International Journal of Mathematical Archive-3(7), 2012, 2470-2473
Available online through www.ijma.info ISSN 2229 – 5046

APPLICATION OF LAPLACE TRANSFORMATION IN CRYPTOGRAPHY

P. D. Pansare*, S. P. Chalke and A. G. Choure
MAEER's MIT Arts, Commerce and Science College Alandi (D), Pune, India

(Received on: 15-05-12; Accepted on: 31-05-12)

ABSTRACT

Information protection has been an important part of human life from ancient time. In computer society, information security becomes more and more important for humanity and new technologies are emerging in an endless stream. Cryptography is one of the most important technique that provide data and information security by hiding it. It is done through mathematical technique.

In this paper we have derived an algorithm using Laplace transformation and congruence modulo operator to encrypt and decrypt a secrete message.

Key words*: Encryption, Decryption, Laplace transform, plain text, cipher text, key.*

1. INTRODUCTION

Human beings are always suspicious. When you send a message to someone, you always suspect that someone else will intercept it and read it or modify it before re-sending. And this suspicion or doubt is not at all baseless. This is because human beings are also nosy. There is always a desire to know about a secret message being sent/ received between two parties-with or without any personal, financial or political gains. It is no wonder then that the desire to send such a message to someone that nobody else can interpret is as old as human history.

Thus information security has become a very critical aspect of modern computing system. Information security is mostly achieved through the use of cryptography, a science based on abstract algebra.

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science art of transforming message to make them secure and immune to attacks. Following figure 1.1 shows the components involved in cryptography.

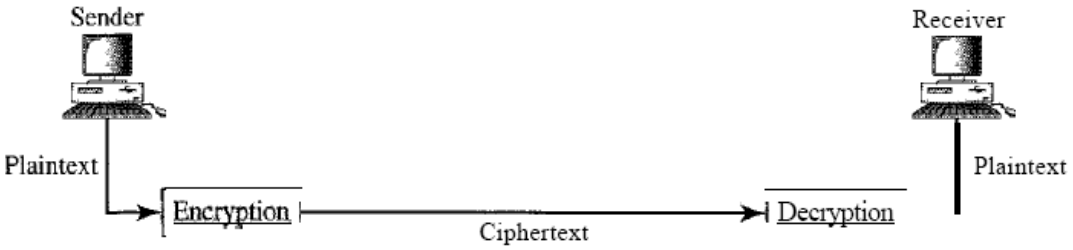

Figure 1.1

Definition: Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Definition: When plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Definition: Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

Every encryption and decryption process has two aspects: The algorithm and the key. The key is used for encryption and decryption that makes the process of cryptography secure.

Corresponding author: *P. D. Pansare**
MAEER's MIT Arts, Commerce and Science College Alandi (D), Pune, India

Definition: Laplace transform of a function $f(t)$ defined for all real numbers $t \geq 0$, is the function $F(s)$, defined by $F(s) = L\{f(t), s\} = \int_0^\infty e^{-st} f(t)\, d$

Definition: The expression of the form $p(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \cdots\cdots + a_{n-1} \cdot x + a_n$

where $a_0 \neq 0$, is called a polynomial of degree n.

PROPERTIES

Linearity: The Laplace transformation is a linear transformation, i.e.

$L\{a \cdot f(t) + b \cdot g(t)\} = a \cdot L\{f(t)\} + b \cdot L\{g(t)\}$, where a, b are constants.

Laplace and inverse Laplace transform of some elementary functions:

I. $L\{x^n, s\} = \frac{n!}{s^{n+1}}$, where n is positive integer.

II. $L^{-1}\left\{\frac{1}{s^{n+1}}\right\} = \frac{x^n}{n!}$

2. ENCRYPTION ALGORITHM

I. Treat every letter in the plain text message as a number, so that A=1, B=2, C=3, … Z=26, [space]=0.

II. The plain text message is organized as a finite sequence of numbers, based on the above conversion. For example our plain text is "THANK YOU".

Based on the above step; we know that, T=20, H=8, A=1, N=14, K=11, Y=25, O=15, U=21.

Therefore our plain text finite sequence is

20, 8, 1, 14, 11, 0, 25, 15, 21.

III. If $n+1$ is the number of term in the sequence; consider a polynomial of degree n with coefficients as the terms of the given finite sequence.

Above finite sequence contains 8+1 terms. Hence consider a polynomial $p(x)$ of degree 8.

$$p(x) = 20 + 8 \cdot x + 1 \cdot x^2 + 14 \cdot x^3 + 11 \cdot x^4 + 0 \cdot x^5 + 25 \cdot x^6 + 15 \cdot x^7 + 21 \cdot x^8$$

IV. Next take Laplace transform of a polynomial $p(x)$.

$$\begin{aligned} L\{p(x), s\} &= L\{20 + 8 \cdot x + 1 \cdot x^2 + 14 \cdot x^3 + 11 \cdot x^4 + 0 \cdot x^5 + 25 \cdot x^6 + 15 \cdot x^7 + 21 \cdot x^8\} \\ &= \frac{20}{s} + \frac{8 \times 1!}{s^2} + \frac{1 \times 2!}{s^3} + \frac{14 \times 3!}{s^4} + \frac{11 \times 4!}{s^5} + \frac{0 \times 5!}{s^6} + \frac{25 \times 6!}{s^7} + \frac{15 \times 7!}{s^8} + \frac{21 \times 8!}{s^9} \\ &= \frac{20}{s} + \frac{8}{s^2} + \frac{2}{s^3} + \frac{84}{s^4} + \frac{264}{s^5} + \frac{0}{s^6} + \frac{18000}{s^7} + \frac{75600}{s^8} + \frac{846720}{s^9} \\ &= \sum_{i=1}^{8+1} \frac{q_i}{s^i} \end{aligned}$$

