Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 4 (2022) 49–53

Journal of the Nigerian Society of Physical Sciences

Jensen-Based New Cryptographic Scheme

S. A. Osikoya*, E. O. Adeyefa

Department of Mathematics, Faculty of Science, Federal University Oye-Ekiti, Ekiti State, Nigeria

Abstract

The surgent availability of data and the demand for more data to implement several technological products which heavily depends on data have made the issue of cyber attacks, a global threat, of great concern. To ensure the protection of information, the heart of every nation, the development of formidable techniques which contribute to the advancement of present schemes is crucial to combat the challenge. In this research work, a mathematical framework, from the idea of cryptography, is developed using Jensen polynomial. Jensen polynomial is used for the encryption algorithm, and the Laplace transform is used as a transformation tool to convert the plain text message to cipher text message. The decryption is a reversal which involves the use of structured mathematical techniques and the key for the message.

DOI:10.46481/jnsps.2022.325

Keywords: Jensen polynomial, Laplace transform, Cryptographic algorithm, Information security,cryptographic scheme

Article History :
Received: 31 July 2021
Received in revised form: 22 November 2021
Accepted for publication: 23 November 2021
Published: 28 February 2022

Communicated by: J. Ndam

1. Introduction

Cryptography has always played major role in the security of information. There are many existing cryptographic schemes which are being adopted for internet security measure. This research is to contribute to the new research direction of developing cryptographic schemes using Laplace transform as a transformation tool for encryption of text message from plain text to cipher text. In the existing literature, there are limitations imposed by the polynomials and functions adopted for the encryption. The integer coefficients, which play an important role in the encryption algorithm of the message, are restricted to the coefficients of the polynomials adopted for the schemes. This may open these schemes to brute force attack, or cryptanalytic attack, or both.

In [1], Hiwarekar introduced the application of Laplace transform for cryptographic scheme using hyperbolic function as the mathematical object for the transformation of the message into ciphertext using Laplace transform. The concept was further extended in [2] adopting the ASCII values and hyperbolic functions for the encryption of secret message using Laplace transform for conversion into ciphertexts. Adeyefa et al. introduced a new cryptographic scheme using Chebyshev polynomials and Laplace transform which further solidifies the idea introduced in [1]. The concept of cryptographic scheme developed with the aid of Laplace transform was applied to network security in [4] and [5]. All of the schemes developed by the authors aforementioned are symmetric key cryptography. As an extension of Laplace-based cryptography to public key cryptography, Nagalakshmi et al. in [9] implemented the concept of Laplace transform to ElGamal Scheme but this possesses an inherent computational problem at the decryption phase.
The symmetric schemes developed in he existing literature pos-

*Corresponding author tel. no: +234(0)8076344051
Email address: samuelabidemi2@gmail.com (S. A. Osikoya)

sess a unique problem. The functions and polynomials used by the authors are to generate integer coefficients for the Laplace transformation which plays an integral part of the schemes. But such coefficients which are restricted to the coefficients of the hyperbolic functions, exponential functions or polynomials which are well-known can expose such schemes to cryptanalysis attacks. In this research, Jensen polynomial which include an arithmetic function is adopted to overcome the problem inherent with other polynomials, exponential functions or hyperbolic functions used in the existing literature. The coefficients of Jensen polynomial are generated through the arithmetic function, thus making the coefficients unrestricted by the polynomial. This non-restriction of integer coefficients makes the algorithm developed using Jensen polynomials more robust and versatile. Jensen polynomials permit the use of any arithmetic function thus making it more reasonable for practical usage compare to other functions and polynomials. The rest of the paper is summarized as follows. In Section 2, the basic mathematical tools required to develop the cryptographic algorithm is discussed. Section 3 introduces the crytographic algorithm with illustration, followed by an example to substantiate the algorithm. The paper is concluded in Section 4 in which further research directions are suggested for the readers.

2. Major Result Preliminaries

In this section, the mathematical tools needed for the development of the algorithm are presented.

