Simulation and Analysis on Cryptography by Maclaurin Series and Laplace Transform

Anthony Adam Pranajaya, Iwan Sugiarto

***Abstract*—This research paper discussed about cryptography, which consists of the process of encryption of a plaintext to form a ciphertext, as well as the process of decryption and generation of keys. The plaintext, written in Roman or Latin alphabet is converted into a sequence of numbers using a certain rule, e.g., A into 0, B into 1, and so on. To encrypt the plaintext, a function which is representable as a Maclaurin series will be used; the numbers in the mentioned sequence are used as coefficients. Using the Laplace transform and modulus 26, one obtains the key and the ciphertext. The function will also be generalized to a family of functions of several parameters. The process of encryption can be iterated to generate more than one key. To decrypt the ciphertext, the inverse of Laplace transform will be used. The analysis on the use of parameters will also be discussed. The use of another alphabet aside from Roman or Latin will also be shown.**

***Index Terms*—analysis, cryptography, Laplace transform, Maclaurin series, simulation.**

I. Introduction

IN this modern times where usage of personal datas are used in the internet, informations are vulnerable to be stolen or used by unwanted third parties. This issue of information security had existed since thousands of years ago, and the study for this subject is called cryptography. Cryptography is a very old subject, but is very relevant to this day. As technology advances, cryptography becomes increasingly more imporant since the basis involves mathematical permutation that can be renewed or cracked. Fundamentally cryptography is used for data security, where the message that was sent cannot be read by anyone even through a public channel [1], [2], [3]. Cryptography also plays a role in breaking ciphers, like sir Alan Turing who created a machine to decipher the enigma cipher that was sent by the Nazi german in world war two [4]. Even though it is more often applied to the field of information technology, cryptography can also be used to solve cipher puzzles or codes. Another example is a letter written in symbols left by a murderer called the zodiac killer that were cracked in the year 2020 [5].

Cryptography usually involves the usage of an algorithm to encrypt an original message called a plaintext into an unreadable form called the ciphertext. It usually involves a process of encryption, decryption, and generation of keys. The process of encryption is a process in which a mathematical permutation is used to change a plaintext into a ciphertext. The process of encryption is usually accompanied by generation of keys where the keys are private information that comes from a part of the mathematical permutation. When someone sent a ciphertext, the receiver could decrypt using the key [1], [6], [2].

As of now, there are a lot of algorithms to encrypt and decrypt sensitive data that are categorized into a few types. First is symmetric cryptography in which the same key will be used to encrypt and to decrypt the data. The second is asymmetric cryptography in which two different but related keys are used to encrypt and decrypt the data. Another type of cryptography is hash cryptography in which no keys are used, but rather the key is mixed with the data[7]. In a symmetric cryptography, a mathematical permutation is used to encrypt a plaintext. It also uses the same permutation to decrypt a ciphertext. On the other hand, asymmetric cryptography uses a private key and a public key to encrypt a plaintext. Symmetric cryptography is usually used when speed is prioritized over advance safety. An example is the usage of credit card for transaction. While asymmetric cryptography are usually used when advance safety is more prioritized over speed. Asymmetric cryptography is usually used in digital signature, blockchain, and public key infrastructure [2]. In this research paper, author will use symmetric cryptography since it generates faster keys.

In the process of encryption, a Maclaurin series will also be used. Maclaurin series are power series to know the approximate value of a function, with that function being infinitely differentiable [8]. In the process of encryption, the Maclaurin series will first be decided and a coefficient will be multiplied to the series where the coefficient is a numerical value of an alphabet.

Furthermore, Laplace transform will be used on the series for encryption. Laplace transform is a useful tool that is often used in a lot of fields like electrical system analysis, communication system, hydrodynamics, nuclear physics, heat conduction, wave equation, solar systems, signal and system [3]. In mathematics, Laplace transform, named after Pierre-Simon Laplace, is an integral transform that change a function of a real variable t into a function of complex variable s. Transformation does have a lot of application in science and engineering because this can be used as a tool to solve differential equations. Specifically, this transformation could change a differential equation into an algebraic equation, and convolution into multiplication [9]. Moreover, encryption by Laplace transform could resist almost all types of attack on a symmetric encryption algorithm [1].

This research paper will show how to encrypt a plaintext using Laplace transform by first expanding a function into a Maclaurin series. The process of decryption will also be shown using the keys generated in the process of encryption and the inverse of Laplace transform. An iteration process will also be applied to encrypt multiple times and the results

Manuscript received August 31, 2021; revised March 15, 2022.

I. Sugiarto is an associate professor of the Faculty of Information Technology and Sciences, Parahyangan Catholic University, Ciumbuleuit Road, No.94, Hegarmanah, Cidadap, Bandung, Jawa Barat, Indonesia 40141 e-mail: (iwans@unpar.ac.id).

A. A. Pranajaya is a graduate of the Faculty of Information Technology and Sciences, Parahyangan Catholic University, Ciumbuleuit Road, No.94, Hegarmanah, Cidadap, Bandung, Jawa Barat, Indonesia 40141 e-mail: (anthonyadam787@gmail.com).

will also be analysed.

II. Definitions and methods

A. Laplace transform

Laplace transform is an integral transform that is often used in mathematics, physics, and other fields. It changes a time function into a complex function. In other words, Laplace transform transform a function of real variable t into a function of complex variable s, while the inverse of Laplace transform take a function of complex frequency domain and gives the function in the time domain [3].

