Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 6s (2024)

Encryption and Decryption using Hill Cipher and Integral Transforms

Gobburi Rekha[1], V. Srinivas[2]
[1] Department of Humanities and Sciences, Malla Reddy College of Engineering and Technology
[2] Department of Mathematics, Osmania university

Article History:

Received: 26-05-2024

Revised: 16-07-2024

Accepted: 27-07-2024

Abstract:

We know that Hill Cipher is one of the regular methods that is used in cryptography for encryption and decryption of data using modular arithmetic under different modulus. Moreover, we have seen results using some integral transforms like Laplace transforms, Aboodh transforms and many more. This paper extracts the result of dual encryption and decryption with a combination of Hill Cipher and few integral transforms.

Introduction: In many circumstances, the sender wants to keep the message private from the public or from unauthorized users. Here, we combine Hill Cipher with Laplace and Kamal transforms to encrypt the message and apply their inverse transforms to decrypt it. In contrast to cipher text, which is a coded version of plaintext, the original message written by the user is referred to as plaintext.

Objectives: In this paper, we focus on two stages of encryption and two stages of decryption under modulo 255.

Methods: Using Hill Cipher with different transformation techniques, we have encrypted and decrypted the data. One is Hill Cipher with Laplace transform technique while the other is Hill Cipher with Kamal transform technique.

Results: In this paper, we see that the original text is transformed to cipher text which could be retrievable using some techniques.

Conclusions: This is a novel method that uses dual techniques to safeguard data: first, it encrypts the encrypted cipher text, and then it decrypts it again. The data is protected all along the way because the key that is transmitted to the recipient is very big and difficult to crack.

Keywords: Encryption, Decryption, Hill cipher, Laplace transform, Inverse Laplace transform, Kamal transform and Inverse Kamal transform.

1. Introduction

As security of information plays a crucial role, we discuss a dual encryption and decryption of data using Hill cipher with combination of Laplace transform and Kamal transform. The study of encrypted messages is known as cryptography. In many circumstances, the sender wants to keep the message private from the public or from unauthorized users. Information is protected using encryption, and the original message is unlocked using decryption. Integral transformations have a wide range of uses, especially in the realm of cryptography. In cryptography, hyperbolic functions such as sine, cosine,

exponential, polynomial, etc. are transformed using the Laplace, Elzaki, and Kamal methods. While Elzaki transform is used by [2] and Kamal Transform [9], [5, 6], [1] employ Laplace transform.

Here, we combine Hill Cipher with Laplace and Kamal transforms to encrypt the message and apply their inverse transforms to decrypt it. In contrast to cipher text, which is a coded version of plaintext, the original message written by the user is referred to as plaintext. Encryption, also known as the process of rendering information unintelligible, decryption, or the process of creating cipher, is referred to as cryptography. There are two components to the encryption and decryption process: the algorithm and the key. The use of the key for encryption and decryption makes cryptography safer. We need the following well-known formulas because in this study we will cover the uses of Laplace transforms and Kamal transform.

2. Definitions

Laplace Transform:

If $f(t)$ is a function defined for all positive values of t, then the Laplace Transform of $f(t)$ is defined as: $L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt$, provided that the integral exists. Here the parameter S is a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t)$.

Some standard results of Laplace transform

$L\{1\} = \frac{1}{s}$	$L^{-1}\{\frac{1}{s}\} = 1$
$L\{t^n\} = \frac{n!}{s^{n+1}}$	$L^{-1}\{\frac{1}{s^{n+1}}\} = \frac{t^n}{n!}$
$L\{e^{at}\} = \frac{1}{s-a}$	$L^{-1}\{\frac{1}{s-a}\} = e^{at}$
$L\{t^n f(t)\} = (-1)^n \frac{d^n}{ds^n} F(s)$	$L^{-1}\{\frac{d^n}{ds^n} F(s)\} = t^n f(t)\, ds$

Kamal Transform:

The Kamal transforms defined by the integral equation:

$K[f(t)] = G(v) = \int_0^\infty f(t)\, e^{\frac{-t}{v}}\, dt$, $t \geq 0$, $k_1 \leq v \leq k_2$, where k_1, k_2 may be finite or infinite.

