Southeast Europe Journal of Soft Computing
Available online: http://scjournal.ius.edu.ba

ISSN 2233 – 1859

Vol 12, No. 2, September 2023, pp. 34-38

NOVEL CRYPTOGRAPHIC APPROACH BASED ON PDF AND CDF

[1]R. Narmada Devi, [1]Kala Raja Mohan and [1]Nagadevi Bala Nagaram

[1]Department of Mathematics
Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology,
Avadi, Chennai – 600062
Tamilnadu, India.
**Corresponding Author*:narmadadevi23@gmail.com

Article Info

Article history:

Article received on 09 10 2023

Received in revised form 30 10 2023

Keywords:

Cryptography, Encryption, ,
Decryption, PDF and CDF Matrix

ABSTRACT: Secret Information sharing is all time requirement in this internet world, especially in Electronic communications such as system security, smart card, mobile communications etc. Cryptography is based on transformation of multiple rounds of transformation of messages in the form of plain text as input into encrypted text message. Through suitable mathematical technique, secrecy of the information is maintained. Many researchers have shown their interest in making use of mathematical techniques in Cryptography. This paper proposes a cryptographic technique using PDF and CDF. In this, plain text message is transformed as cipher text using a single key is used for both encryption and decryption. Using this proposed method, the information is also shared in safe manner and an illustration is done.

1. INTRODUCTION

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. Cryptography is the practice and study of hiding information from all but those with the means or key to decode the message. Also the area of cryptography employs many different means of transforming normal data in to unreadable form. Cryptography mainly consists of encryption and decryption. Encryption is the transformation of data in to some unreadable form its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended even those who can see the encrypted data. Decryption is the reverse of encryption it is the transformation of encrypted data back in to some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a key depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. This paper describes an activity build around one of the techniques that illustrates an application of probability function to cryptography.

A. P. Hiwarekar in 2014 proposed two cryptographic technique applying Laplace Transform and Hyperbolic functions [1,3]. M. TuncayGencoglu in 2017 introduced a crytographic process involving Laplace Transform with Hyperbolic functions [2]. Dr. K. Hemant K. Undegaonkar introduced a secured communication method involving Laplace Transform [4]. S. Sujatha in 2013 made use of the application of Laplace Transform in the field of cryptography [5]. G. Nagalakshmi et al in 2020 involved Laplace Transform Laplace Transform using Asymmetric key for secured communication [7]. S. Dhingra et al proposed a network security method involving Laplace Transform [8]. M. Saha in 2017 utilized Laplace Mellin Transform in forming a cryptographic method for secured information sharing [9]. A. K. H. Sedeeg et al in 2016 formulated a new cryptographic algorithm applying Aboodh Transform [10]. Kala Raja Mohan et al in 2022 applied Bilinear Transform with Probability in identifying a secured information sharing algorithm and Laplace transform and hyperbolic tangent function in cryptography [11,13]. A. Meenakshi et al applied graph network in designing a crypographic algorithm [12]. This paper aims at developing a cryptographic algorithm using probability functions

In section 2, the methodology made use of in this crypto analysis are described. Section 3 and 4 represents the algorithm which is applied for encryption and decryption. The process of encryption and decryption are demonstrated with an example in section 5 and Section 6. The conclusion followed by references are given in the Section 7.

2. VARIOUS TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms based the number of keys that are employed for encryption and decryption, they are.

2.1. Secret Key Cryptography (SKC)

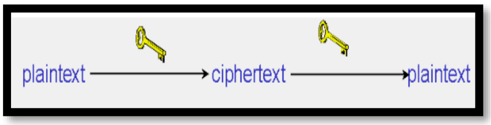
Cryptography in which a single key is used for both encryption and decryption.

It is also symmetric encryption.

Primarily used for privacy and confidentiality.

The sender uses the key to encrypt the plain text message and sends the cipher text message to the receiver.

The receiver applies the same key to decrypt the message and recover the plain text message.