If f is a function defined for every positive t, then the Laplace transform is defined as

$$F(s) = \mathcal{L}(f(t)) = \int_0^\infty e^{-st} f(t)dt \tag{1}$$

as long as the integral exists. The variable s is either real or complex number. Since the Laplace transform produces a function of variable s, the notation $F(s) = \mathcal{L}(f(t))$, is often used to denote the Laplace transform of $f(t)$. The capital $F(s)$ is often used to denote Laplace transform of a function named with a small letter that corresponds to $f(t)$ [9].

Laplace transform is defined as an improper integral. The integral is evaluated by taking the limit of a definite integral:

$$\int_0^\infty f(t)dt = \lim_{M\to\infty} \int_0^M f(t)dt, \tag{2}$$

or

$$\int_0^\infty f(t)dt = \lim_{\epsilon\to 0^+, M\to\infty} \int_\epsilon^M f(t)dt. \tag{3}$$

As an example, $F(s) = \mathcal{L}\{f(t)\}$ for $f(t) = 1$:

$$\begin{aligned} F(s) &= \int_0^\infty e^{-st} \cdot 1dt \\ &= \lim_{M\to\infty} \int_0^M e^{-st} \cdot 1dt \\ &= \lim_{M\to\infty} \left[-\frac{1}{s} e^{-st}\right]_0^M \\ &= -\frac{1}{s} \lim_{M\to\infty} \left(e^{-sM} - 1\right) \\ &= -\frac{1}{s}(0-1) \\ &= \frac{1}{s}, s > 0. \end{aligned} \tag{4}$$

Since limit does not exist at $s < 0$, that means $\mathcal{L}\{1\}$ is only defined at $s > 0$, so the domain of $\mathcal{L}\{1\}$ is $(0, \infty)$.

Theorem 2.1.1. *Linear characteristic of Laplace transform. Suppose $c_1, c_2, ..., c_n$ are constants, and the Laplace transform of $f_1(t), f_2(t), ..., f_n(t)$ exist. Then,*

$$\begin{aligned} &\mathcal{L}\{c_1 f_1(t) + c_2 f_2(t) + \cdots + c_n f_n(t)\} \\ &= c_1 F_1(s) + c_2 F_2(s) + \cdots + c_n F_n(s). \end{aligned} \tag{5}$$

Some Laplace transforms will be shown in Table I The following are some Laplace transforms for frequently encountered functions:

B. Power series

Power series in mathematics is an infinite series of the form

$$f(x) = \sum_{n=0}^{\infty} a_n (x-c)^n \tag{6}$$

with a_n representing the coefficient of the nth term, and c is a constant.

There are other form of power series such as the Taylor series that consist of infinite terms that contain the derivative at one point. The Taylor series was named from Brook Taylor that introduced the series in 1715. The sum of the first n terms of the Taylor series is a polynomial of degree n which is called the nth Taylor polynomial of the function. The Taylor polynomial is an approximation of the function, which generally gets better as n gets bigger. If the Taylor series of a function converges, its sum is the limit of the infinite series of Taylor polynomials [8].

A one dimensional Taylor series is an expansion of a real function f around $x = a$ given by

$$\begin{aligned} f(x) &= f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 \\ &+ \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n \\ &+ \cdots \end{aligned} \tag{7}$$

If $a = 0$, then the series (7) is called a Maclaurin series, which is:

$$\begin{aligned} f(x) &= f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \frac{f^{(3)}(0)}{3!}x^3 \\ &+ \cdots + \frac{f^{(n)}(0)}{n!}x^n + \cdots \end{aligned} \tag{8}$$

The following are the Maclaurin series of some functions:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \tag{9}$$

$$\sin(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1} \tag{10}$$

$$\sinh(x) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)!} x^{2n+1} \tag{11}$$

$$cos(x) = \sum_{n=0}^{\infty} \frac{(-1^n}{(2n)!} x^{2n} \tag{12}$$

$$\cosh(x) = \sum_{n=0}^{\infty} \frac{1}{(2n)!} x^{2n} \tag{13}$$

C. Cryptography

Cryptography, or cryptology (from an old greek word kryptós that means secret) is a practice and study of safe communication in the presence of a third party. The main focus in this research paper is for encrypting a ciphertext from a plaintext. These are the definitions for ciphertext, encryption, and decryption [1]:

TABLE I
LAPLACE TRANSFORM FOR SOME FUNCTIONS

$f(t)$	$F(s) = \mathcal{L}(f(t))$	$f(t)$	$F(s) = \mathcal{L}(f(t))$
1	$\frac{1}{s}$, $s > 0$	t^n, $n \in N$	$\frac{n!}{s^{n+1}}$, $s > 0$
e^{at}	$\frac{1}{s-a}$, $s > a$	$t^n e^{at}$, $n \in N$	$\frac{n!}{(s-a)^{n+1}}$
$\sin kt$	$\frac{k}{s^2+k^2}$	$e^{at} \sin kt$	$\frac{k}{(s-a)^2+k^2}$
$\cos kt$	$\frac{s}{s^2+k^2}$	$e^{at} \cos kt$	$\frac{s-a}{(s-a)^2+K^2}$
$\sinh kt$	$\frac{k}{s^2-k^2}$	$e^{at} \sinh kt$	$\frac{k}{(s-a)^2-k^2}$
$\cosh kt$	$\frac{s}{s^2-k^2}$	$e^{at} \cosh kt$	$\frac{s-a}{(s-a)^2-k^2}$
$t^n f(t)$, $n \in N$	$(-1)^n \frac{d^n}{ds^n} \mathcal{L}(f(t)) = (-1)^n \frac{d^n F}{ds^n}(s)$		

Definition 2.3.1. (Plaintext) Plaintext is a message or text that can be understood by the sender, receiver, and anyone that have an access to that message.