2.1. Jensen Polynomial [8]

Jensen polynomial of degree d and shift n of an arbitrary sequence $\{\alpha_k\}_{k=1}^{\infty}$ of real numbers is the polynomial

$$J_{\alpha}^{d,n} = \sum_{j=0}^{d} \binom{d}{j} \alpha(n+j) X^j \tag{1}$$

2.2. The Laplace Transform [7]

Let $f(t)$ be a function for $t \geq 0$. The Laplace transform of $f(t)$ denoted by $L[f(t)]$ or $F(s)$ is defined by the equation:

$$L[f(t)] = F(s) = \int_0^{\infty} e^{-st} f(t)\, dt \tag{2}$$

where $\in \mathfrak{R}$ or C, supposing the integral converges.
The inverse of the Laplace transform in (1) is defined as:

$$L^{-1}[F(s)] = L^{-1}\left(\int_0^{\infty} e^{-st} f(t)\, dt \right) \tag{3}$$

3. Methodology

The encryption function is the function in equation (1). For the purpose of this study, we shall slightly modify equation (1) to enable its adaptability for the encryption process of the text message. Define

$$f(x) = \sum_{j=1}^{d} \phi_j \alpha(n+j)\, x^j \tag{4}$$

where ϕ_j is the ASCII value of each string in the message. The required sequence to be chosen must be such that satisfies the following properties.

1. The range of $\{\alpha_k\}_{k=1}^{\infty}$ is the set of positive integers $Z^+ \subset \mathbb{R}$;
2. The sequence $\{\alpha_k\}_{k=1}^{\infty}$ is a non-decreasing sequence.
3. The *nth* term of the sequence should be a large number of about 128-bits.

The following subsections outline the steps involved in the cryptographic algorithm.

3.1. Encryption Algorithm

Let M be the message to be encrypted with length L. Suppose $\phi_1, \phi_2, \ldots, \phi_L$ are the strings in the message. The encryption of the message is outline in the following steps.
Step I: Obtain the ASCII value of each of the alphabets(and symbols) in the text message. Define an arbitrary sequence which satisfies the properties above. The degree of the polynomial is the length of the string to be encrypted. The shift n is is equivalent to the length of the message.
Step II: Obtain the Laplace transform of the function obtained in Step I. The numerators of the Laplace transform are saved as resultant values, R_j , for the message to be encrypted.
Step III: Obtain the cipher text by taking the modulo 52 of each of the resultant values, that is $(R_j + X) mod 52$, where X is a value known to Emmanuel and Samuel. The cipher presented using the alphabet system provided in Table 1.

Example 3.1. The message "Attack" is to be sent through a channel an eavesdropper has access to just like Emmanuel and Samuel who are to share the information. Define the arbitrary sequence:

$$\alpha(n) = 2^{2n} - 1$$

$$\alpha(n+j) = 2^{2n+2j} - 1$$

The Jensen polynomial is the equation

$$f(x) = \sum_{j=1}^{d} \binom{j}{d} \phi_j \left(2^{2n+2j} - 1\right) x^j$$

where ϕ_j is the ASCII value of each letter in the message. Therefore, the ASCII value of each letter in the message is, $\phi_1 = 65, \phi_2 = 116, \phi_3 = 116, \phi_4 = 97, \phi_5 = 99, \phi_6 = 107$. Choose$n = 13$. Then the encryption function is computed in the simplest form as:

$$\begin{aligned} f(x) = {} & 104689827450x + 1868310792020x^2 \\ & + 9964324124400x^3 + 24996709661265x^4 \\ & + 40819369180590x^5 + 29411936042901x^6 \end{aligned} \tag{5}$$

Table 1: The alphabet system for the encryption and decryption

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	0	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m
26	27	28	29	30	31	32	33	34	35	36	37	38
n	0	p	q	r	s	t	u	v	w	x	y	z
39	40	41	42	43	44	45	46	47	48	49	50	51

Take the Laplace transform of the function above.

$$L[f(x)] = \frac{104689827450}{s^2} + \frac{3736621544040}{s^3} + \frac{59785944746400}{S^4} + \frac{599921031870360}{s^5} + \frac{4898324301670800}{s^6} + \frac{21176593950888720}{s^7} \tag{6}$$

The resultant values are obtained from the last equation are presented in Table 2. Next, the cipher text are obtained with the equation, $\phi_j^c = \left(R_j + X\right) mod 52$, where $X = 17.\phi_1^c = 43, \phi_2^c = 25, \phi_3^c = 45, \phi_4^c = 9, \phi_5^c = 17, \phi_6^c = 49$. Using the English letters presented in the Table 1, we obtain the cipher text "rZtJRx" with the key: 2013265912, 71858106616, 1149729706661, 11536942920584, 94198544262900, 407242191363244.

