frac{2^6 t^8}{6!} + 77\frac{2^7 t^9}{7!} + 69\frac{2^8 t^{10}}{8!} + 78\frac{2^9 t^{11}}{9!} + 84\frac{2^{10} t^{12}}{10!}. (1)$$

Applying the KAJ-integral technique to both sides, we then get:

$$S_m\{h(t)\} = S_m\{Ft^2 e^{\beta t}\}$$

$$= \frac{69}{0!}\left(\frac{2!}{v^{n+3}}\right) + \frac{156}{1!}\left(\frac{3!}{v^{n+4}}\right) + \frac{344}{2!}\left(\frac{4!}{v^{n+5}}\right) + \frac{584}{3!}\left(\frac{5!}{v^{n+6}}\right) + \frac{1312}{4!}\left(\frac{6!}{v^{n+7}}\right) + \frac{2528}{5!}\left(\frac{7!}{v^{n+8}}\right) + \frac{4992}{6!}\left(\frac{8!}{v^{n+9}}\right) + \frac{9856}{7!}\left(\frac{9!}{v^{n+10}}\right) + \frac{17664}{8!}\left(\frac{10!}{v^{n+11}}\right) + \frac{39936}{9!}\left(\frac{11!}{v^{n+12}}\right) + \frac{86016}{10!}\left(\frac{12!}{v^{n+13}}\right). (2)$$

Assess the remainders r_k in the encryption process using step four of the encryption technique so that $r_k = M_k \bmod 500$, ask might be any of values in N. As $M_k$stands for $S_m\{h(t)\}$ coefficients that are stated in eq. (2) mentioned above, and modulo is chosen for any value; for example, modulo 500 is taken.

A new finite sequence of remainders $r_1, r_2, \cdots$, and $r_{11}$are created by using the stage described above in the manner specified below in step five of the encryption process (see table 3):

Table 3

$r_i, i = 1, 2, \ldots, 11$	**values**	**mod 500**
r_1	138	$500(0) + 138 = 138$
r_2	936	$500(1) + 436 = 436$
r_3	4128	$500(8) + 128 = 128$

r_4	11680	$500(23) + 180 = 180$
r_5	39360	$500(78) + 360 = 360$
r_6	106176	$500(212) + 176 = 176$
r_7	279552	$500(559) + 52 = 52$
r_8	709632	$500(1419) + 132 = 132$
r_9	1589760	$500(3179) + 260 = 260$
r_{10}	4392960	$500(8785) + 460 = 460$
r_{11}	11354112	$500(22708) + 112 = 112$

An encrypted text is introduced via the amounts of ASCII of the remainders$\{138, 436, 128, 180, 360, 176, 52, 132, 260, 460, 112\}$, as well as a collection of the quotients that were practiced to state the key, in the sixth step of the encryption process.

$Co_1 = 0, Co_2 = 1, Co_3 = 8, Co_4 = 23, Co_5 = 78, Co_6 = 212, Co_7 = 559, Co_8 = 1419, Co_9 = 3179, Co_{10} = 8785, Co_{11} = 22708.$

As a result, applying the values of ASCII of the remainders $r_1, r_2, \cdots,$ and r_{11} (got by click the Alt key of these remainders amounts applying the keyboard of computer), the prime text "ENVIRONMENT" is turned into the cipher text ‘èyÇ┤Ũ▒4äĄffip’.

4.2. *Procedure for decryption*

Use the provided key Co_k for $k = 1,2,3,4,5,6,7,8,9,10,11$ as $0, 1, 8,23, 78, 212, 559, 1419, 3179, 8785, 22708$ to decrypt the secret message provided and restore it to its original text. To accomplish this, enter these values in the relevant fields.

It has been pointed out to us that the encrypted text contains the numbers $138, 436, 128, 180, 360, 176, 52, 132, 260, 460, and\ 112$ in the form of the finite sequence

Using corresponding finite sequence of $r_1 = 138, r_2 = 436, r_3 = 128, r_4 = 180, r_5 = 360, r_6 = 176, r_7 = 52, r_8 = 132, r_9 = 260, r_{10} = 460$ and $r_{11} = 112$.