Definition 2.3.2. (Ciphertext) When a plaintext is codified using a certain scheme or algorithm, the result is called a ciphertext.

Definition 2.3.3. (Encryption and Decryption) Encryption changes a plaintext into a ciphertext, while decryption changes a ciphertext back into a plaintext. Every process of encryption and decryption have two aspects: the algorithm and the keys. Keys are what makes the process of cryptography safe.

There exist many kind of cryptography, in this subsection, a classic cryptosystem will be discussed. As a simple example, say Haru wanted to send a message to Shota. The plaintext will be decided as 'CHILDE'. Haru decided to shift forward every letter by 4 to obtain the ciphertext 'GLMPHI':

$$\text{CHILDE} \rightarrow \text{GLMPHI}$$

Shota accepts the ciphertext GLMPHI and shifted backward by 4 to obtain the original plaintext CHILDE:

$$\text{GLMPHI} \rightarrow \text{CHILDE}$$

In this simple scheme, the key is known by both the sender and receiver. Also, in this example, the key is the amount of shifts done. Generally, the keys are secret information or mathematical permutation for encrypting and decrypting a text.

In the example, there are 26 possible keys. This makes the system relatively easy to be cracked. A foreign individual could intercept the ciphertext and force all 26 keys until a readable message is found. Thus, the cryptosystem can be enhanced by first multiplicating a positive whole number that is relatively prime by 26 before shifting. Note that for every alphabets, a number is allocated for each letter. In another perspective, it is not important how to do this. In this research paper, to keep things simple, start with $A = 0$ as shown in Figure 1.

Mathematically,

$$x \mapsto ax + b \mod 26, \tag{14}$$

where $\gcd(a, 26) = 1$ with a note that gcd is the abbreviation for greatest common divisor. The value of a must be relatively prime to 26 so that decryption could be done. If a is not relatively prime to 26, then the mapping (14) is invertible. In this situation, the pair (a, b) is the key in the cipher. Since there are 12 numbers that are relatively prime to 26, there are 12 choice for a and 26 choice for b, by that there are $12 \cdot 26 = 312$ possible keys [10]. The modulus or mod 26 will be used so that the resulting number can be allocated into one of the 26 letters that was decided. There are many ways to make an algorithm more complex, the previous is just an example.

D. Method of encryption

A function of real variable t that has a Laplace Transform will first be decided, for example, $f(t) = t \sinh t$. This function is then expanded into a Maclaurin series. A plaintext will also be decided. This plaintext will be allocated into a number as in Figure 1. The plaintext will act as the coefficient of the function that is represented as a Maclaurin series. Afterward, Laplace transform will be applied to obtain a function of s variable. The numerator of the function will be modulated by 26, and the result is the ciphertext. The keys that are the results of dividing the numerators by 26 is also generated. The whole operation of encryption can be applied successively to obtain more form of ciphertexts [1].

Suppose, the chosen function is $f(t) = Gt^l \sinh rt$, where r and l are parameters, with j as the number of iterations. The method of encryption can be represented as in Theorem II-D

Theorem 2.4.1 *Plaintext represented by $G_{i,j-1}$, $i \in \{0, 1, 2, \ldots\}$, in the Laplace transform of $Gt^l \sinh rt$, can be converted into a ciphertext $G_{i,j}$, which is*

$$\begin{aligned} G_{i,j} &= G_{i,j-1} r^{2i+1} (2i+1+l)(2i+l)(2i+l-1) \\ &\quad \cdots (2i+2) \mod 26 \\ &= G_{i,j-1} r^{2i+1} (2i+1+l)(2i+l)(2i+l-1) \\ &\quad \cdots (2i+2) - 26k_{i,j} \\ &= q_{i,j} - 26k_{i,j} \end{aligned} \tag{15}$$

for $i \in \{0, 1, 2, \ldots\}$ with $q_{i,1} = G_{i,0} 2^{2i+1} (2i+3)(2i+2)$ and key

$$k_{i,j} = \frac{q_{i,j} - G_{i,j}}{26}. \tag{16}$$

E. Method of decryption

The ciphertext can be decrypted by the use of inverse Laplace transform and each respective keys to transform the function of s, $F(s)$, into $f(t)$. Its form can be represented as the following equation:

$$\begin{aligned} &G_{i,j-1} \\ &= \frac{26k_{i,j} + G_{i,j}}{r^{2i+1}(2i+1+l)(2i+l)(2i+l-1) \cdots (2i+2)} \end{aligned} \tag{17}$$

for $i \in \{0, 1, 2, \ldots\}$ and $j \in \{0, 1, 2, \ldots\}$.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Fig. 1. Alphabet

III. Simulation

A. Frequency of alphabets

A simulation of encryption will be shown using Laplace transform. The function expansion will be the same as in subsection II-D, that is $t^l \sinh rt$, where $r = l = 2$. Encryption will be done on a text [11] without iteration.

Ciphertext will not be able to be read that easily since the frequency of the letter A is so high. The frequency of occurence for each letter can be seen easier as bar graph in Figure 2.

The use of other functions with different texts [12], [13] will also be shown, such as $t^l \cosh rt$ and $t^l e^{rt}$, with $r = l = 2$, without iteration using a bar graph as shown in Figure 3 and Figure 4.