Table 2: The resultant values from the Laplace transform

R_1	R_2	R_3
104689827450	3736621544040	59785944746400
R_4	R_{15}	R_6
599921031870360	4898324301670800	21176593950888720

3.2. Decryption Algorithm

The following steps describe the encryption phase of the cryptographic scheme.
Step I: Obtain the resultant value of each string in the cipher text received with the equation:

$$R_i = 52k_i + c_i - X$$

Step II: Expand equation (1) in terms of the $\phi_i' s$.
Step III: The ASCII values of the original message, that is the plain text, is computed using the equation:

$$\phi_i = \frac{R_i}{coeff_i * i!} \tag{7}$$

where $coeff_i * i!$ is the coefficient of R_i in the equation obtained in Step II.

Using the steps outlined in the decryption algorithm, the resultant values in Table 2 are obtained. Next, equation (1) is expanded in terms of the $\phi_i s$ to obtain:

$$\begin{aligned} f(x) &= \sum_{j=1}^{6} \phi\binom{j}{6}\left(2^{26+2j} - 1\right)x^j \\ &= 1610612730\phi_1 + 16106127345\phi_2 \\ &+ 85899345900\phi_3 + 257698037745\phi_4 \\ &+ 412316860410\phi_6 + 274877906943\phi_6 \end{aligned} \tag{8}$$

The ASCII values of the plain text is obtained using the equation (8). Therefore,$\phi_1 = 65; \phi_2 = 116; \phi_3 = 116; \phi_4 = 97; \phi_5 = 99; \phi_6 = 107$. This implies the original message. The next example below is an improvement of the illustration given in the algorithm. The value of j chosen is 1024 bits. The value of n chosen is such that have only two primes as its prime factors. One of the primes is used in the arithmetic function while the other is used for the value of X. The message to be encrypted is 'Missile'. Although in the next example, we shall not use a 1024 bits number because of space. But we shall demonstrate the idea proposed.

Example 3.2. The Encryption Phase

First, the ASCII value of each letter in the message is obtained as follows:$M = 77, i = 105, s = 115, s = 115, i = 105, l = 108, e = 101$.

The encryption function in the illustration is used in this example.

$$f(x) = \sum_{j=1}^{d} \phi\binom{j}{d}\left(2^{2n+2j} - 1\right)x^j$$

The large integer chosen is the number, $Q = n = X = 221$ where $n = 13$, and $X = 17$. The Jensen polynomial for the encryption is computed as:

$$\begin{aligned} f(x) &= 144686710245x + 2367600719715x^2 \\ &+ 17287243362375x^3 + 69148973461575x^4 \\ &+ 151526446200675x^5 + 207807697648908x^6 \\ &+ 111050674405275x^7 \end{aligned} \tag{9}$$

The Laplace transform of equation (7) is next obtained:

$$L[f(x)] = \frac{144686710245}{s^2} + \frac{4735201439430}{s^3} + \frac{103723460174250}{s^4} + \frac{1659575363077800}{s^5} + \frac{18183173544081000}{s^6} + \frac{149621542307213760}{s^7} + \frac{559695399002586000}{s^8} \quad (10)$$

Thus, the resultant values of the message are stored in a computer memory in Table 3.

Table 3: The resultant values of the message.

R_1	R_2
144686710245	4735201439430
R_3	R_4
103723460174250	1659575363077800
R_5	R_6
18183173544081000	149621542307213760
R_7	
559695399002586000	

Next, the cipher text values are computed using the equation:

$$\phi_i' = (R_i + X)\, mod 52$$

where $X = 17$. The cipher text values and the respective keys are presented in Table 4. The corresponding cipher text is 'qLLdRVp'.

Table 4: The cipher text value and the corresponding key value.

