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

International Journal of Scientific Research and Reviews

Multilevel Transformation as a Tool Algorithm for Classical Cryptography

Pundir Shalini

Department of Science and Humanities, Babaria Institue of Technology, Vadodara, GJ, INDIA,
shalinipundir23@gmail.com

ABSTRACT:

This paper is based on using a mathematical technique of transformation as an algorithm for classical cryptography. Algorithm uses alphabets, numbers and (x, y) coordinate system. Here information to be encrypted is taken in English language. Methodology described here is useful for the programmers to built a secure system for data transfer.

KEYWORDS: Algorithm, Cryptography, Transformation, Inverse Transformation and Encryption.

***Corresponding Author:-**

Pundir Shalini

Department of Science and Humanities,

Babaria Institue of Technology, Vadodara, GJ, INDIA,

E Mail - shalinipundir23@gmail.com

INTRODUCTION

Cryptography is a word with Greek origins, means “secret writing”. We generally use this term “cryptography” to encrypt and decrypt the information for the security purpose. For more understanding we can take it as mechanism which receives information from sender, secure it under a lock using some keys and then at the receiver’s end, unlock the secured information using some keys again. Here I have developed a tool for classical cryptography, consisting of multilevel encryption of the information. We will have a brief about history of cryptography in upcoming section.

LITERATURE REVIEW

Cryptography is becoming a very wide subject of study. It has a vast literature base from classical to modern one[1]. Oded Goldreich also explains history of cryptography and also remarks on the connection of mathematics with the subject[2]. Mahdi.F. Mosa used Laplace transformation as a tool algorithm of classical cryptography[3] in 2016. He gave a good example that how mathematical techniques can be used in creating more secured passwords that are difficult to break. Here I have used mathematical transformations as the primary tool. In Mathematics a “Transformation” is a function from a set X to itself [4], such as linear transformation, rotation, reflection etc and their combinations.

In the next section of this paper, we will see a fusion of these transformation and classical cryptography.

STATEMENT OF THE PROBLEM

Today, in the world of digital communications it is a difficult task to transfer the information safely from one point to other. For such secure channel we need to generate multi-tier or multi-level cryptographic algorithms. In this research paper, I will present a multi-level mathematical method as a tool for classical cryptography. Here I will use two cryptographic algorithms – they both consist of encrypting the information using mathematical transformations: a) Magnification and translation together. b) Rotation by 90 degree.

Magnification is a transformation which increases the size of the object. In simple words multiplication of given value with a positive real number. For example: 2x, 5y, 3n... where x, y and n can be taken as the input values.

Translation is shifting the object from one position to another. For example: x+3, y+4... where x is shifted by value 3 and y by 4.

Magnification and translation together can be taken as functions like 2x+5, 3x-2....etc.

Rotation is a transformation which rotates the object about centre of rotation with some specific angle. Here we have taken the angles 90 degree clockwise and 90 degree anticlockwise. Further details of the methods described above are discussed in upcoming sections.

SIGNIFICANCE OF THE STUDY

This study may have significant value for the professionals who are working on the security of the information. Also it may have important impact on teachers, students and programmers for creating more secured algorithms. From this they may develop some more technically sound ideas and programs.

BACKGROUND

Basically the idea consist of converting the alphabetical information first to the numerical code, then after applying the described methodology to it, the password will be converted to more secured levels. Then protected information will travel through the channel. At the receiver's end a reverse algorithm will be applied so that receiver has the same information as it was sent by the sender.

METHODOLOGY

First algorithm described is for encrypting the information:

Level 1: Converting the alphabetical information to numerical code. Take A=0, B=1, C=2, ... , Z=25. Let the information be "AK...."

Level 2: Here we use mathematical transformations say "T" on the numerical code generated in level1 –combination of magnification and translation

$T(N) = 2N+3$ for N=0,1,2,.....25

For example: T(0) =03 , T(10)= 23 .....T(25) =53 .

Result will be of the form 0323.....