From the simulation using three different functions, the letters that are equivalent to the odd numbers did not appear at all because of the expanded form of the function itself that is the product of consecutive numbers. From equation (15) that is the general form of the hyperbolic sine function used, the numbers generated will always be even because the product of two consecutive natural numbers will always yield an even number. Therefore, letters that are equivalent to an odd number such as B, D, F, and so on cannot be generated.

The frequency of the letter A is also very high in comparison with the other letters. This is because of a few things. First, the chances of each letters appearing in a sentence are not uniform. In example, vocal letters like the letter A in Indonesian or English literature have the highest frequency. Second, the expanded form of the function only involves multiplication in the Maclaurin series. In example, a letter A will always yield a zero no matter how many times it is encrypted. Third, the usage of modulus 26. As an example, in the function $t^2 \sinh 2t$, if a letter N that is equivalent to 13 is encrypted using the expansion of Maclaurin series, then the result will be zero. In addition, suppose at the 25th index, since $2i + 2 = 52$ is a multiplication of 13, then the result will be zero when modulated by 26.

B. Change in parameter r and l

The change in parameter r and l changes the outcome of the ciphertext. In the following table, the varying value of r for the function $t^l \sinh rt$ with $l = 2$ will be shown.

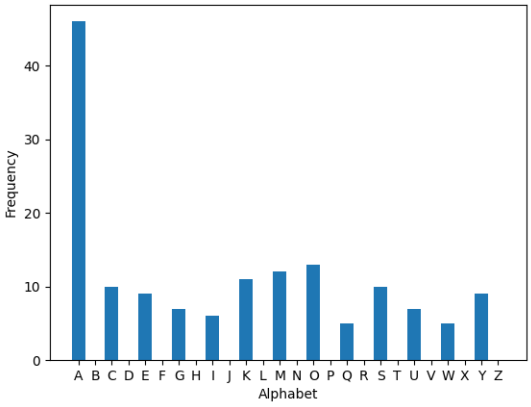

Fig. 3. Frequency of alphabet in ciphertext $t^2 \cosh 2t$

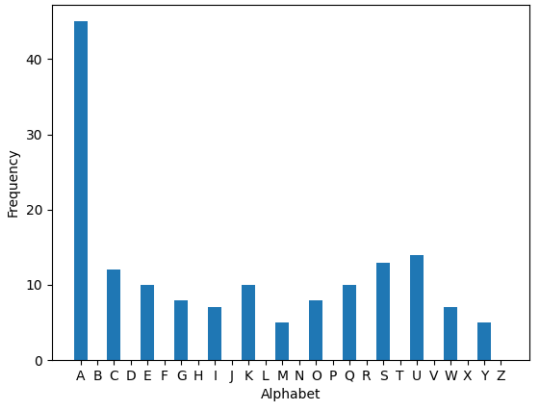

Fig. 2. Frequency of alphabet in ciphertext $t^2 \sinh 2t$

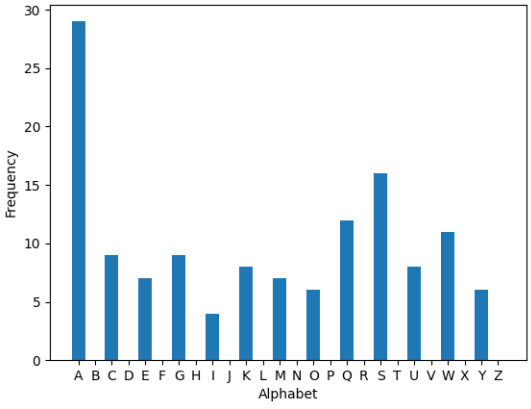

Fig. 4. Frequency of alphabet in ciphertext $t^2 e^{2t}$

TABLE II
ENCRYPTION OF $t^2 \sinh 2t$

Plaintext	Ciphertext
IN THE AGE OF GODS AND MONSTERS	SA EGQ AYU YM WOAG AAO KAAWECYU
I WISH NOT FOR DOMINION	S KOIC AEE QSG QAEYAUQA
I CANNOT WATCH FOLK SUFFER	S IAAAAY GAEQU AWUS GIACCU
I WILL HAVE ORDER	S KOCS AAOS SGQAK
TO CLEANSE AND DEFEND OUR PLACE	UE KCQAAMS AAQ AKCCAW AIC KMAIA
THAT WAS OUR FIRST CONTRACT	UCAU KAU EMU OIAGS OWAAMAKQ
FINAL CONTRACT IS SET IN STONE	IGAAS AEAOUACA UC WKS AA WEUAQ

TABLE III
ENCRYPTION OF $t^2 \cosh 2t$

Plaintext	Ciphertext
HEY SUNSHINE IN THE DARK	OKC GCAAMMAS MA WSK EAIA
CHANGING NIGHT SKY INTO DAY	EYAAYEAO ACOEA OWI CAMA CAY
KEEPING US IN YOUR WARM EMBRACE	UKWSGAA MO CA KAEO QAMY AIGEAMA
AS THE SEASONS TURNING RED	AG UYQ WAAOKAO AEOACAM AUS
I WANNA BE WITH YOU	Q QAAAA AS UCOE AIS
EVEN WHEN STARS START TO FALL	IUWA KKAA OIAGA OIAOS MA MAYQ
THIS WORLD WILL MISS A FLOWER	MYSG KUAEY MKKA SCGY A KASCEU