ϕ_i	Cipher value	Key
ϕ_1	42	2782436735
ϕ_2	11	91061566143
ϕ_3	11	1994681926428
ϕ_4	29	31914910828419
ϕ_{15}	17	349676414309250
ϕ_6	21	2877337352061803
ϕ_7	41	10763373057742038

The Decryption Phase The resultant values of the original message are first obtained using the equation:

$$R_i = 52k_i + \gamma_i - X$$

where the γ_i is the respective cipher value of the cipher text. Substituting the respective cipher value and key, the resultant values in Table 3 are obtained.
The equation (4) is expanded in form of the $\phi_i s$ as follows:

$$f(x) = 1879048185\phi_1 x + 22548578283\phi_2 x^2 + 150323855325\phi_3 x^3 + 601295421405\phi_4 x^4 + 1443109011435\phi_5 x^5 + 1924145348601\phi_6 x^6 + 1099511627775\phi_1 x^7 \quad (11)$$

The plain text is obtained using equation (8) to get the $\phi_i.\phi_1 = 77, \phi_2 = 105, \phi_3 = 115, \phi_4 = 115, \phi_5 = 105, \phi_6 = 108, \phi_7 = 101$. These are the ASCII values of the original message. Hence, the decryption of the cipher text is obtainable.

4. Security Analysis

The plaintext is distinctively different from the ciphertext. The number of shifts cannot be calculated under this scheme as the same letter corresponds to different letter in the ciphertext thereby making the scheme secured against passive attack.
The developed scheme is secured against Chosen-plaintext Attack (CPA) which is an active type of attacks against cryptographic scheme. It involves the attacker's performance of encryption queries for plaintext of their choice and observation of resulting ciphertexts [10]. But the model developed involved the use of arithmetic function which may be kept secret between two parties thus protecting the transmission of the message. The knowledge of the arithmetic function does not guarantee the decryption of the message because the algorithm permits the addition of other keys in the steps thus making it harder for the attackers to break. Thus, the scheme is protected against CPA.
The length of message string is the same as the length of the ciphertext, thus making the issue of storage memory of little concern.

5. Conclusion

The mathematical modeling for cryptography using Jensen polynomials is free from the integer coefficients constraint associated with other polynomials like Chebyshev, Hermite, Legendre etc., or functions adopted for the encryption and decryption of text message. The possibility of using a suitable encryption through the Jensen polynomial makes the scheme more robust and versatile. The coefficient of the polynomial can be made as large as possible, a property which constitutes the security of the scheme against brute force attack. The complexity aspect of the algorithm is in the management of the key; as a key cannot be shared between more than two parties. This implies that a user will have about ten different keys in order to communicate with ten different people. Therefore, the concept introduced can be explored in different directions. First, the study can be used as the basis for public key cryptographic scheme, also known as asymmetric cryptography which overcome the issue of key management. This kind of extension will further help the implementation of the scheme for more practical use. Also, the research can be deeply explored to handle image encryption which it is hoped to be the next research, and the introduction of the concept to asymmeric key cryptography.

References

[1] A. P. Hiwarekar, "Application of Laplace transform for cryptographic scheme", Proceedings of world congress on Engineering, **1** (2013) 95.
[2] C. Jayanthi & V. Srinivas, "Mathematical Modeling for Cryptography using Laplace Transform",International Journal of Mathematical Trends and Technology, **2** (2019) 10.

[3] E. O. Adeyefa, L. S. Akinola, & O. D. Agbolade, "A New Cryptographic Scheme Using Chebyshev Polynomials", 2020 International Conference in Mathematics, Computer Engineering (ICMCECS), (2020) 3.
[4] A. Mittal & R.Gupta, "Kamal transformation based cyrptography technique in network security involving ASCII value", International Journal of Innovative Technology and Exploring Engineering, **8** (2019) 3448.
[5] D. Swati, A. Archana and J. Swati, "Laplace transformation based cryptographic technique in network security", International Journal of Computer Applications, **7** (2016) 10.
[6] M. Saha, "Application of Laplace-Mellin transform for cryptography", Rai Journal of Technology, Research and Innovation, **1** (2017) 12.
[7] B. D. Gupta, "Mathematical Physics", Ist ed., reprint, Ansari Road, New Delhi: India, (1980).
[8] M. Griffin, K. Ono, L. Rolen & D. Zagier, "Jensen Polynomials for the Riemann Zeta Function and Other Sequences", (2019).
[9] G. Nagalakshmi, S. A. Chandra, & S. N. Ravi, "An Implementation of ElGamal Scheme for Laplace Transform Cryptosystem", Indian Journal of Computer Science and Engineering (IJCSE, **1** (2020) 48.
[10] Jean-Philippe Aumasson, "Serious Cryptography: A Practical Introduction to Modern Encryption", (2018).