V. Next find r_i such that $q_i \equiv r_i \bmod 26$, for each $i, 1 \le i \le n+1.$

Therefore,

$$q_1 = 20 \equiv 20 \bmod 26 \qquad q_2 = 8 \equiv 8 \bmod 26$$
$$q_3 = 2 \equiv 2 \bmod 26 \qquad q_4 = 84 \equiv 6 \bmod 26$$
$$q_5 = 264 \equiv 4 \bmod 26 \qquad q_6 = 0 \equiv 0 \bmod 26$$
$$q_7 = 18000 \equiv 8 \bmod 26 \qquad q_8 = 75600 \equiv 18 \bmod 26$$
$$q_9 = 846720 \equiv 4 \bmod 26$$

VI. Hence $q_i = 26k_i + r_i$.

Thus we get a key k_i for $i = 1, 2, 3, \ldots, n+1$

$$\therefore k_1 = 0, k_2 = 0, k_3 = 0, k_4 = 3, k_5 = 10, k_6 = 0, k_7 = 692, k_8 = 2907, k_9 = 32566.$$

VII. Now consider a new finite sequence $r_1, r_2, \ldots, r_{n+1}$

i.e. 20, 8, 2, 6, 4, 0, 8, 18, 4.

VIII. Now translating the numbers and space to alphabets.

Therefore our cipher text is “THBFD HRD” and key is 0, 0, 0, 3, 10, 0, 692, 2907, 32566.

3. DECRYPTION ALGORITHM

I. Consider the cipher text and key received from sender. In the above example cipher text is “THBFD HRD” and key is 0, 0, 0, 3, 10, 0, 692, 2907, 32566.

II. Convert the given cipher text to corresponding finite sequence of numbers $r_1, r_2, \ldots, r_{n+1}$.

20, 8, 2, 6, 4, 0, 8, 18, 4.

III. Let $q_i = 26k_i + r_i, \ \forall i = 1, 2, 3, \ldots, n+1$

$$\therefore q_1 = 26 \times 0 + 20 = 20 \qquad q_2 = 26 \times 0 + 8 = 8$$
$$q_3 = 26 \times 0 + 2 = 2 \qquad q_4 = 26 \times 3 + 6 = 84$$
$$q_5 = 26 \times 10 + 4 = 264 \qquad q_6 = 26 \times 0 + 0 = 0$$
$$q_7 = 26 \times 692 + 8 = 18000 \qquad q_8 = 26 \times 2907 + 18 = 75600$$
$$q_9 = 26 \times 32566 + 4 = 846720$$

IV. Let $F(p) = \sum_{i=1}^{n+1} \frac{q_i}{s^i}$

$$F(p) = \frac{20}{s} + \frac{8}{s^2} + \frac{2}{s^3} + \frac{84}{s^4} + \frac{264}{s^5} + \frac{0}{s^6} + \frac{18000}{s^7} + \frac{75600}{s^8} + \frac{846720}{s^9}$$

V. Now take Inverse Laplace transform of $F(p)$.

$$\therefore L^{-1}\{F(p), x\} = L^{-1}\left\{\frac{20}{s} + \frac{8}{s^2} + \frac{2}{s^3} + \frac{84}{s^4} + \frac{264}{s^5} + \frac{0}{s^6} + \frac{18000}{s^7} + \frac{75600}{s^8} + \frac{846720}{s^9}\right\}$$

$$p(x) = 20 \times \frac{x^0}{0!} + 8 \times \frac{x^1}{1!} + 2 \times \frac{x^2}{2!} + 84 \times \frac{x^3}{3!} + 264 \times \frac{x^4}{4!} + 0 \times \frac{x^5}{5!} + 18000 \times \frac{x^6}{6!} + 75600 \times \frac{x^7}{7!} + 846720 \times \frac{x^8}{8!}$$

$$p(x) = 20 + 8 \cdot x + 1 \cdot x^2 + 14 \cdot x^3 + 11 \cdot x^4 + 0 \cdot x^5 + 25 \cdot x^6 + 15 \cdot x^7 + 21 \cdot x^8$$

VI. Consider the coefficients of a polynomial $p(x)$ as finite sequence.

20, 8, 1, 14, 11, 0, 25, 15, 21.

VIII. Now translating the numbers of above finite sequence to alphabets.

We get the original plain text as "THANK YOU".

4. ACKNOWLEDGMENT

We would like to thank Prof. Dr. B. B. Waphare, Principal, MIT Arts, Commerce and Science College, Alandi (D), Pune, India for continuous motivation and support us to do research.

4. REFERENCES

[1] Atul Kahate, Cryptography and Network Security, Tata McGraw Hill Education Private Limited, New Delhi, India.

[2] Behrouz A. Forouzan, Data Communications and Networking, Fourth Edition, Tata McGraw Hill Education Private Limited, New Delhi, India.

[3] Stallings W., Cryptography and Network Security, Fourth Edition, Prentice Hall, 2005.

[4] I.N. Sneddon, The Use of Integral Transforms, Tata McGraw-Hill Publishing Company Ltd, New Delhi, 1972.

[5] A.H. Zemanian Generalized Integral Transformation, Interscience, New York, 1968.

[6] G. Naga Lakshmi, B. Ravi Kumar and A. Chandra Sekhar – A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2(12), 2011, 2515-2519.

Source of support: Nil, Conflict of interest: None Declared