TABLE IV
ENKRIPSI $t^2 e^{2t}$

Plaintext	*Ciphertext*
WHAT WORDS WILL YOU TELL	SGAY ESKKU KEAA SYW WSGQ
IM CLUMSY BUT I HOPE	QO SSGIGC ECQ A AEWU
IT REACHES YOU PROPERLY	QU KQAKYWU SUA AQYKGSGQ
UNCERTAIN AND AFRAID	OASQWEASA AAA AUSAMU
REGRET AND BLAME THE PAST	IWCQWE AAM EMAAQ OWG WAMO
YET CONTINUE TO LOVE ME	WWC IMACSACC AA SYOG CO
EVEN IF THE WORLD ENDS	ISKA SM CGQ KUAAM SAYQ

TABLE V
CHANGE OF PARAMETER r IN $t^2 \sinh rt$

Plaintext	$r = 2$	$r = 13$	$r = 421$
VIRIDESCENT	SGUSMAUKSAW	AAAAAAAYWQK	GGICIMKEGAM
ARCHAIC	AQKGAAI	AAAAAAW	AQEGAYM
CHIVALRY	YCOSAAQQ	AAAAAAKQ	ICQSAQAQ

The same also applies to the parameter l, the change does not correspond to how big a value is, but to a specific value such as $l = 10$. It will also be shown in the following table using the function $t^l \sinh rt$ with $r = 2$ and other functions.

From the change of r in Table V, Table VII, and Table IX, the outcome is not decided by how big a value is, but rather to a specific value. That is because multiplication by specific value like $r = 13$ will yield multiplication of 26 that when modulated by 26 will gives out zero value. The change of l in Table VI, Table VIII, and Table X, also applies to specific value.

C. Change in parameter j

Suppose an encryption is iterated j times, where $j > 1$. The encryption will generate j set keys, where each set of keys will be used to for each respective ciphertext.

An encryption will be shown using function $t^l \sinh rt$ as in subsection II-D, with $r = l = 2$, to encrypt the word 'FROZEN' with iteration. From observation the iteration will repeat every 12 times. This is because of the expanded form of Maclaurin series and the use of modulus 26. The expanded form is the product of consecutive numbers that yield even numbers, thus the iteration will repeat every 12 times if modulated by 26. This also affects the keys that repeat. The use of other functions will also be shown.

As proof, let 2 be the first non-zero even number. The number is multiplied by 2 and modulated by 26. Then, the process will be repeated again and again, until the following sequence is formed

$$2 \quad 4 \quad 8 \quad 16 \quad 6 \quad 12 \quad 24 \quad 22 \quad 18 \quad 10 \quad 20 \quad 14 \quad 2 \quad \cdots.$$

From the sequence, the iteration repeats for every 12 times. When a number is modulated by 26, the result will always be smaller than 26. Every natural numbers that are smaller than 26 have the same factor as those in the sequence like 1, 2, 3, 5, 7, 11, and such when a number bigger than 1 is multiplied by 2 and applied modulus 26, the resulting number will enters the sequence. As an example, pick a prime number 127. If that number is multiplied by 2 and applied modulus 26, the result will be 20 which is one of the numbers in the sequence above.

D. Analysing the decryption

Previously the usage of parameter r, l, and j was shown. Those parameters affect directly to the key generated, because there are also a repeating pattern in the keys generated.

When a plaintext is encrypted into a ciphertext, a key will also be generated. If iterated j times, then j set keys will also be generated. From here, a ciphertext will be decrypted

TABLE VI
CHANGE OF PARAMETER l IN $t^l \sinh 2t$

Plaintext	$l = 2$	$l = 10$	$l = 24$
VIRIDESCENT	SGUSMAUKSAW	QAAAAAISAAA	YKYYWEKSSOO
ARCHAIC	AQKGAAI	AAAAAAY	AOQEAIU
CHIVALRY	YCOSAAQQ	EAAAAAWI	EMMMAIUG

TABLE VII
CHANGE OF PARAMETER r IN $t^2 \cosh rt$

Plaintext	$r = 2$	$r = 13$	$r = 421$
NOBLESSE	AWMIQWAS	AAAAAAEM	AOESEGQW
OBLIGE	CWCUYC	CAAAAA	COSGCE
MAIDEN	YASOQA	YAAAAA	YAGMEQ

TABLE VIII
CHANGE OF PARAMETER l IN $t^l \cosh 2t$

Plaintext	$l = 2$	$l = 10$	$l = 24$
NOBLESSE	AWMIQWAS	AYAAAAAQ	WIYASCSE
OBLIGE	CWCUYC	GYAAAA	OCGQOS
MAIDEN	YASOQA	UAAAAA	SAKQSG

TABLE IX
CHANGE OF PARAMETER r IN $t^2 e^{rt}$

Plaintext	$r = 2$	$r = 13$	$r = 421$
RETRACING	IWCQAKUAY	IAAAAAAAA	IQGQAEGEC
GLADIATOR	MCAMSACMQ	MAAAAAAAA	MSAMGAYMQ
MILLELITH	YSISWQUUC	YAAAAAAAA	YGYSQWGCS

TABLE X
CHANGE OF PARAMETER l IN $t^l e^{2t}$

Plaintext	$l = 2$	$l = 10$	$l = 24$
RETRACING	IWCQAKUAY	YIOAAAAAA	CIKOAQQOO
GLADIATOR	MCAMSACMQ	KWAAAAAAA	WCAUKASIY
MILLELITH	YSISWQUUC	UQEAAAAAA	SQUASCQYG

