# CRYPTOGRAPHY – 'THE MATHEMATICS OF ENCRYPTION' BASED ON LAPLACE TRANSFORM

Dr. Vivek Parkash

*Asstt. Prof. of Mathematics*

*Dyal Singh College, Karnal (Haryana), India*

**Email ID**: lethal007@hotmail.com

**Accepted**: 06.05.2022 **Published**: 01.06.2022

**Keywords**: Cryptography, Laplace transform, ASCII Code, Cipher Text.

## Abstract

*Cryptography plays an indispensable and very crucial part in various fields of technology. Cryptography is an important tool that evades the threat against possible attacks by hackers during transmission of the message. Since the invent of communication system, information protection has been the first and foremost need of humans. In modern world inspired by technology, security of information and communication becomes all the more important for existence. Cryptography is one of the most important techniques used for protection of transmission of messages and protection of data. It is widely used in e-commerce, mobile communications, emails, business transactions, transmitting financial information, security of ATM cards, computer passwords etc. Cryptography means safeguarding the information by hiding it. It is done through mathematical technique or we can say Mathematical modelling. Laplace transform has many applications in various fields. Here we are going to discuss its application to cryptography. An attempt has been made in this paper to show how we can use Laplace transform of suitable polynomial for encrypting the plain text and apply corresponding inverse Laplace transform for decryption.*

## Paper Identification

**Introduction:**

Cryptography plays an indispensable and very crucial part in various fields of technology. Cryptography is an important tool that evades the threat against possible attacks by hackers during transmission of the message. The central objective of cryptography is to enable smooth and secured passage of the information being sent. Communications security is gaining importance as a result of the use of electronic communications in this technology driven world. Cryptography is the only practical means to provide security and is becoming a powerful tool in many applications for information security. So we can indeed say that 'Cryptography is the art of achieving security by enclosing messages to make them non readable'. Some common terms belonging to the process of Cryptography are as below:

1. Plain text: The original message, which written by user.
2. Cipher text: It is the coding form of plaintext.
3. Encryption: The process of obscuring information to make it unreadable without special knowledge.
4. Decryption: The process of converting cipher text into plaintext.
5. Cryptography: The art of devising the cipher i.e. the art of writing or solving codes.

**Laplace Transformation**:

Let $f(t)$be a function defined for $t \geq 0$.Then the Laplace transform of $f(t)$ is defined as $L\,f(t) = \int_0^\infty e^{-st} f(t)dt = F(s)$, where $e^{-st}$ is the kernel of the Laplace transformation and $s > 0$.

The inverse Laplace transform is given by

$$L^{-1}F(s) = f(t)$$

**Linearity Property:**

$$L\{a\,f(t) + bg(t)\} = aL\{f(t)\} + bL\{g(t)\}$$

Where $a$ and $b$ are constants.

**Laplace Transforms of Some Elementary Functions:** $L(t^n) = \frac{n!}{s^{n+1}}$

$$L^{-1}\left\{\frac{n!}{s^{n+1}}\right\} = t^n; \quad L(e^{at}) = \frac{1}{s-a}$$

$$L(te^{at}) = \frac{1}{(s-a)^2}; \quad L^{-1}\left\{\frac{1}{(s-a)^2}\right\} = te^{at}$$

**Methodology:**

a. Select the message to be sent, and convert into ASCII code. Let length of message be n.
b. The plain text message is arranged as a finite sequence of numbers, based on the above conversion. For example, if our plain text is "OK" then n=2.

The corresponding ASCII code of plain text is $O = 79\,, K = 75$

Let us take$C_0 = 79, \quad C_1 = 75$

Now take $f(t) = Cte^{2t}$

$$= t\{C_0.1 + C_1.2t\}$$
$$= 79t + 75.2t^2$$

Next take Laplace transform of both sides:

$$L\,f(t) = L\{79t + 150\,t^2\}$$
$$= L\{\,79t\} + L\{\,150\,t^2\}$$

$$= 79L(t) + 150L(t^2)$$
$$= 79.\frac{1}{s} + 150.\frac{2}{s^3}$$
$$= 79.\frac{1}{s} + 300.\frac{1}{s^3}$$

Take $D_0 = 79, D_1 = 300$

We now find the remainders as;

$D_0 \equiv r_0(mod\ 50), D_1 \equiv r_1(mod\ 50)$

$or\ \ 79 \equiv 29(mod\ 50)$ and $300 \equiv 0(mod\ 50)$

So,

$$r_0 = 29\ and \quad r_1 = 0$$

Take the keys as

$$k_0 = \frac{D_0 - r_0}{50} = \frac{79-29}{50} = 1$$
$$k_1 = \frac{D_1 - r_1}{50} = \frac{300-0}{50} = 6$$

Therefore, the cipher text derived from the plain text is $GS \quad NUL$ and the key is 1 6.

Now we convert the cipher text to a finite sequence of numbers as 29,0

Take $C_0' = 29, \ C_1' = 0$

Using $D_0 = 50k_0 + C_0' = 50.1 + 29 = 79$

$D_1 = 50k_1 + C_1' = 50.6 + 0 = 300$

Consider $C\{\frac{1}{(s-2)^2}\} = \frac{79}{s^2} + \frac{300}{s^3}$

Applying inverse transform on both sides, we have

$$f(t) = \ Cte^{2t} = L^{-1}\left\{\frac{79}{s^2} + \frac{300}{s^3}\right\}$$
$$= 79L^{-1}\left(\frac{1}{s^2}\right) + 300L^{-1}\left(\frac{1}{s^3}\right)$$

$$= 79.t + \frac{300}{2}.t^2$$

$$= 79.t + 150.t^2$$

$$= 79.t + 75.(2.t^2)$$

Now take$C_0 = 79, and \quad C_1 = 75,$ So we have the sequence of numbers as 79, 75.

Translating the above sequence as original plain text, we have the original message as "OK".

**Conclusion:**

We, thus, conclude that Laplace transform is used for protecting confidential and secret documents from unauthorized access. We encrypt the confidential data by creating codes and then decode the data using Inverse Laplace transform. So, application of Laplace transforms is quite extensive in cyber security.

**RÉFÉRENCIAS**


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

[2] Grewal B.S., "Higher Engineering Mathematics", Khanna Pub. Delhi

[3] Ramana B.V., "Higher Engineering Mathematics", Tata McGraw-Hills

[4] Alexander Stanoyevitch, Introduction to cyrptography with mathematical foundations and computer implementations, CRC Press, (2002).

[5] Laplace Transformation based Cryptographic Technique in Network, Security International Journal of Computer Applications (0975 – 8887) Volume 136 – No.7, February 2016.

[6] Applications of Laplace Transforms In Cryptography, International Journal of Mathematical Archive-4(3), 2013