Some standard results of Kamal transform

$K[1] = v$	$K^{-1}[v] = 1$
$K[t] = v^2$	$K^{-1}[v^2] = t$
$K[t^n] = n!\, v^{n+1}$	$K^{-1}[v^{n+1}] = \frac{t^n}{n!}$
$K[te^{at}] = \frac{v^2}{(1-av)^2}$	$K^{-1}[\frac{v^2}{(1-av)^2}] = te^{at}$

3. Methods

In this we discuss how to encrypt the original text into cipher text using the following steps.

Encryption Algorithm:

Step 1: Select the plain text and convert the text into numbers by assigning the values as A=1, B=2…. Z=26, Space=27, a=28, b=29, z=53.Arrange the plain text which transformed in numbers in matrix form of order nxn or mxn.

Step 2: Let the matrix be denoted by P.
Step 3: Define a key matrix whose inverse exists. Let A be the key matrix of order nxn which acts as encryption key and the inverse of the matrix A acts as decryption key.
Step 4: Let us define $E \equiv AP(mod\ 53)$ which is the first stage of encryption.
Step 5: Let us define the function $f(t) = \sum_{i=0}^{n} G_i\, t^2 \cosh t$, where G_i are constants.The values in E are taken as the coefficients in the function.

Step 6: Apply Laplace transform for the function $f(t)$.

That is, $L\{f(t)\} = G(s)$ which is the second level of encryption and adjust the coefficients in G(s) under modulo 255 and transform them into symbols using the ASCII values. Hence, the sender sends the cipher text along with the key r_i, where $r_i = (F_i - q_i) / 255$.

Now, we discuss how to decrypt the cipher text to original text using the following steps.

Decryption Algorithm:

Step 1: Transform the cipher text into numbers using the ASCII values. Now, using the cipher text which are transformed into numbers and the key we find the coefficients q_i using,

$q_i = F_i + 255r_i$.

Hence, $G(s) = \sum_{i=0}^{n} \frac{q_i}{s^{2i+3}}$.

Step 2: Apply inverse Laplace transform for $G(s)$ on both sides.

That is, $L^{-1}\{G(s)\} = L^{-1}\left\{\sum_{i=0}^{n} \frac{q_i}{s^{i+3}}\right\}$ which is the first level of decryption.

Hence, we get $L^{-1}\{G(s)\} = f(t)$.

Step 3: Now, write the coefficients of $f(t)$ in matrix form say E.

Step 4: Let $D \equiv A^{-1}E(\mathrm{mod}\ 53)$ which is the second level of decryption.

Step 5: Hence, we get D which is same as that of P. Therefore, on converting the values of the matrix D into symbols we get original plain text.

4. Results

To see how the algorithm works let us consider the following illustrations.

Example I. This illustration explains about Hill Cipher using Laplace integral transform.

Step 1. Let the plain text to be sent is **Environment Day.** Now convert the plain text into numbers by assigning A=1, B=2…. Z=26, space = 27, a=28, b=29…. z=53.

Therefore, the plaintext in the form of numbers is 5 41 49 36 45 42 41 40 32 41 47 27 4 28 52.

Step 2: Arrange the numbers in matrix form as $P = \begin{pmatrix} 5 & 41 & 49 & 36 & 45 \\ 42 & 41 & 40 & 32 & 41 \\ 47 & 27 & 4 & 28 & 52 \end{pmatrix}$.

Step 3: Let A = $\begin{pmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{pmatrix}$ be the encryption key and its inverse $A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ -2 & 3 & -4 \\ -2 & 3 & -3 \end{pmatrix}$ be the decryption key.

Step 4: **I stage of encryption**

Let $E \equiv AP \pmod{53}$.

$$\equiv \begin{pmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 5 & 41 & 49 & 36 & 45 \\ 42 & 41 & 40 & 32 & 41 \\ 47 & 27 & 4 & 28 & 52 \end{pmatrix} (\text{mod } 53).$$

$$E \equiv \begin{pmatrix} 77 & 108 & 43 & 124 & 220 \\ 72 & 67 & -6 & 88 & 175 \\ 5 & -14 & -36 & -4 & 11 \end{pmatrix} (\text{mod } 53).$$

$$\mathbf{E} = \begin{pmatrix} \mathbf{24} & \mathbf{2} & \mathbf{43} & \mathbf{18} & \mathbf{8} \\ \mathbf{19} & \mathbf{14} & \mathbf{47} & \mathbf{35} & \mathbf{16} \\ \mathbf{5} & \mathbf{39} & \mathbf{17} & \mathbf{49} & \mathbf{11} \end{pmatrix}.$$

Step 5: **II stage of encryption**

Now for the matrix E let us apply Laplace transform.

