# Enhanced Cryptography Algorithm based on Numerical Methods

Daniel Giftson [20110051]   Jinay Dagli [20110084]   Mumuksh Tayal [20110116]

Kush Patel [20110131]   Patel Vrajesh [20110134]

# Abstract

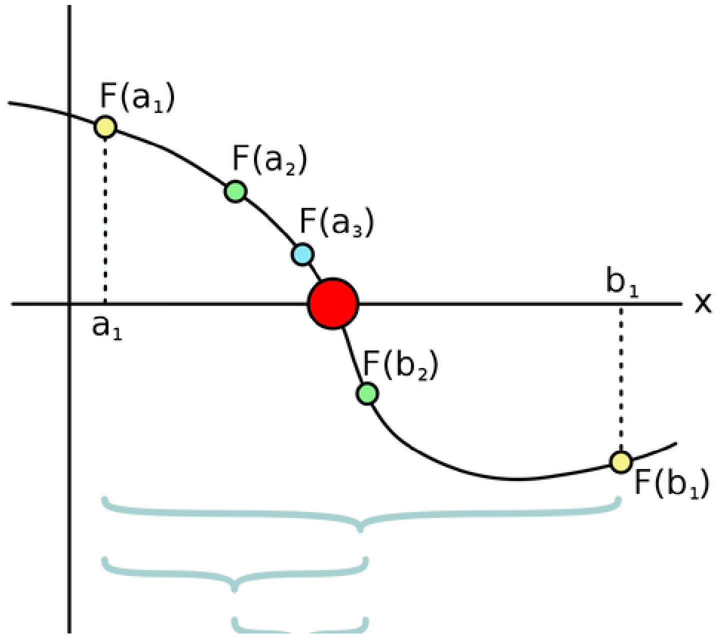
Cryptography is not a new concept. Rather, it has been in use for hundreds of years now. It is the study of mathematical methods pertaining to aspects of security of information like data integrity, authentication, confidentiality, and data origin authentication.

# Introduction

**What should you expect?**

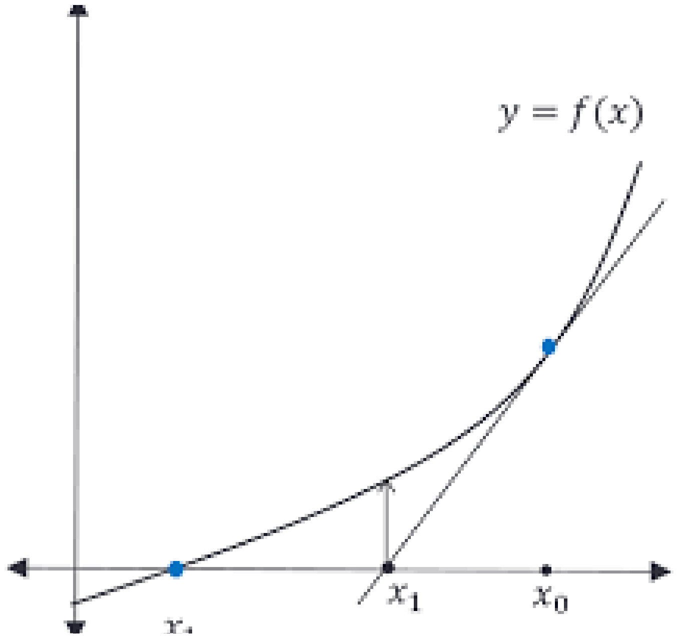
- What is Cryptography?
- Why this topic?
- Brief description of numerical methods
- Use of numerical methods in cryptography
- Live demonstration
- Comparing the various numerical methods

# Numerical Methods used



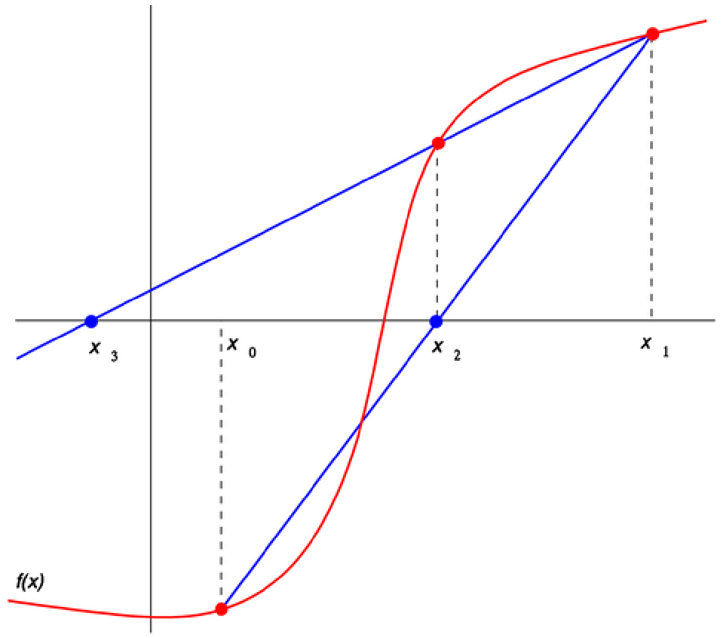
## Bisection Method

The bisection method or interval halving is a type of incremental search method, where the search interval is always divided into half.