TABLE XI
ITERATION OF $t^2 \sinh 2t$ AND KEY

j	*Text*	Key	j	*Text*	Key
0	FROZEN	-	15	IWIOWA	8, 73, 620, 4253, 25993, 0
1	IQSOQA	2, 104, 723, 8861, 8664, 159744	16	SKOMKA	3, 135, 413, 4962, 47655, 0
2	SMMMMA	3, 98, 930, 4962, 34658, 0	17	IOSOOA	8, 61, 723, 4253, 21661, 0
3	IWIOWA	8, 73, 620, 4253, 25993, 0	18	SEMMEA	3, 86, 930, 4962, 30326, 0
4	SKOMKA	3, 135, 413, 4962, 47655, 0	19	IQIOQA	8, 24, 620, 4253, 8664, 0
5	IOSOOA	8, 61, 723, 4253, 21661, 0	20	SMOMMA	3, 98, 413, 4962, 34658, 0
6	SEMMEA	3, 86, 930, 4962, 30326, 0	21	IWSOWA	8, 73, 723, 4253, 25993, 0
7	IQIOQA	8, 24, 620, 4253, 8664, 0	22	SKMMKA	3, 135, 930, 4962, 47655, 0
8	SMOMMA	3, 98, 413, 4962, 34658, 0	23	IOIOOA	8, 61, 620, 4253, 21661, 0
9	IWSOWA	8, 73, 723, 4253, 25993, 0	24	SEOMEA	3, 86, 413, 4962, 30326, 0
10	SKMMKA	3, 135, 930, 4962, 47655, 0	25	IQSOQA	1, 7, 258, 1654, 3544, 0
11	IOIOOA	8, 61, 620, 4253, 21661, 0	26	SMMMMA	3, 98, 930, 4962, 34658, 0
12	SEOMEA	3, 86, 413, 4962, 30326, 0	27	IWIOWA	8, 73, 620, 4253, 25993, 0
13	IQSOQA	8, 24, 723, 4253, 8664, 0	28	SKOMKA	3, 135, 413, 4962, 47655, 0
14	SMMMMA	3, 98, 930, 4962, 34658, 0	29	IOSOOA	8, 61, 723, 4253, 21661, 0

multiple times using each respective set of keys. However, due to the influence of the parameter, the key mathematically can not be used to obtain a readable message.

In example, in Table XI, the first set of keys generated are 2, 104, 723, 8861, 8664, 159744. Those keys can be used by the inverse Laplace transform to decrypt a ciphertext for specific j. Suppose ciphertext 'IOIOOA' will be chosen in the 11th, 23rd, and so on j. The resulting plaintext will be 'FROZEN' which is the original plaintext.

Although it rarely happens, the plaintext generated will be close to the original plaintext if the first generated set of keys is used. This applies to all functions that have a repeating pattern due to the influence of the parameters. The first set of keys generated can be used directly to obtain a text close to the original, but to be fully certain, then the whole set must be used. The simulation for decryption will be shown for $t^2 \sinh 2t$, $t^2 \cosh 2t$, and $t^2 e^{2t}$.

IV. OTHER FORM OF SIMULATION

In this section, instead of a Roman or Latin alphabet, a portion of Japanese alphabet will be used as shown in table XV.

However, the usage of just those 46 letters will not be enough as there are other forms called the *dakuten*,

TABLE XII
ITERATION OF $t^2 \cosh 2t$ AND KEY

j	*Text*	Key	j	*Text*	Key
0	FROZEN	-	15	OEMMWA	1, 22, 258, 1378, 10633, 0
1	KKMEQA	0, 31, 258, 3446, 3544, 67584	16	CKOEKA	1, 7, 221, 1654, 19495, 0
2	UMOKMA	0, 18, 221, 551, 14178, 0	17	EMMKOA	0, 18, 258, 551, 8861, 0
3	OEMMWA	1, 22, 258, 1378 , 10633, 0	18	IEOMEA	0, 22, 221, 1378, 12406, 0
4	CKOEKA	1, 7, 221, 1654, 19495, 0	19	QKMEQA	0, 7, 258, 1654, 3544, 0
5	EMMKOA	0, 18, 258, 551, 8861, 0	20	GMOKMA	1, 18, 221, 551, 14178, 0
6	IEOMEA	0, 22, 221, 1378, 12406, 0	21	MEMMWA	0, 22, 258, 1378, 10633, 0
7	QKMEQA	0, 7, 258, 1654, 3544, 0	22	YKOEKA	0, 7, 221, 1654, 19495, 0
8	GMOKMA	1, 18, 221, 551, 14178, 0	23	WMMKOA	1, 18, 258, 551, 8861, 0
9	MEMMWA	0, 22, 258, 1378, 10633, 0	24	SEOMEA	1, 22, 221, 1378, 12406, 0
10	YKOEKA	0, 7, 221, 1654, 19495, 0	25	KKMEQA	1, 7, 258, 1654, 3544, 0
11	WMMKOA	1, 18, 258, 551, 8861, 0	26	UMOKMA	0, 18, 221, 551, 14178, 0
12	SEOMEA	1, 22, 221, 1378, 12406, 0	27	OEMWA	1, 22, 258, 1378, 10633, 0
13	KKMEQA	1, 7, 258, 1654, 3544, 0	28	CKOEKA	1, 7, 221, 1654, 19495, 0
14	UMOKMA	0, 18, 221, 551, 14178, 0	29	EMMKOA	0, 18, 258, 551, 8861, 0