Let $f(t) = \sum_{i=0}^{14} t^2 G_i \, cosht$, where $cosht = 1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \frac{t^6}{6!} + \frac{t^8}{8!} + \cdots \ldots \ldots$

Here, n=14.

Therefore, $cosht = 1 + \frac{t^2}{2!} + \frac{t^4}{4!} + \frac{t^6}{6!} + \frac{t^8}{8!} + \frac{t^{10}}{10!} + \frac{t^{12}}{12!} + \frac{t^{14}}{14!} + \frac{t^{16}}{16!} + \frac{t^{18}}{18!} + \frac{t^{20}}{20!} + \frac{t^{22}}{22!} + \frac{t^{24}}{24!} + \frac{t^{26}}{26!} + \frac{t^{28}}{28!}$.

$f(t) = G_0 + G_1 \frac{t^2}{2!} + G_2 \frac{t^4}{4!} + G_3 \frac{t^6}{6!} + G_4 \frac{t^8}{8!} + G_5 \frac{t^{10}}{10!} + G_6 \frac{t^{12}}{12!} + G_7 \frac{t^{14}}{14!} + G_8 \frac{t^{16}}{16!} + G_9 \frac{t^{18}}{18!} + G_{10} \frac{t^{20}}{20!} + G_{11} \frac{t^{22}}{22!} + G_{12} \frac{t^{24}}{24!} + G_{13} \frac{t^{26}}{26!} + G_{14} \frac{t^{28}}{28!}$ Where $G_0 = 24, G_1 = 2, G_2 = 43, G_3 = 18,$ $G_4 = 8$, $G_5 = 19, G_6 = 14, G_7 = 47, G_8 = 35, G_9 = 16, G_{10} = 5, G_{11} = 39, G_{12} = 17, G_{13} = 49, G_{14} = 11.$

$f(t) = t^2 \left[24 + 2\frac{t^2}{2!} + 43\frac{t^4}{4!} + 18\frac{t^6}{6!} + 8\frac{t^8}{8!} + 19\frac{t^{10}}{10!} + 14\frac{t^{12}}{12!} + 47\frac{t^{14}}{14!} + 35\frac{t^{16}}{16!} + 16\frac{t^{18}}{18!} + 5\frac{t^{20}}{20!} + 39\frac{t^{22}}{22!} + 17\frac{t^{24}}{24!} + 49\frac{t^{26}}{26!} + 11\frac{t^{28}}{28!}\right].$

$f(t) = \left[24t^2 + 2\frac{t^4}{2!} + 43\frac{t^6}{4!} + 18\frac{t^8}{6!} + 8\frac{t^{10}}{8!} + 19\frac{t^{12}}{10!} + 14\frac{t^{14}}{12!} + 47\frac{t^{16}}{14!} + 35\frac{t^{18}}{16!} + 16\frac{t^{20}}{18!} + 5\frac{t^{22}}{20!} + 39\frac{t^{24}}{22!} + 17\frac{t^{26}}{24!} + 49\frac{t^{28}}{26!} + 11\frac{t^{30}}{28!}\right].$

Apply Laplace transform for f(t).

