Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Application of N-transform in Cryptography

Dharshini Priya S [1]., Muthu Amirtha A[2] and Senthil Kumar P [3] *

[1,2] Department of Electronics and Instrumentation Engineering
[3] Department of Mathematics
[1,2,3] SNS College of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Cryptography is the study of understanding the secret messages. It is the art of converting plain text to encrypted data and also decrypting the data to get the original text using mathematical algorithms. There were several algorithms to achieve cryptography. This paper aims to encrypt and decrypt a message by using an integral transform N - transform and congruence modulo operator.

KEYWORDS : Caesar Cipher, N – transform, Encryption, Decryption

***Corresponding Author**

Dr. P. Senthil Kumar

Professor
Department of Mathematics
SNS College of Technology
Coimbatore – 641035.
Tamil Nadu. India.
Email : psenthil3@gmail.com

INTRODUCTION

Cryptography involves creating written or generated codes that allow information to be kept secret. It converts data into a format that is unreadable for an unauthorized user. Cryptography is mainly used for information security. An encryption algorithm or cipher, is a means of transforming plain text into cipher text under the control of a secret key. This process is called an encryption. The reverse process is called decryption. One of the earliest ciphers is called the Caesar cipher [6] or Shift cipher. In this scheme, encryption is performed by replacing each letter with the letter a certain number of places following the alphabet order. For example, if the key was three, then the plain text A would be replaced by the cipher text D, the next letter B would be replaced by E and so on. This is the process of making a message secret. This can be represented mathematically as $p(t) = (t + k) mod\ 26$. The function p that assigns to the non-negative integer t, $t \leq 26$, the integer in the set { 1,2,3,…26 } with $p(t) = (t + k) mod\ 26$.

In this paper, our research concept is to encrypt and decrypt a message by using a new integral transform N – transform.[9] N - transform is derived from the classical Fourier integral and is widely used in applied mathematics and engineering fields. This transform has deeper connection with Laplace and Sumudu transforms.[10] Based on the mathematical simplicity of this transform and its fundamental properties, we have to apply encryption and decryption algorithms to get the message in a simple way. Shaikh Jamir Salim, et.al [4] and Uttam Dattu Kharde [7] proposed a method to encrypt and decrypt a plain text message by using Elzaki transform. Abdelilah K. Hassan Sedeeg, et.al[5] proposed a method by using Aboodh transform.

N - TRANSFORM

Let $f(t)$ be a function defined for all $t \geq 0$. The N – transform of $f(t)$ is the function R(u,s) defined by

$$R(u,s) = N(f) = \int_0^\infty f(ut)\, e^{-st}\, dt \qquad (1)$$

provided the integral on the right side exists.

Some Standard Functions

For any function $f(t)$, we assume that the integral equation (1) exist.

(i) Let $f(t) = 1$ then N [1] = $\frac{1}{s}$

(ii) Let $f(t) = t$ then N [t] = $\frac{u}{s^2}$

(iii) Let $f(t) = t^2$ then N [t^2] = $\frac{2!u^2}{s^3}$

(iv) In general case, if n > 0, then N [t^n] = $\frac{n!u^n}{s^{n+1}}$

Inverse N - Transform

(v) $N^{-1}\left[\frac{1}{s}\right] = 1$

(vi) $N^{-1}\left[\frac{1}{s^2}\right] = \frac{t}{u}$

(vii) $N^{-1}\left[\frac{1}{s^3}\right] = \frac{t^2}{2\,!\,u^2}$

(viii) $N^{-1}\left[\frac{1}{s^{\,4}}\right] = \frac{t^3}{3\,!\,u^3}$ and so on.

When u = 1, all above functions and its inverses are same as Laplace transform.

ENCRYPTION ALGORITHM

(I) Assign every alphabet in the plain text message as a number like A = 1, B = 2, C = 3, … Z = 26, and space = 0

(II) Now replace each of the numbers t by $p(t) = (\,t + k)mod\ 26$

(III) Apply N- transform of polynomial $p(t)$

(IV) Find r_i such that $q_i \equiv r_i\ mod\ 26$ for each $i, 1\ \leq i\ \leq n$

(V) Consider a new finite sequence $r_1, r_2, r_3\ , \dots\ r_n$

(VI) The output text message is in cipher text.

DECRYPTION ALGORITHM

(I) Convert the cipher text in to corresponding finite sequence of numbers $r_1, r_2, r_3\ , \dots\ r_n$

(II) Take the inverse N- transform

(III) The coefficient of a polynomial $p(t)$ as a finite sequence

(IV) Now replace each of the numbers by $p^{-1}(t) = (\,t - k)mod\ 26$

(V) Translate the number of the finite sequence to alphabets. We get the original text message.

PROPOSED METHODOLOGY

Example 1 : Consider the plain text message is **" SUCCESS "** .

Encryption Procedure:

Now the corresponding finite sequence is 19,21,3,3,5,19,19. The number of terms in the sequence is 7. That is n = 7. Consider a polynomial of degree n – 1 with coefficient as the term of the given finite sequence. Hence the polynomial $p(t)$ is of degree 6. The above finite sequence shift by k letters (k = 4), this results 23,25,7,7,9,23,23.