TABLE XIII
ITERATION OF $t^2 e^{2t}$ AND KEY

j	*Text*	Key	j	*Text*	Key
0	FROZEN	-	15	OWOOWA	1, 1, 29, 61, 73, 0
1	KWWWWA	0, 7, 25, 153, 73, 672	16	CEWEEA	1, 10, 25, 86, 406, 0
2	UEQKEA	0, 10, 40, 135, 406, 0	17	EWQQWA	0, 1, 40, 24, 73, 0
3	OWOOWA	1, 1, 29, 61, 73, 0	18	IEOMEA	0, 10, 29, 98, 406, 0
4	CEWEEA	1, 10, 25, 86, 406	19	QWWWWA	0, 1, 25, 73, 73, 0
5	EWQQWA	0, 1, 40, 24, 73, 0	20	GEQKEA	1, 10, 40, 135, 406, 0
6	IEOMEA	0, 10, 29, 98, 406, 0	21	MWOOWA	0, 1, 29, 61, 73, 0
7	QWWWWA	0, 1, 25, 73, 73, 0	22	YEWEEA	0, 10, 25, 86, 406, 0
8	GEQKEA	1, 10, 40, 135, 406, 0	23	WWQQWA	1, 1, 40, 24, 73, 0
9	MWOOWA	0, 1, 29, 61, 73, 0	24	SEOMEA	1, 10, 29, 98, 406, 0
10	YEWEEA	0, 10, 25, 86, 406, 0	25	KWWWWA	1, 1, 25, 73, 73, 0
11	WWQQWA	1, 1, 40, 24, 73, 0	26	UEQKEA	0, 10, 40, 135, 406, 0
12	SEOMEA	1, 10, 29, 98, 406, 0	27	OWOOWA	1, 1, 29, 61, 73, 0
13	KWWWWA	1, 1, 25, 73, 73, 0	28	CEWEEA	1, 10, 25, 86, 406, 0
14	UEQKEA	0, 10, 40, 135, 406, 0	29	EWQQWA	0, 1, 40, 24, 73, 0

TABLE XIV
DECRYPTION BY THE FIRST SET OF KEYS

$t^2 \sinh 2t$	Plaintext	$t^2 \cosh 2t$	Plaintext	$t^2 e^{2t}$	Plaintext
IQSOQA	FROZEN	KKMEQA	FROZEN	KWWWWA	FROZEN
SMMMMA	GROZEN	CKOEKA	BROZEN	UEQKEA	KQOZEN
IWIOWA	FROZEN	UMOKMA	KROZEN	OWOOWA	HROZEN
SKOMKA	GROZEN	EMMKOA	CROZEN	CEWEEA	BQOZEN
IOSOOA	FROZEN	OEMMWA	HROZEN	EWQQWA	CROZEN
SEMMEA	GROZEN	IEOMEA	EROZEN	IEOMEA	EQOZEN
IQIOQA	FROZEN	QKMEQA	IROZEN	QWWWWA	IROZEN
SMOMMA	GROZEN	GMOKMA	DROZEN	GEQKEA	DQOZEN
IWSOWA	FROZEN	MEMMWA	GROZEN	MWOOWA	GROZEN
SKMMKA	GROZEN	YKOEKA	MROZEN	YEWEEA	MQOZEN
IOIOOA	FROZEN	WMMKOA	LROZEN	WWQQWA	LROZEN
SEOMEA	GROZEN	SEOMEA	JROZEN	SEOMEA	JQOZEN

TABLE XV
46 HIRAGANA LETTERS

あ	い	う	え	お	か	き
0	1	2	3	4	5	6
く	け	こ	さ	し	す	せ
7	8	9	10	11	12	13
そ	た	ち	つ	て	と	な
14	15	16	17	18	19	20
に	ぬ	ね	の	は	ひ	ふ
21	22	23	24	25	26	27
へ	ほ	ま	み	む	め	も
28	29	30	31	32	33	34
や	ゆ	よ	ら	り	る	れ
35	36	37	38	39	40	41
ろ	わ	を	ん			
42	43	44	45			

handakuten, and a few small forms as to make a sentence much more easier to be formed. Table XVI, table XVII, and table XVIII will also be used resulting in a total of 75 letters to be allocated.

TABLE XVI
20 HIRAGANA DAKUTEN FORMS

が	ぎ	ぐ	げ	ご
46	47	48	49	50
ざ	じ	ず	ぜ	ぞ
51	52	53	54	55
だ	ぢ	づ	で	と
56	57	58	59	60
ば	び	ぶ	べ	ぼ
61	62	63	64	65

Since there are 75 letters, modulus of 75 will be used

TABLE XVII
5 HIRAGANA HANDAKUTEN FORMS

ぱ	ぴ	ぷ	ぺ	ぽ
6 6	6 7	6 8	6 9	7 0

TABLE XVIII
4 HIRAGANA SMALL FORMS

っ	ゃ	ゅ	ょ
7 1	7 2	7 3	7 4

instead of 26. An encryption will be shown using the function $t^l \sinh rt$, where $r = l = 2$ with no iteration similar to section III using a text [13]. The text will only include *hiragana* letters, so any other type as in *kanji* will be in *hiragana* instead.

TABLE XIX
ENCRYPTION OF $t^2 \sinh 2t$ WITH HIRAGANA

	Plaintext
1	あなたがいることでとんなあしたも
2	あるいていけるひかりになるから
3	ほしがみえないことくなよるでも
4	しんじられるぼくらまたここで
5	わらえるひを
	Ciphertext
1	あごとゆぼんまげばあたああっあろ
2	あはべぶほぜあっんたふあどかま
3	ぐやのにととんりたんぼあどょた
4	ぢあぶめなんあぬすあまあざょ
5	ばかぢたなゃ

The result of the encryption, that is the ciphertext, can indeed be read, but it has no meaning whatsoever. It also shows that there might be another approach in the usage of this Laplace Transform method. It might be more prevalent in the usage of other foreign alphabets and also jumbling the allocations of the alphabets by making it not in the ascending order, and thus creating more keys.