By using step 2 of the decryption method and the previous step, find the values of $M_1, M_2, \cdots,$, and so on up to M_{11}.The following values are obtained: $M_1 = 138, M_2 = 936, M_3 = 4128, M_4 = 11680, M_5 = 39360, M_6 = 106176, M_7 = 279552, M_8 = 709632, M_9 = 1589760, M_{10} = 4392960$ and $M_{11} = 11354112$.

Using equation (2), we get:

$$S_m\{h(t)\} = 138\left(\frac{1}{v^{n+3}}\right) + 936\left(\frac{1}{v^{n+4}}\right) + 4128\left(\frac{1}{v^{n+5}}\right) + 11680\left(\frac{1}{v^{n+6}}\right) + 39360\left(\frac{1}{v^{n+7}}\right) + 106176\left(\frac{1}{v^{n+8}}\right) + 279552\left(\frac{1}{v^{n+9}}\right) + 709632\left(\frac{1}{v^{n+10}}\right) + 1589760\left(\frac{1}{v^{n+11}}\right) + 4392960\left(\frac{1}{v^{n+12}}\right) + 11354112\left(\frac{1}{v^{n+13}}\right).$$

After performing the inverse of the KAJ-integral transform in the fourth step of the decryption process, we arrive at:

$$h(t) = (69)t^2 + (78)\frac{2t^3}{1!} + (86)\frac{2^2t^4}{2!} + (73)\frac{2^3t^5}{3!} + (82)\frac{2^4t^6}{4!} + (79)\frac{2^5t^7}{5!} + (78)\frac{2^6t^8}{6!} + (77)\frac{2^7t^9}{7!} + (69)\frac{2^8t^{10}}{8!} + (78)\frac{2^9t^{11}}{9!} + (84)\frac{2^{10}t^{12}}{10!}.$$

Place the coefficients of last equation in a finite sequence applying the fifth step of the decryption process. You could, for instance, take the following action: 69,78,86,73,82,79,78,77,69,78,84.

In step 6 of the decryption procedures, we restore the prime text "ENVIRONMENT" by using the values of ASCII to the integer numbers in the finite sequence and reversing them to letters.

Acknowledgement

The provided message is encrypted and decrypted using the KAJ-transformation technique of exponential functions with the amounts of ASCII. We utilized some of this transformation's beneficial elements in our work with cryptography. The algorithmic part is not at all challenging. The prime text in safety formula is allowed 500 since such operation requires a high value of modulus. This greatly increases the security of the encryption and decryption of data.

References

[1] D. Bhatta, Integral Transform and Their Applications, 2nd ed. Springer Science & Business Media, LLC (1985).

[2] D. Priya S, M. Amirtha, S. Kumar P., "Application of N-transform in Cryptography," *Int. J. Sci. Res. Rev.*, vol. 8, no. 1, pp. 2143-2147 (2019).

[3] H. K. Undegaonkar, "Security in Communication by using Laplace Transforms and Cryptography," *Int. J. Sci. Technol. Res.*, vol. 8, no. 12, pp. 3207-3209 (2019).

[4] K. H. Rosen, Discrete Mathematics and Its Applications, McGraw Hill (2012).

[5] L. Debnath and D. Bhatta, Integral Transforms and Their Applications, 2nd ed. Chapman & Hall/CRC (2006).

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

[7] E. A. Kuffi, S. A. Mehdi, and E. A. Mansour, "Color Image Encryption Based on New Integral Transform SEE," J. Phys.: Conf.

Ser. (2022). [Online]. Available: https://doi.org/10.1088/1742-6596/2322/1/012016.

[8] E. A. Mansour, E. A. Kuffi, and S. A. Mehdi, "Applying Complex SEE Transformation in Cryptography," *MJPS*, vol. 8, no. 2, pp. 99-104 (2021). [Online]. Available: https://doi.org/10.52113/2/08.02.2021/99-104.