Now the polynomial $p(t)$ is

$$p(t) = 23 + 25t + 7t^2 + 7t^3 + 9t^4 + 23t^5 + 23t^6$$

Apply N- transform on both sides

$$N\,[p(t)] = N\,\{\,23 + 25t + 7t^2 + 7t^3 + 9t^4 + 23t^5 + 23t^6\,\}$$

$$= 23\,N[1] + 25\,N[\,t\,] + 7\,N[\,t^2\,] + 7\,N[\,t^3\,] + 9\,N[\,t^4\,] + 23\,N[\,t^5\,] + 23\,N[\,t^6\,]$$

$$= 23\,.\frac{1}{s} + 25\,.\frac{u}{s^2} + 7.\frac{2\,!\,u^2}{s^3} + 7\,.\frac{3\,!\,u^3}{s^4} + 9.\frac{4\,!\,u^4}{s^5} + 23.\frac{5\,!\,u^5}{s^6} + 23.\frac{6\,!\,u^6}{s^7}$$

$$= 23\,.\frac{1}{s} + 25\,.\frac{1}{s^2} + 7.\frac{2\,!}{s^3} + 7\,.\frac{3\,!}{s^4} + 9.\frac{4\,!}{s^5} + 23.\frac{5\,!}{s^6} + 23.\frac{6\,!}{s^7} \qquad (\,u = 1\,)$$

$$= 23\,.\frac{1}{s} + 25\,.\frac{1}{s^2} + \frac{14}{s^3} + \frac{42}{s^4} + \frac{216}{s^5} + \frac{2760}{s^6} + \frac{16560}{s^7}$$

$$N\,[\,p(t)] = \sum_{i=0}^{6} \frac{q_i}{s^{i+1}}$$

where, q_1=23, q_2=25, q_3=14, q_4=42, q_5=216, q_6= 2760, q_7= 16560

Now, find r_i such that $q_i \equiv r_i \; mod\; 26$

⇒ $r_1 = 23$, $r_2 = 25$, $r_3 = 14$, $r_4 = 16$, $r_5 = 8$, $r_6 = 4$, $r_7 = 24$

Now consider a new finite sequence is $r_1, r_2, r_3, \ldots\, r_7$. That is, 23,25,14,16,8,4,24.

The corresponding cipher text is **“ WYNPHDX ”**

Decryption Procedure:

To recover the original message encrypted by Caesar cipher, the inverse p^{-1} is used. For that, take the finite sequence corresponding to cipher text is 23,25,14,16,8,4,24.

Let $N[p(t)] = 23\,.\frac{1}{s} + 25\,.\frac{1}{s^2} + \frac{14}{s^3} + \frac{42}{s^4} + \frac{216}{s^5} + \frac{2760}{s^6} + \frac{16560}{s^7}$

Take inverse N- transform on both sides, we get

$$p(t) = N^{-1}\,\{\,23\,.\frac{1}{S} + 25\,.\frac{1}{s^2} + \frac{14}{s^3} + \frac{42}{s^4} + \frac{216}{s^5} + \frac{2760}{s^6} + \frac{16560}{s^7}\,\}$$

$$= 23\,.\,1 + 25\,.\,t + 14\,.\frac{t^2}{2\,!} + 42.\frac{t^3}{3\,!} + 216.\frac{t^4}{4\,!} + 2760.\frac{t^5}{5\,!} + 16560.\frac{t^6}{6\,!}$$

$$\boldsymbol{p(t) = 23 + 25t + 7t^2 + 7t^3 + 9t^4 + 23t^5 + 23t^6}$$

The coefficient of a polynomial p(t) as a finite sequence 23,25,7,7,9,23,23. Now replace each of the numbers in the finite sequence by $p^{-1}(t) = (\,t - 4\,)mod\; 26$. The corrected new finite sequence is 19, 21, 3, 3, 5, 19, 19. Now by translating the numbers to alphabets. We get the original plain text message **“SUCCESS” .**

CONCLUSION

In this proposed work, a cryptographic scheme (Caesar cipher) with a new integral transform N-transform with congruence modulo operator is introduced and the results are verified. The algorithmic part is also simple. This procedure is allowed the plain text message in double time safety form. and thus the process of plain text security is strengthened as well as the process of decryption is simplified.

REFERENCES

1. Tarig. M.Elzaki., 2011, “The New Integral Transform El Zaki Transform”, Global Journal of Pure and Applied Mathematics, 2011; 7(1) : 57 – 64
2. Mohand M. Abdelrahim Mahgoub., 2016, “The New Integral Transform Mahgoub Transform”, Advances in Theoretical and Applied Mathematics, 2016; 11(4) : 391 – 398
3. Khalid Suliman Aboodh., 2013, “ The New Integral Transform Aboodh Transform Global Journal of Pure and Applied Mathematics, 2013; 9(1): 35 – 43
4. Shaikh Jamir Salim., and Mundhe Ganesh Ashruji., 2016, “ Application of El-zaki Transform in Cryptography”, Inter. Journal of Modern Sciences and Engineering Technology, 2016; 3(3) : 46 – 48
5. Abdelilah K. Hassan Sedeeg., Mohand M. Abdelrahim Mahgoub, and Muneer A.Saif Saeed., “An Application of the New Integral Aboodh Transform in Cryptography”, Pureand Applied Mathematics Journal, 2016; 5(5) : 151 – 154
6. Kenneth H. Rosan., Discrete Mathematics and Its Applications, Mcgraw Hill, 2012
7. Uttam Dattu Kharde., “ An Application of the Elzaki Transform in Cryptography”,Journal for Advanced Research in Applied Sciences, 2017; 4(5): 86 – 89
8. P. Senthil Kumar and S. Vasuki, “ An application of Mahgoub transform in Cryptography”, Advances in Theoretical and Applied Mathematics, 2018; 13(2) : 91 - 99
9. Zafar H Khan and Waqar A Khan, “N- transform – Properties and Applications”, NUST Journal of Engineering Sciences, 2008; 1(1): 127 – 133
10. G.K. Watugala, “ Sumudu Transform : a new integral transform to solve differential equations and control engineering problems” International Journal of Mathematical education in science and technology, 1993; 24(1) : 35 - 43