2.2. Public Key Cryptography (PKC)

Cryptography in which a one key is used for encryption and another key used for decryption.

It is also called an asymmetric encryption.

Primarily used for authentication, non-repudiation, and key exchange.

2.3. Hash Functions

Cryptography has no key

It uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint.

Primarily used for message integrity.

2.4. Probability Density Function (PDF) and Cumulative Distribution Function (CDF)

Probability is a branch of mathematics that deals with the occurrence of a random event. A random variable is a rule that assigns a numerical value to each outcome in a sample space. Random variables may be either discrete or continuous. A random variable is said to be discrete if it assumes only specified values in an interval. Otherwise, it is continuous.

The Probability Density Function (PDF) defines the probability function representing the density of a continuous random variable lying between a specific ranges of values. In other words, the probability density function produces the likelihood of values of the continuous random variable. Sometimes it is also called a probability distribution function.

The probability density function is said to be valid if it obeys the following conditions:

f(x) should be non-negative for all values of the random variable.

The area underneath f(x) should be equal to 1.

The formula to calculate a pprobability density function of a continuous random variable is given as

$$\mathrm{P}(\mathrm{a} < X < b) = \int_{\mathrm{a}}^{\mathrm{b}} \mathrm{f(x)dx}, \mathrm{a} < x < b$$

The cumulative distribution function (CDF) F(x) describes the probability that a random variable X with a given probability distribution will be found at a value less than or equal to x. This function is given as $\mathrm{F(X)} = \mathrm{P(X \leq x)} = \int_{-\infty}^{\mathrm{x}} \mathrm{f(x)\ dx}$.

3. METHODOLOGY

In this proposed cryptographic algorithm, the idea of Secret Key Cryptography (SKC) is used and having the following procedure:

The information which is to be shared to the other person secretly is the plain text.

The encrypted message making use of the key specified for the process is the cipher text.

The process by which the plain text gets transformed into the cipher text is the cipher.

The process involved in converting plain text into secret message is encryption.

The reverse process of encryption is decryption, which convert secret message to plain text.

Find the Probability density function, cumulative distribution which are express as matrix.

4. ALGORITHM FOR ENCRYPTION USING PDF AND CDF

The steps to be followed in the process of encryption is as given below.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26	27			

Step 1: Convert the plain text message of length (n) in to a stream of numerals using the following above table.

Step 2: Form the mathematical terms likex^{n-1}, x^{n-2},… and constant term, where n is the number of the letter in the plain text message.

Step 3: Each term is multiplied with the numerals of the plain text message which is obtained in the step 1 in the order of left to right direction.

Step 4: Find the mathematical function f(x) using the terms existed in step 3 by considering equal intervals from 0 to n (number of letter in the plain text) and also by multiply suitable k such that f(x) becomes probability density function.

Step 5: Evaluate the cumulative density function F(x) from the pdf f(x) corresponding to each intervals using the formula as

$$F(x) = \int_a^x f(x)dx, a < x < b \qquad (1)$$

Step 6:Convert as matrix of order (n-1,n) in which the elements are the coefficients of the cumulative density function F(x) which are obtain in the step 5 for each intervals.

Step 7: Matrix attain in step 6 is consider as cipher text.

5. ALGORITHM FOR DECRYPTION USING PDF AND CDF

The decryption process involves the steps as specified below.

Step 1: Consider the matrix is obtained in the encryption process.

Step 2: From each row of the matrix, form a function with term x^n, x^{n-1},.and constant term, by multiplied its entries, that gives the cumulative distribution function for corresponding each intervals.

Step 3: Find the probability density function for each cumulative distribution function for corresponding each intervals using the formula

$$(x) = \frac{dF(x)}{dx}. \qquad (2)$$

Step 4: Consider the coefficient of each term of x^{n-1}, x^{n-2},… and constant term and after divide by the value of k in such way that f(x) is pdf for the given interval.