Level 3: Taking that numerical code to one level ahead by taking two digits of the code as (x,y) in x-y plane, thereafter applying anticlockwise rotation by 90 degree. Rotation by 90 degree means applying the real function

$f : R^2 \rightarrow R^2$ defined by f(x, y) = (-y, x) $\forall (x, y) \in R^2$

For example: f(0,3) = (-3,0) , f(2,3) = (-3,2). Result will be transferred in the form -30-42.....

The encrypted material will be then sent to the receiver's end where he can decrypt the material using reverse algorithm discussed below:

Level 1: Split the code in to tupples (-3,0) , (-3,2) and so on

Then apply clockwise rotation by 90 degree using real function

$f : R^2 \rightarrow R^2$ defined by f(x, y) = (y, -x) $\forall (x, y) \in R^2$

Result will be of the form (0,3), (2,3) and so on.....

Level 2: considering each tupple as a two digit number (N) apply inverse transformation given by:

$T^{-1}(N)= \frac{N-3}{2}$

For example: $T^{-1}(03) = 0$, $T^{-1}(23)=10$ and so on.....

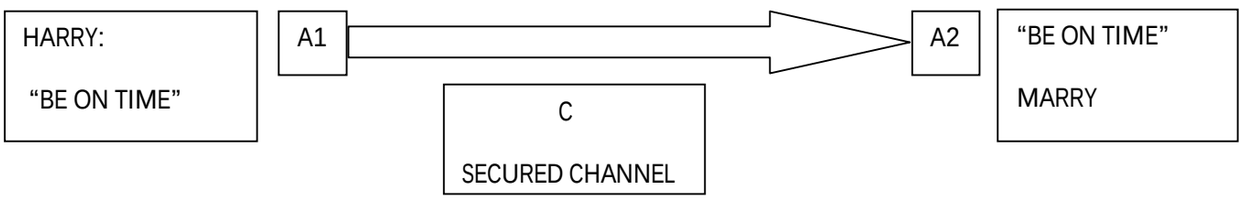
Result will be of the form 0, 10, ...

Level 3: Again convert the numbers to alphabets as 0 means A , 10 means K and so on....

In this way the receiver gets the original information "AK..... "

APPLICATION

Suppose HARRY wants to transfer the message “BE ON TIME” to his friend MARRY secretly via channel “C”. Where “C” has algorithm A1 at sender’s point which convert the information to “-50-11-13-92-14-91-72-11”, through the channel information will travel in this encrypted form and at the receiver’s end, algorithm A2 will decrypt the information to “BE ON TIME”.



RESULT AND DISCUSSION

Above discussed algorithm for cryptography is able to introduce high level security in a system to hide its important information from the unknown means. This algorithm can work on all kinds of passwords consisting of alphabets. Also it is independent of number of alphabets i.e it works for both even and odd number of total alphabets used in the password. As mentioned above, it consist of coding or encryption at two levels and at result obtained at the end is difficult to decode as it require the idea of anticlockwise rotation and then inverse transformation.

CONCLUSION

This article can be sum up in the following manner:

1) Algorithm used depends upon mathematical transformations and their combinations.
2) System consists of multilevel encryption.
3) It can be easily programmed using most of the computer languages.
4) This idea can be implemented in any small or large scale organisations.
5) Level of security is high and password generated is difficult to decode.
6) May be utilised by the students or professionals to generate more algorithms of this kind.

REFERENCES

1. Oded G. University lecture series 55 - A primer on pseudorandom generators. American Mathematical Society. Rhode Island USA. 2010.
2. Oded G. Foundations of Cryptography- A Primer. FnT-TCS. 2005; 1(1): 116.
3. Mahdi FM . Laplace transformation as a tool algorithm for the Classical Cryptography. IJSR : ISSN(2319-7064). 2016; (5): 10.
4. Olexandr, Ganyushkin, Volodymyr, Mazorchuk. Classical Finite Transformation Semi groups. Edition 1. Springer – Verlag. London. 2009.