$L\{f(t)\} = L\left\{24t^2 + 2\frac{t^4}{2!} + 43\frac{t^6}{4!} + 18\frac{t^8}{6!} + 8\frac{t^{10}}{8!} + 19\frac{t^{12}}{10!} + 14\frac{t^{14}}{12!} + 47\frac{t^{16}}{14!} + 35\frac{t^{18}}{16!} + 16\frac{t^{20}}{18!} + 5\frac{t^{22}}{20!} + 39\frac{t^{24}}{22!} + 17\frac{t^{26}}{24!} + 49\frac{t^{28}}{26!} + 11\frac{t^{30}}{28!}\right\}.$

$L\{f(t)\} = 24\frac{2!}{s^3} + 2\frac{4!}{2!s^5} + 43\frac{6!}{4!s^7} + 18\frac{8!}{6!s^9} + 8\frac{10!}{8!s^{11}} + 19\frac{12!}{10!s^{13}} + 14\frac{14!}{12!s^{15}} + 47\frac{16!}{14!s^{17}} + 35\frac{18!}{16!s^{19}} + 16\frac{20!}{18!s^{21}} + 5\frac{22!}{20!s^{23}} + 39\frac{24!}{22!s^{25}} + 17\frac{26!}{24!s^{27}} + 49\frac{28!}{26!s^{29}} + 11\frac{30!}{28!s^{31}}.$

$L\{f(t)\} = \frac{48}{s^3} + \frac{24}{s^5} + \frac{1290}{s^7} + \frac{1008}{s^9} + \frac{720}{s^{11}} + \frac{2508}{s^{13}} + \frac{2548}{s^{15}} + \frac{11280}{s^{17}} + \frac{10710}{s^{19}} + \frac{6080}{s^{21}} + \frac{2310}{s^{23}} + \frac{21528}{s^{25}} + \frac{11050}{s^{27}} + \frac{37044}{s^{29}} + \frac{9570}{s^{31}}.$

Adjusting the values under modulo 255, we get

$48 \equiv 48 \bmod 255$

$24 \equiv 24 \bmod 255$

$1290 \equiv 15 \bmod 255$

$1008 \equiv 243 \bmod 255$

$720 \equiv 210 \bmod 255$

$2508 \equiv 213 \bmod 255$

$2548 \equiv 253 \bmod 255$

$11280 \equiv 60 \bmod 255$

$10710 \equiv 0 \bmod 255$

$6080 \equiv 215 \bmod 255$

$2310 \equiv 15 \bmod 255$

$21528 \equiv 108 \bmod 255$

$11050 \equiv 85 \bmod 255$

$37044 \equiv 69 \bmod 255$

$9570 \equiv 135 \bmod 255$

And the keys are 0,0,5,3,2,9,9,44,42,23,9,84,43,145,37.

Hence, the receiver receives the cipher text ***0CANSIóÒÕý<NUL×lUE‡*** along with key: 0,0,5,3,2,9,9,44,42,23,9,84,43,145,37.

Step 6: **I stage of decryption**

Transform the cipher text into numbers using the ASCII values along the key: 0,0,5,3,2,9,9,44,42,23,9,84,43,145,37.

Since, $q_i = F_i + 255r_i$.

we get,

$G(s) = \sum_{i=0}^{14} \frac{q_i}{s^{2i+3}}$.

$G(s) = \left\{\frac{48}{s^3} + \frac{24}{s^5} + \frac{1290}{s^7} + \frac{1008}{s^9} + \frac{720}{s^{11}} + \frac{2508}{s^{13}} + \frac{2548}{s^{15}} + \frac{11280}{s^{17}} + \frac{10710}{s^{19}} + \frac{6080}{s^{21}} + \frac{2310}{s^{23}} + \frac{21528}{s^{25}} + \frac{11050}{s^{27}} + \frac{37044}{s^{29}} + \frac{9570}{s^{31}}\right\}$.

Step 6: Apply inverse Laplace transform for $G(s)$

Hence, $L^{-1}\{G(s)\} = L^{-1}\left\{\frac{48}{s^3} + \frac{24}{s^5} + \frac{1290}{s^7} + \frac{1008}{s^9} + \frac{720}{s^{11}} + \frac{2508}{s^{13}} + \frac{2548}{s^{15}} + \frac{11280}{s^{17}} + \frac{10710}{s^{19}} + \frac{6080}{s^{21}} + \frac{2310}{s^{23}} + \frac{21528}{s^{25}} + \frac{11050}{s^{27}} + \frac{37044}{s^{29}} + \frac{9570}{s^{31}}\right\}$.

