International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Laplace Transformation as Tool Algorithm for Classical Cryptography

Mahdi F. Mosa

AMA International University Bahrain, College of Engineering, Department of Mathematics and Science

Abstract: ***This article is a model of cryptography base on algorithm from Laplace transformation. The algorithm language is English alpha beta and the usage of number system, odd and prime numbers. The numbers assign to the alpha beta and then the formation of matrices. The final output of this method is a workable method of cryptography and can be used by any small or large company for a secure exchange of information.***

Keywords: Laplace transform, Algorithm, Cryptography and Matirces

1. Introduction

Cryptography is an old subject, used to hide information from those who are not allowed to know these information and its grown up with time and reach its maximum during the first and second world wars. But however those who interested in the problems of security of information start a new direction and jump from classical cryptography to modern one[1].

However still the classical cryptography is the one which follow the ideas toward the new modern cryptograph which base on the numbers theory, algebra and probability, in addition to other mathematical theory[2].In this article we try to insert new methodology based on the Laplace transform as a tool for classical cryptography, such that:
$L\{e^{at}sinbt\}=\frac{b}{(s-a)^2+b^2}$ and $L^{-1}[\frac{b}{(s-a)^2+b^2}]=e^{at}sinbt$.

Where a and b are constants and used as passwords for the cryptography process of this model. Also, it is understood that the Laplace transform generates to many algorithms, which can used for case of cryptography, such as, for example:
1) $L(e^{at}cosbt) = (s-a) / \{(s-a)^2 + b^2$.
2) $L(t^2-2+e^{-t}-sin3t) = (3/s^3) – (2/s) + (1/s+1) – (3/ s^2+9)$.
3) $L\{(5/3)e^{-2t}sin3t\}= 5/\{(s+2)^2+9$. Etc……

1.1 Statement of the Problem

A new problem arising, namely the security of these information. Attack and discrepancy through the webs channels, with a meaning and without, becomes one of the most vital problems for all business communications. According to that, computers and all types of communications are giving a great attention to the security of their information. In this research. I will present a mathematical method base on Laplace transform.

1.2 Objective of the Project

In this place I will say that it is important to use all possible way of transform information through the communications channel under a secure method. I will use the Laplace transform as tool to hide the information from any possible attack by the hackers.

1.3 Significance of the Study

This study is expected to have significant value to companies which deal with computers and security of information. Also, it can have value to stakeholders of higher education, such as instructors, students, educators, parents and so forth.

2. Literature Review

The history of cryptography is a very wide subject in the problem of reviewing the literatures. However, Reich mentioned a good detail of cryptography history, showing the importance of mathematics in this field of applied mathematics [3]. Koblitz “discus the algebraic aspects of cryptography, algorithms and computation in mathematics” [4]. Alireza Pour shows the importance of the numbers theory and prime numbers, specially the mathematical algorithm [5].Barakat and Hanke gave a wide detail about cryptography of the two types, classical and modern, such that, “Security properties [6].

A cryptosystem is said to have the security property
1) one wayness(OW) if it is unfeasible for the attacker to decrypt an arbitrary given cipher text.
2) in distinguishability(IND) or semantic security if it is unfeasible for the attacker to associate to a given cipher text one among several known plaintexts.
3) non-malleability(NM) if it is unfeasible for the attacker to modify a given cipher text in such a way, that the corresponding plaintext is sensible”.

Attacks. “One distinguishes the following different attack scenarios
1) Cipher text-only attack (COA): The attacker only receives cipher texts.
2) Known-plaintext attack (KPA): The attacker receives pairs consisting of a plaintext and the corresponding cipher text.
3) Chosen-plaintext attack (CPA): The attacker can once choose plaintexts and then receive their corresponding cipher texts. “Once” in the sense that he is not allowed to alter his choice depending on what he receives.
4) Adaptive chosen-cipher text attack (CCA2): The attacker is able to adaptively choose cipher texts and receive their corresponding plaintexts. “Adaptive” means that he is

allowed to alter his choice depending on what he receives. If he is challenged to decrypt a cipher text he is of course not allowed to receive its plain text. But normally such attacks are intended to recover the decryption key d of the decryption algorithm Dd.

As it was mentioned above in this research, that we insert the Laplace transform as a good tool for cryptography, as it will be mentioned in the next chapters".