V. WEAKNESSES

This section will talk about the possible weaknesses of the algorithm discussed in this paper. Suppose a cipher is given with no keys given. Assuming that the independent variables r, l, and j are given, and the method of encryption are known, a third person trying to decipher may try to brute force attack it by applying all possible form of ciphers for each of those alphabet.

For example, a cipher 'G Q Q C E', from the expansion of $t^l \sinh rt$ with $r = l = 2$ and $j = 1$ is given. The third person may refer to the cipher generated for each subsequent letters as in table XX. It is expected to have at least two possible plaintext as per discussed in the previous section due to repetition.

The first letter 'G' have two possible letter as in 'H' or 'U'. The second letter 'Q' have two possible letter as in 'E' or 'R'. This goes on until a plaintext can be formed. In this case, 'G Q Q C E' has a plaintext of 'H E L L O'. The same way can also be concluded if suppose iterations, where $j > 1$, is used.

However, it would be impossible to brute force attack if the algorithm or the variables are not known.

TABLE XX
ENCRYPTION OF LETTERS

Plaintext	Ciphertext	Plaintext	Ciphertext
AAAAA	AAAAA	NNNNN	AAAAA
BBBBB	MESME	OOOOO	MESME
CCCCC	YIKYI	PPPPP	YIKYI
DDDDD	KMCKM	QQQQQ	KMCKM
EEEEE	WQUWQ	RRRRR	WQUWQ
FFFFF	IUMIU	SSSSS	IUMIU
GGGGG	UYEUY	TTTTT	UYEUY
HHHHH	GCWGC	UUUUU	GCWGC
IIIII	SGOSG	VVVVV	SGOSG
JJJJJ	EKGEK	WWWWW	EKGEK
KKKKK	QOYQO	XXXXX	QOYQO
LLLLL	CSQCS	YYYYY	CSQCS
MMMMM	OWIOW	ZZZZZ	OWIOW

VI. CONCLUSIONS AND DISCUSSIONS

A. Conclusions

A message or a plaintext can be encrypted into a ciphertext using Maclaurin expansion of a function by Laplace transform. The function have to be infinitely differentiable such that it can be expressed as a Maclaurin series. Here are some concluding remarks:

1) The frequency of occurence for each letter in a generated ciphertext is not the same with the letter A being the most frequent. This is because the chance of each letter appearing in a sentence is not uniform; the use of modulus 26 also makes some of the generated ciphertext into zero value if it involves multiplication of 26.
2) The change of parameters r and l have a significant effect to the generated ciphertext. However, it relies on a specific value such as $r = 13$ and $l = 10$ that gives out more letter As, but not by how big the value is.
3) There are patterns in the iteration by the use of parameter j. This is because of the usage of modulus 26.
4) Using other foreign alphabets might be more effective under certain cases.

B. Discussion

Other series and transformation can be tested such as the Fourier series and Fourier transform in encryption as well as its inverse in decryption. Moreover, since this research paper uses a function that generates a set of keys, then a further test can be done to mathematically permutates the set into one set only. A second set of keys for each encryption can be made such as the one used in end-to-end-encryption. Moreover, another form of alphabet can be used that is not a Roman nor Latin alphabet.

REFERENCES

[1] A. P. Hiwarekar, "New mathematical modelling for cryptography," *Journal of Information Assurance and Security*, vol. 9, pp. 27–33, 2014.
[2] M. Sowmiya and S. Prabavathi, "Symmetric and asymmetric encryption algorithms in cryptography," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 355–357, 2019.
[3] C. H. Jayanti and V. Srinivas, "Mathematical modelling for cryptography using laplace transform," *International Journal of Mathematics Trends and Technology*, vol. 65, pp. 10–15, 2019.

[4] S. B. Cooper and J. V. Leeuwen, *An Introduction to Number Theory with Cryptography*, 1st ed. USA: Elsevier Science, 2013.
[5] D. Sadler, "Melbourne mathematician cracks zodiac killer's code, https://ia.acs.org.au/article/2020/melbourne-mathematician-cracks-zodiac-killer-s-code.html," 2020.
[6] A. M. Abdullah, "Advanced encryption standard algorithm to encrypt and decrypt data," Eastern Mediterranean University – Cyprus, 2017.
[7] G. Singh, "A study of encryption algorithms (rsa, des, 3des and aes) for information security," *International Journal of Recent Technology and Engineering*, vol. 67, p. 19, 2013.
[8] C. Canuto and A. Tabacco, *Mathematical Analysis I*, 2nd ed. Italy: Springer, 2015.
[9] M. L. Abell and J. P. Braselton, *Introductory Differential Equations*, 5th ed. US: Academic Press, 2018.
[10] J. S. Kraft and L. C. Washington, *An Introduction to Number Theory with Cryptography*, 2nd ed. New York: Chapman and Hall/CRC, 2018.
[11] Mihoyo, "Zhongli: The listener, https://www.hoyolab.com/genshin/article/94742," 2020.
[12] AIJ, "Before dawn, https://mojim.com/usy161957x6x3.htm," 2016.
[13] Uru, "Your presence, https://www.uta-net.com/song/280477/," 2020.