$= 48\frac{t^2}{2!} + 24\frac{t^4}{4!} + 1290\frac{t^6}{6!} + 1008\frac{t^8}{8!} + 720\frac{t^{10}}{10!} + 2508\frac{t^{12}}{12!} + 2548\frac{t^{14}}{14!} + 11280\frac{t^{16}}{16!} + 10710\frac{t^{18}}{18!} + 6080\frac{t^{20}}{20!} + 2310\frac{t^{22}}{22!} + 21528\frac{t^{24}}{24!} + 11050\frac{t^{26}}{26!} + 37044\frac{t^{28}}{28!} + 9570\frac{t^{30}}{30!}$.

$= 24t^2 + 2\frac{t^4}{2!} + 43\frac{t^6}{4!} + 18\frac{t^8}{6!} + 8\frac{t^{10}}{8!} + 19\frac{t^{12}}{10!} + 14\frac{t^{14}}{12!} + 47\frac{t^{16}}{14!} + 35\frac{t^{18}}{16!} + 16\frac{t^{20}}{18!} + 5\frac{t^{22}}{20!} + 39\frac{t^{24}}{22!} + 17\frac{t^{26}}{24!} + 49\frac{t^{28}}{26!} + 11\frac{t^{30}}{28!}$.

$L^{-1}\{G(s)\} = t^2\left[24 + 2\frac{t^2}{2!} + 43\frac{t^4}{4!} + 18\frac{t^6}{6!} + 8\frac{t^8}{8!} + 19\frac{t^{10}}{10!} + 14\frac{t^{12}}{12!} + 47\frac{t^{14}}{14!} + 35\frac{t^{16}}{16!} + 16\frac{t^{18}}{18!} + 5\frac{t^{20}}{20!} + 39\frac{t^{22}}{22!} + 17\frac{t^{24}}{24!} + 49\frac{t^{26}}{26!} + 11\frac{t^{28}}{28!}\right]$.

Therefore, $L^{-1}\{G(s)\} = f(t)$.

Step 7: **II stage of decryption**

Let the coefficients of $f(t)$ be written in matrix form.

Therefore, E = $\begin{pmatrix} 24 & 2 & 43 & 18 & 8 \\ 19 & 14 & 47 & 35 & 16 \\ 5 & 39 & 17 & 49 & 11 \end{pmatrix}$.

Step 8: Now we find D $\equiv A^{-1}E \pmod{53}$.

D $\equiv \begin{pmatrix} 1 & -1 & 0 \\ -2 & 3 & -4 \\ -2 & 3 & -3 \end{pmatrix}\begin{pmatrix} 24 & 2 & 43 & 18 & 8 \\ 19 & 14 & 47 & 35 & 16 \\ 5 & 39 & 17 & 49 & 11 \end{pmatrix} \pmod{53}$.

$\equiv \begin{pmatrix} 5 & -12 & -4 & -17 & -8 \\ -11 & -118 & -13 & -127 & -12 \\ -6 & -79 & 4 & -78 & -1 \end{pmatrix} \pmod{53}$.

D = $\begin{pmatrix} 5 & 41 & 49 & 36 & 45 \\ 42 & 41 & 40 & 32 & 41 \\ 47 & 27 & 4 & 28 & 52 \end{pmatrix}$.

The matrix D is same as matrix P.

Hence, on arranging the numbers in order we get 5 41 49 36 45 42 41 40 32 41 47 27 4 28 52 and on transforming into alphabets we get the plain text as **Environment Day.**

Example II. This illustration explains about Hill Cipher using Kamal integral transform.

Step 1: Let the plain text to be sent is **Pseudo Prime**.

Step 2: Transform the plain text into numbers using ASCII values.

Let $P = (80\ 115\ 101\ 117\ 100\ 111\ 32\ 80\ 114\ 105\ 109\ 101)$.

Arrange P in the matrix form

Hence $P = \begin{bmatrix} 80 & 115 & 101 \\ 117 & 100 & 111 \\ 32 & 80 & 114 \\ 105 & 109 & 101 \end{bmatrix}$.

Step 3: Let $A = \begin{bmatrix} -1 & -3 & 3 & -1 \\ 1 & 1 & -1 & 0 \\ 2 & -5 & 2 & -3 \\ -1 & 1 & 0 & 1 \end{bmatrix}$ be the matrix which acts as an encryption key whose inverse exists. Therefore, $A^{-1} = \begin{bmatrix} 0 & 2 & 1 & 3 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix}$ is the matrix which acts as a decryption key.