Step 5 : Obtain the corresponding numerals of the coefficient of the term into Alphabet using the table 1. The message formed from this is decoded message.

6. ILLUSTRATION OF ENCRYPTION PROCESS

In this section, the encryption process is illustrated using the text message "CAT" Consider the plain text message "CAT" convert as numerical equivalent assigned letter using above table 1.

Table 1

C	A	T
3	1	20

This message consists of 3 characters.That is, n =3. The mathematical terms are $3x^2$, x and the constant term = 20 are found. Then find a function f(x) by choosing value of $k = \frac{2}{45}$ such that f(x) is pdf which is defined as

$$f(x)=\begin{cases} \frac{6}{45}x^2, & 0<x<1 \\ \frac{2}{45}x, & 1<x<2 \\ \frac{40}{45}, & 2<x<3 \end{cases}$$

Calculate the corresponding cumulative distribution function F(x) of the above pdf function f(x) as follows:

Table 2

Interval	**PDF**	$\boldsymbol{F(x) = \int_a^x f(x)dx}$
$\boldsymbol{0 < x < 1}$	$\frac{6}{45}x^2$	$\int_0^x \frac{6}{45}x^2 dx$ $= \left(\frac{6}{45}\left(\frac{x^3}{3}\right)\right)_0^x$ $= \frac{2}{45}x^3$
$\boldsymbol{1 < x < 2}$	$\frac{2}{45}x$	$\int_0^1 \frac{6}{45}x^2 dx + \int_1^x \frac{2}{45}x dx$ $= \frac{x^2}{45} + \frac{1}{45}$
$\boldsymbol{2 < x < 3}$	$\frac{40}{45}$	$\int_0^1 \frac{6}{45}x^2 dx + \int_1^2 \frac{2}{45}x dx$ $+ \int_2^x \frac{40}{45} dx = \frac{40x}{45} - \frac{75}{45}$

Hence we get,

$$F(x) = \begin{cases} \frac{2}{45}x^3, & 0<x<1 \\ \frac{1}{45}+\frac{x^2}{45}, & 1<x<2 \\ \frac{40}{45}x-\frac{75}{45}, & 2<x<3 \end{cases}$$

Convert into the matrix of order (3,4) by considering the elements as its coefficient of cumulative distribution function $F(x)$. Hence the matrix is given as

$$\begin{pmatrix} \frac{2}{45} & 0 & 0 & 0 \\ 0 & \frac{1}{45} & 0 & \frac{1}{45} \\ 0 & 0 & \frac{40}{45} & \frac{-75}{45} \end{pmatrix}$$

This matrix of the cumulative distribution function is to be shared to the receiver as a cipher text message.

7. ILLUSTRATION OF DECRYPTION PROCESS

This section describes the decryption process involved with the example cited in section 5. Before proceeding with the decryption process,

Consider the matrix which is obtained in step 5 of section 5.

$$\begin{pmatrix} \frac{2}{45} & 0 & 0 & 0 \\ 0 & \frac{1}{45} & 0 & \frac{1}{45} \\ 0 & 0 & \frac{40}{45} & \frac{-75}{45} \end{pmatrix}$$

Form the cumulative distribution function for corresponding each intervals from each rows and it is given as

$$F(x)=\begin{cases} \frac{2}{45}x^3, & 0<x<1 \\ \frac{1}{45}+\frac{x^2}{45}, & 1<x<2 \\ \frac{40}{45}x-\frac{75}{45}, & 2<x<3 \end{cases}$$

Find the probability density function using cumulative distribution function of each intervals.