3. Background and Methodology

Since the new revolution of computers and communication with the internet activities, there are many if all businesses, all over the word communicate with each other for exchange information. Then a new problem is arising, namely the security of these information. Attack and discrepancy through the webs channels, with a meaning and without, becomes one of the most vital problems for all business communications. According to that, computers and all types of communications are giving a great attention to the security of their information. In this research I will present a mathematical method base on Laplace transform.

The expectation in such a problem clears and I will create forms of security which can prevent the hackers from attacking the information.

i- The methodology of this research

1) Use one of the Laplace transforms, namely for this article, to choose algorithm.
2) Consider the A&B are the passwords of the system.
3) Name of the alpha beta of the used language through a prime number system, or an odd numbers greater than three.
4) Write the substitution for any text by numbers through the numbers theory.
5) Then the result can be organized as matrices with new additional passwords.
6) Send the encrypted material.
7) The receiver, has/have the passwords to open the encrypted materials.

This type of research is important in all the places, of large and small companies.

ii- Application:

The impose algorithm of this article is based on the Laplace transformation, such that $L\{e^{-at}\sin bt\}= \frac{b}{(s+a)^2+b^2}= F(s)$, where a and b are constants.

For the purpose of this article, we use the reciprocal of the function F(s) above, such that, $G(s) = \frac{1}{F(s)} = \frac{(s+a)^2+b^2}{b}$ and the constants a and b are considered as password, in this stage, use a=3 and b=2. In addition, we assume that $s \geq 3$.

The language for this problem considered to be the English alpha beta

(A, B, ……, Y,Z).

As it was mentioned above in this article, we assign each English letter to the output of the algorithm G(s), such that:

A=20, B= 34,……..., Y=1460 and Z= 1570.

This means that we can form an nxn square matrix with elements from the new values of the above English alpha beta. It is well known that one can always split a large matrix to small ones.

Simple example: We want to encrypt the name REEM for certain purpose, then from the values of the alpha beta, $\begin{bmatrix} R & E \\ E & M \end{bmatrix} = \begin{bmatrix} 802 & 100 \\ 100 & 452 \end{bmatrix}$ =A. Then we need to introduce a new matrix call it C, of the same size as A. Let C = $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ as a new pass word(or some time we call it additional password), we multiply A and C, in a usual matrices multiplication, we will have

D=AC = $\begin{bmatrix} 1904 & 3708 \\ 1536 & 2660 \end{bmatrix}$. Then, we can now send the final result, 1904 3708 1536 2660, to the place which we need.

Decryption:

Since D=AC, then $A=DC^{-1}$, where C^{-1} is the inverse of C. Using the definition of matrices operations for inverse, we find that, $C^{-1} = \begin{bmatrix} -5/2 & 3/2 \\ 2 & -1 \end{bmatrix}$ then, $A=C^{-1}D= \begin{bmatrix} 802 & 100 \\ 100 & 452 \end{bmatrix}$ = REEM.

4. Results and Discussion

The output of this algorithm for cryptography seems as an important result for security of information, under two password with odd and prime numbers.

The process follow the matrices theory and its inverses leading to hide the information, through the any communication channel. The results of this article shows that this algorithm leads to simple steps and the computers time for the numbers operation, is expected to be small.

5. Conclusion

The finding of this article can be summarize as follow:

1) The Laplace transformation is used as an algorithm, for the cryptography process.
2) English alpha beta have been used but one can use any other language.
3) Since the process have two password system, the security of the information is very high.
4) This method can be used for any double languages.
5) This method can be used in any company, small or large.

References

[1] A primer on pseudorandom generators, University Lecture Series, vol. 55, American Mathematical Society, Providence, RI, 2010. MR 2677397 (2011h:68001).
[2] AlirezaN.Pour, Sept. 2002, Japan.
[3] OdedGoldreich, Foundations of cryptography—a primer, Found. Trends Theor. Comput. Sci. 1 (2005), no. 1, 1–116. MR 2379506 (2010d:94086).
[4] Neal Koblitz, Algebraic aspects of cryptography, Algorithms and Computation in Mathematics vol. 3, Springer-Verlag, Berlin, 1998, With an appendix by

Alfred J. Menezes, Yi-Hong Wuand Robert J. Zuccherato. MR 1610535 (2000a:94012)
[5] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of applied cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, BocaRaton, FL, 1997, With a foreword by Ronald L. Rivest. MR 1412797 (99g:94015).
[6] "Mohamed Barakat and TimoHanke,2012.Cryptography — Lecture notes"