Step 4: **I Stage of encryption**

Let $E \equiv AP \pmod{255}$.

$$E \equiv \begin{bmatrix} -1 & -3 & 3 & -1 \\ 1 & 1 & -1 & 0 \\ 2 & -5 & 2 & -3 \\ -1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 80 & 115 & 101 \\ 117 & 100 & 111 \\ 32 & 80 & 114 \\ 105 & 109 & 101 \end{bmatrix} (\text{mod } 255).$$

$$\equiv \begin{bmatrix} -440 & -284 & 62 \\ 165 & 135 & 98 \\ -676 & -437 & -428 \\ 142 & 94 & 111 \end{bmatrix} (\text{mod } 255).$$

$$E = \begin{bmatrix} 70 & 226 & 62 \\ 165 & 135 & 98 \\ 89 & 73 & 82 \\ 142 & 94 & 111 \end{bmatrix}.$$

Step 5: **II Stage of encryption**

For further security purpose let us encode the above E matrix using Kamal integral transform

Let $f(t) = \sum_{i=0}^{11} G_i t^2 e^{2t}$.

Here , G_i are the coefficients which takes the values of matrix E.

$G_0 = 70, G_1$ =226,$G_2 = 62, G_3$ =165,$G_4 = 135, G_5$ = 98,$G_6 = 89, G_7$ =73,$G_8 = 82, G_9$ =142,

$G_{10} = 94, G_{11}$ =111.

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

Therefore, $e^{2t} = 1 + 2t + \frac{(2t)^2}{2!} + \frac{(2t)^3}{3!} + \frac{(2t)^4}{4!} + \cdots ..$

$f(t) = t^2\left[G_0 + G_1(2t) + G_2\frac{(2t)^2}{2!} + G_3\frac{(2t)^3}{3!} + G_4\frac{(2t)^4}{4!} + G_5\frac{(2t)^5}{5!} + G_6\frac{(2t)^6}{6!} + G_7\frac{(2t)^7}{7!} + G_8\frac{(2t)^8}{8!} + G_9\frac{(2t)^9}{9!} + G_{10}\frac{(2t)^{10}}{10!} + G_{11}\frac{(2t)^{11}}{11!}\right]$.

Where, $G_0 = 70, G_1 = 226, G_2 = 62, G_3 = 165, G_4 = 135, G_5 = 98, G_6 = 89, G_7 = 73, G_8 = 82,$ $G_9 = 142, G_{10} = 94, G_{11} = 111.$

$f(t) = t^2\left[70 + 226(2t) + 62\frac{(2t)^2}{2!} + 165\frac{(2t)^3}{3!} + 135\frac{(2t)^4}{4!} + 98\frac{(2t)^5}{5!} + 89\frac{(2t)^6}{6!} + 73\frac{(2t)^7}{7!} + 82\frac{(2t)^8}{8!} + 142\frac{(2t)^9}{9!} + 94\frac{(2t)^{10}}{10!} + 111\frac{(2t)^{11}}{11!}\right]$.

$= \left[70t^2 + 226(2t)t^2 + 62\frac{(2t)^2}{2!}t^2 + 165\frac{(2t)^3}{3!}t^2 + 135\frac{(2t)^4}{4!}t^2 + 98\frac{(2t)^5}{5!}t^2 + 89\frac{(2t)^6}{6!}t^2 + 73\frac{(2t)^7}{7!}t^2 + 82\frac{(2t)^8}{8!}t^2 + 142\frac{(2t)^9}{9!}t^2 + 94\frac{(2t)^{10}}{10!}t^2 + 111\frac{(2t)^{11}}{11!}t^2\right]$.

Apply Kamal transform on both sides

$K[f(t)] = K\left[70t^2 + 226(2t)t^2 + 62\frac{(2t)^2}{2!}t^2 + 165\frac{(2t)^3}{3!}t^2 + 135\frac{(2t)^4}{4!}t^2 + 98\frac{(2t)^5}{5!}t^2 + 89\frac{(2t)^6}{6!}t^2 + 73\frac{(2t)^7}{7!}t^2 + 82\frac{(2t)^8}{8!}t^2 + 142\frac{(2t)^9}{9!}t^2 + 94\frac{(2t)^{10}}{10!}t^2 + 111\frac{(2t)^{11}}{11!}t^2\right]$.