## Newton's Method

Newton-Raphson Method, is a numerical method where we try to find the root of a function by approximating the function by its tangent line.



## Secant Method

The secant method is a recursive method for finding the root for polynomials by successive approximation..

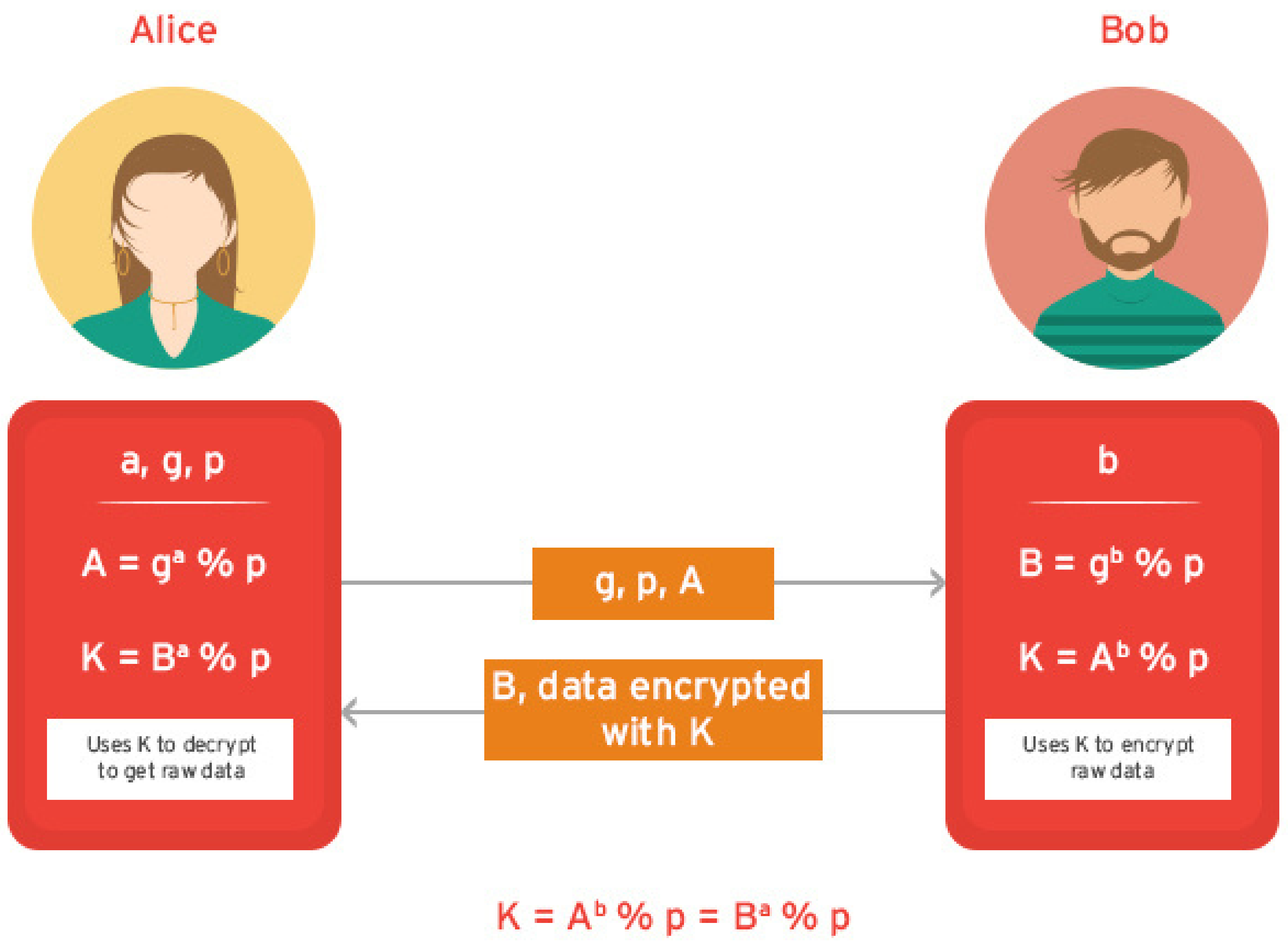
# Mathematical Approach

- **Symmetric Key Exchange algorithms**

- **Encryption algorithm**: Numerical methods to calculate roots of the one-way function