Table 3

Interval	**CDF**	$\boldsymbol{f(x) = \frac{dF(x)}{dx}}$
$\boldsymbol{0 < x < 1}$	$\frac{2}{45}x^3$	$\frac{d\left(\frac{2}{45}x^3\right)}{dx} = \frac{2}{45}(3x^2)$ $= \frac{6x^2}{45}$
$\boldsymbol{1 < x < 2}$	$\frac{x^2}{45} + \frac{1}{45}$	$\frac{d\left(\frac{x^2}{45} + \frac{1}{45}\right)}{dx} = \frac{2x}{45}$
$\boldsymbol{2 < x < 3}$	$\frac{40x}{45} - \frac{75}{45}$	$\frac{d\left(\frac{40x}{45} - \frac{75}{45}\right)}{dx} = \frac{40}{45}$

Hence we get, the pdf is

$$f(x)=\begin{cases} \frac{6}{45}x^2, & 0< x <1 \\ \frac{2}{45}x, & 1< x <2 \\ \frac{40}{45}, & 2< x <3 \end{cases}$$

Consider each of the coefficient of the function and divided by k and convert as numerals. Using the Table 1, convert the numerals as plain text message.

Table 4

Coefficient of the term of $f(x)$	$\frac{6}{45}$	$\frac{2}{45}$	$\frac{40}{45}$
Divided by $k=\frac{2}{45}$(Numerals)	3	1	20
Plain Text Message	C	A	T

8. CONCLUSION

A new cryptographic algorithm has been proposed by applying the probability density function and cumulative distribution function. This process involves plain text is transformed to matrices which was to be sharing cipher text. Then decryption is proceeded by using the properties of probability and then convert as plain text. Thus, this is a very safe procedure in cryptography. The procedure is also illustrated using the Word “CAT”.

REFERENCES

[1] A. P. Hiwarekar, “New mathematical modeling for cryptography,” Journal of Information Assurance and Security, 9, 027-033 (2014).

[2] M. TuncayGencoglu, “Cryptanalaysis of a New Method of Cryptography using Laplace Transform Hyperbolic Functions.” Communications in Mathematics and Applications, 8, 183-189 (2017).

[3] A. P. Hiwarekar, “A new method of Cryptography ussing Laplace transform of Hyperbolic functions,” International Journal of Mathematical Archive, 4, 208-213 (2013).

[4] K. Hemant K. Undegaonkar, “Security in Communication By Using Laplace Transform and Cryptography,” International Journal of Scientific & Technology Research, 8, 3207-3209 (2019).

[5] S. Sujatha, “Application of Laplace Transforms in Cryptography,” International Journal of Mathematical Archive, 4, 67-71 (2013).

[6] C. H. Jayanthi and V. Srinivas, “Mathematical Modelling for Cryptography using Laplace Transform,” International Journal of Mathematics Trends and Technology, 65, 10-15 (2019).

[7] G. Nagalakshmi, A. Chandra Sekhar and D. Ravi Sankar, “Asymmetric key Cryptography using Laplace Transform,” International Journal of Innovative Technology and Exploring Engineering, 9, 3083-3087 (2020).

[8] S. Dhingra, A. A. Savalgi and S. Jain, “Laplace Transformation based Cryptographic Technique in Network Security,” International Journal of Computer Applications, 136, 6-10 (2016).

[9] M. Saha, “Application of Laplace – Mellin Transform for Cryptography,” Raj Journal of Technology Research & Innovation, 5, 12-17 (2017).

[10] A. K. H. Sedeeg, M. M. AbdelrahimMahgoub, and M. A. Saif Saeed, “An Application of the New Integral “Aboodh Transform” in Cryptography,” Pure and Applied Mathematics Journal, 5, 151-154 (2016).

[11] Kala Raja Mohan, Suresh Rasappan, Regan Murugesan, Sathish Kumar Kumaravel and Ahamed A. Elngar, “Secret Information Sharing Using Probability and Bilinear Transformation”, Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science, 115-122 (2022).

[12] A. Meenakshi, J. Senbagamalar, and A. Neel Armstrong, “Encryption on Graph Networks”, Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science, 123-130 (2022).

[13] Kala Raja Mohan, Suresh Rasappan and Sathish Kumar Kumaravel, “Secret Information sharing Using Laplace Transform and Hyperbolic Tangent Function”, AIP Conference Proceedings 2516, 12003, 1-6, (2022).