[9] E. S. Abbas, E. A. Kuffi, and A. A. Jawad, "KAJ Transform and its application on Ordinary Differential Equations," *J. Interdiscip. Math.*, vol. 25, no. 5, pp. 1427-1433 (2022). [Online]. Available: https://doi.org/10.1080/09720502.2022.2046339.

[10] D. M. Burton, Elementary Number Theory, Tata McGraw Hill, New Delhi (2002).

[11] E. Kreyszig, Advanced Engineering Mathematics, John Wiley and Sons Inc. (1999).

[12] J. A. Buchmann, Introduction to Cryptography, Springer (2004).

[13] P. Semwal and M. K. Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing," *Int. J. Emerg. Technol.* (Special Issue NCETST), vol. 8, no. 1, pp. 746-750 (2017).

[14] A. Amiruddin, A. A. P. Ratna, and R. F. Sari, "Systematic review of internet of things security," *Int. J. Commun. Networks Inf. Secur.*, vol. 11, no. 2, pp. 248-255 (2019).

[15] S. K. Yadav and M. Kumar, "On Certain Attacks and Privacy-Protecting Coupon System," *Int. J. Theor. Appl. Sci.*, vol. 3, no. 2, pp. 79-87 (2011).

[16] T. M. Elzaki, "The New Integral Transform Elzaki Transform," *Glob. J. Pure Appl. Math.*, vol. 7, no. 1, pp. 57-64 (2011).

[17] W. Gao and M. R. Farahani, "The hyper-Zagreb index for an infinite family of nanostar dendrimer," *J. Discrete Math. Sci. Cryptography*, vol. 20, no. 2, pp. 515-523 (2017). [Online]. Available: https://doi.org/10.1080/09720529.2016.1220088.

[18] W. Gao, L. Shi, and M. R. Farahani, "Szeged Related Indices of TUAC6[p, q]," *J. Discrete Math. Sci. Cryptography,* vol. 20, no. 2, pp. 553-563 (2017). [Online]. Available: https://doi.org/10.1080/09720529.2016.1228312.

[19] H. Yang and X. Zhang, "The independent domination numbers of strong product of two cycles," *J. Discrete Math. Sci. Cryptography,* vol.

21, no. 7-8, pp. 1495-1507 (2018). [Online]. Available: https://doi.org/10.1080/09720529.2017.1316988.

[20] S. Ediz, İ. Çiftçi, M. Cancan, and M. R. Farahani, "On k-total distance degrees and k-total Wiener polarity index," *J. Inf. Optim. Sci.*, vol. 42, no. 7, pp. 1469-1477 (2021). [Online]. Available: https://doi.org/10.1080/02522667.2021.1896652.

[21] F. Afzal, S. Rukh, D. Afzal, M. R. Farahani, M. Cancan, and S. Ediz, "A study of non-commutative Von-Neumann regular rings," *J. Inf. Optim. Sci.,* vol. 42, no. 7, pp. 1425-1436 (2021). [Online]. Available: https://doi.org/10.1080/02522667.2021.1896650.

[22] A. H. Alwan, "Small Intersection Graph of Subsemimodules of a Semimodule," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2022, no. 1, pp. 15-22 (2022).

[23] S. Ediza, M. Cancana, and M. R. Farahani, "Eccentric Connectivity and Connective Eccentricity Indices of Generalized Petersen Graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.,* vol. 2021, no. 1, pp. 1-6 (2021).

[24] R. Ponraj, S. Prabhu, and M. Sivakumar, "Pair Mean Cordial Labeling of Total Graph of Some Graphs and Prism Related Graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.,* vol. 2024, no. 2, pp. 181-192 (2024).

[25] F. O. Oduol and I. O. Okoth, "Counting vertices among all noncrossing trees by levels and degrees," *Commun. Combinatorics Cryptogr. Comput. Sci.,* vol. 2024, no. 2, pp. 193-212 (2024).

Received May, 2024