$= 70(2!)v^3 + 226(2)(3!)v^4 + 62(4)\frac{2^2}{2!}v^5 + 165(2^3)5!\frac{v^6}{3!} + 135(2^4)6!\frac{v^7}{4!} + 98(2^4)7!\frac{v^8}{5!} + 89(2^6)8!\frac{v^9}{6!} + 73(2^7)9!\frac{v^{10}}{7!} + 82(2^8)10!\frac{v^{11}}{8!} + 142(2^9)11!\frac{v^{12}}{9!} + 94(2^{10})12!\frac{v^{13}}{10!} + 111(2^{11})13!\frac{v^{14}}{11!}$

$= 140v^3 + 2712v^4 + 2976v^5 + 26400v^6 + 64800v^7 + 131712v^8 + 318976v^9 + 672768v^{10} + 1889280v^{11} + 7997440v^{12} + 12705792v^{13} + 35463168v^{14}$.

Adjusting the above coefficients under modulo 255 by taking $q_i \equiv p_i \pmod{255}$.

Here, $q_i's$ are

$140 \equiv 140 \pmod{255}$.

$2712 \equiv 162 \pmod{255}$.

$2976 \equiv 171 \pmod{255}$.

$26400 \equiv 135 \pmod{255}$.

$64800 \equiv 30 \pmod{255}$.

$131712 \equiv 132 \pmod{255}$.

$318976 \equiv 226 \pmod{255}$.

$672768 \equiv 78 \pmod{255}$.

$1889280 \equiv 240 \pmod{255}$.

$7997440 \equiv 130 \pmod{255}$.

$12705792 \equiv 162 \pmod{255}$.

$354631618 \equiv 58(\text{mod } 255)$.

Here p_i's are 140,162,171,135,30,132,226,78,240,130,162,58 which are converted to ASCII codes

Hence, the receiver receives the cipher text along with the key, $k_i = \frac{q_i - p_i}{255}$ where k_i's are 0,10,11,103,254,516,1250,2638,7408,31362,49826,1390712.

Step 6: **I stage of decryption**

To decrypt the message, let $q_i = p_i + 255k_i$.

We define $G(s) = \sum_{i=0}^{11} q_n v^{i+3}$

$G(s) = 140v^3 + 2712v^4 + 2976v^5 + 26400v^6 + 64800v^7 + 131712v^8 + 318976v^9 + 672768v^{10} + 1889280v^{11} + 7997440v^{12} + 12705792v^{13} + 35463168v^{14}$.

Apply inverse Kamal transform

$K^{-1}[G(s)] = K^{-1}[140v^3 + 2712v^4 + 2976v^5 + 26400v^6 + 64800v^7 + 131712v^8 + 318976v^9 + 672768v^{10} + 1889280v^{11} + 7997440v^{12} + 12705792v^{13} + 35463168v^{14}]$.

$= 140\frac{t^2}{2!} + 2712\frac{t^3}{3!} + 2976\frac{t^4}{4!} + 26400\frac{t^5}{5!} + 64800\frac{t^6}{6!} + 131712\frac{t^7}{7!} + 318976\frac{t^8}{8!} + 672768\frac{t^9}{9!} + 1889280\frac{t^{10}}{10!} + 7997440\frac{t^{11}}{11!} + 12705792\frac{t^{12}}{12!} + 35463168\frac{t^{13}}{13!}$.

$=\left[70t^2 + 226(2t)t^2 + 62\frac{(2t)^2}{2!}t^2 + 165\frac{(2t)^3}{3!}t^2 + 135\frac{(2t)^4}{4!}t^2 + 98\frac{(2t)^5}{5!}t^2 + 89\frac{(2t)^6}{6!}t^2 + 73\frac{(2t)^7}{7!}t^2 + 82\frac{(2t)^8}{8!}t^2 + 142\frac{(2t)^9}{9!}t^2 + 94\frac{(2t)^{10}}{10!}t^2 + 111\frac{(2t)^{11}}{11!}t^2\right]$.

$= t^2\left[70 + 226(2t) + 62\frac{(2t)^2}{2!} + 165\frac{(2t)^3}{3!} + 135\frac{(2t)^4}{4!} + 98\frac{(2t)^5}{5!} + 89\frac{(2t)^6}{6!} + 73\frac{(2t)^7}{7!} + 82\frac{(2t)^8}{8!} + 142\frac{(2t)^9}{9!} + 94\frac{(2t)^{10}}{10!} + 111\frac{(2t)^{11}}{11!}\right]$.

$= f(t)$.

Step 7: **II stage of decryption**

Now, the coefficients in f(t) are written in matrix form.

Let E$= \begin{bmatrix} 70 & 226 & 62 \\ 165 & 135 & 98 \\ 89 & 73 & 82 \\ 142 & 94 & 111 \end{bmatrix}$.

Let $D \equiv A^{-1}E(\text{mod } 255)$.

$D \equiv \begin{bmatrix} 0 & 2 & 1 & 3 \\ 1 & 1 & -1 & -2 \\ 1 & 2 & 0 & 1 \\ -1 & 1 & 2 & 6 \end{bmatrix}\begin{bmatrix} 70 & 226 & 62 \\ 165 & 135 & 98 \\ 89 & 73 & 82 \\ 142 & 94 & 111 \end{bmatrix}(\text{mod } 255)$.

$$D \equiv \begin{bmatrix} 845 & 625 & 611 \\ -138 & 100 & -144 \\ 542 & 590 & 369 \\ 1125 & 619 & 866 \end{bmatrix} (\text{mod } 255).$$

$$D = \begin{bmatrix} 80 & 115 & 101 \\ 117 & 100 & 111 \\ 32 & 80 & 114 \\ 105 & 109 & 101 \end{bmatrix} \text{which is same as P.}$$

Hence, the original message is retrieved as **Pseudo Prime**.

5. Conclusion

In most of the cases, Hill Cipher encryption and decryption can be easily hacked as it involves only one key. Hence, in this we discuss the results which includes dual encryption and decryption of data using Hill cipher with integral transforms like Laplace transforms and Kamal transforms where the receiver receives the cipher text along the key which acts as private key throughout cryptoanalysis process. Further, we can extend the results using other integral transforms like Ezaki, Aboodh, Mahgoub and many more.

References

[1] Jadhav Shaila Shivaji. And Hiwarekar A.P., Cryptographic Method Based on Laplace -Elzaki Transform, Journal of the Maharaja Sayajirao University of Baroda, ISSN:0025-0422, Vol-55, No. I (VIII), pp187- 191, (2021).

[2] Akinola Emmanuel Idowu, Alao Saheed, Oderinu Rasaq Adekola and Folorunsa Esther Omofa. An Application of Integral Transform Based method in Cryptograph, Asian Journal of Pure and Applied Mathematics, 3(1):13-18, 2021; Article No. AJPAM.518.

[3] Bhuvaneswari K. and Bhuvaneswari R., Application of Tarig transform in Cryptography, International Journal of creative research thoughts, Vol. 8, Issue 6 pp1878-1880, (June2020).

[4] CH Jayanthi, V Srinivas. Mathematical Modelling for cryptography using Laplace transform, International Journal of Mathematics Trends and Technology Vol 65, pp 10-15,2019.

[5] Hiwarekar A.P., Application of Laplace transform for Cryptography, International Journal of Engineering & Science Research, Vol-5, Issue-4, pp 129-135, (April 2015).

[6] Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), pp 1193-1197, (2012).

[7] Tarig M Elzaki, Salil M Elzaki, Elnour EA. On the new integral transform Elzaki transform fundamental properties investigations and applications, Global Journal of Mathematical Sciences: Theory and Practical. 2012;4(1):1-13.

[8] Naga Lakshmi G, Ravi Kumar B, Chandra Sekhar A. A Cryptographic Scheme of Laplace Transforms, Intr.J. Math. Arch.2011;2(12):2515-2519.

[9] Tarig. M. Elzaki., 2011, "The New Integral Transform Elzaki Transform ", Global Journal of Pure and Applied Mathematics ,7(1), pp 57-64.