- **Decryption algorithm**

# Diffie-Hellman Algorithm



Alice

$a, g, p$

$A = g^a \% p$

$K = B^a \% p$

Uses K to decrypt to get raw data

$g, p, A$

B, data encrypted with K

Bob

$b$

$B = g^b \% p$

$K = A^b \% p$

Uses K to encrypt raw data

$K = A^b \% p = B^a \% p$

# Encryption Approach

## Step-1

Convert the text message to a decimal number (the ASCII values of the letters

## Step-2

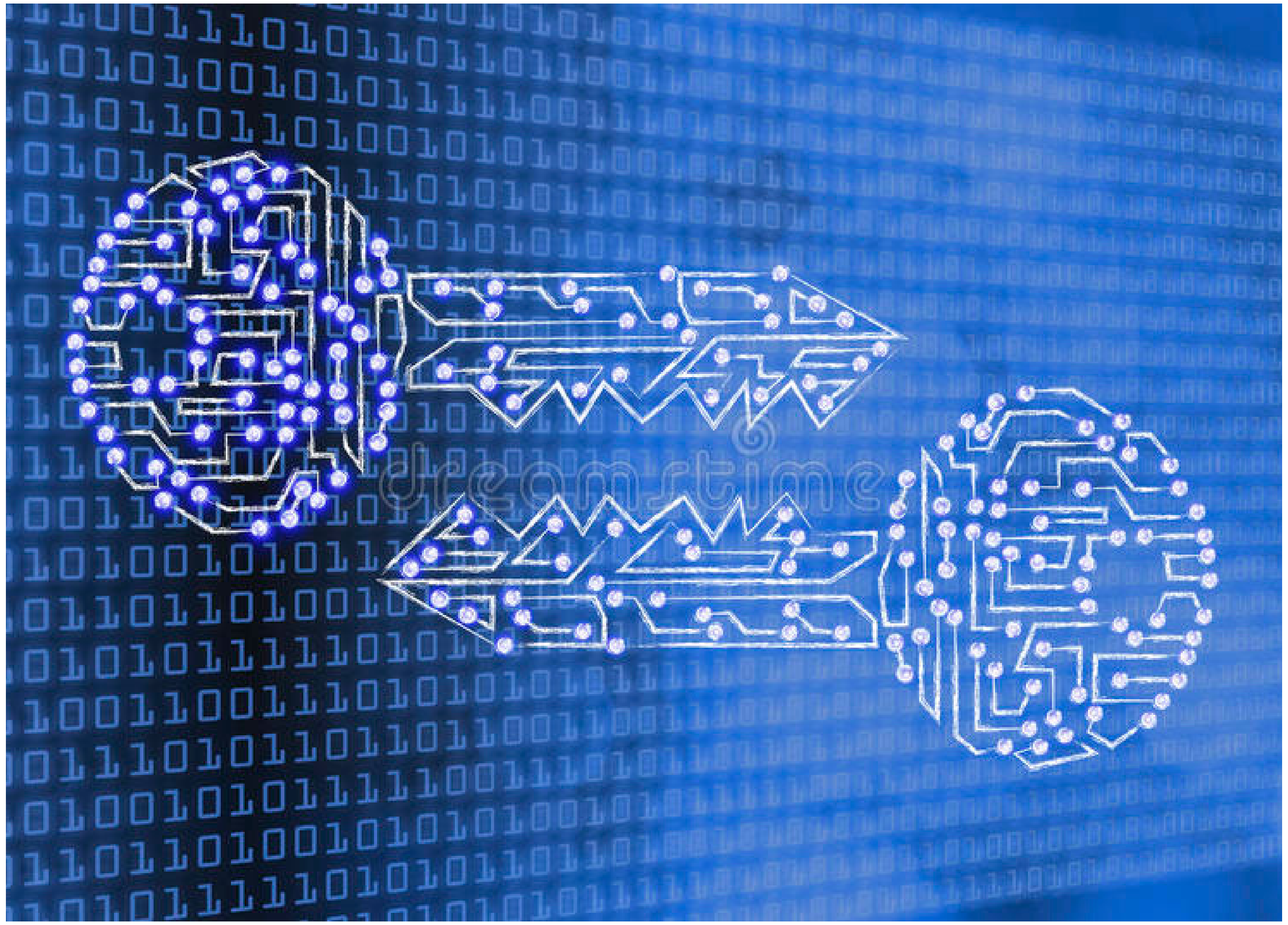
The Diffie-Hellman algorithm is used to get the one-way function f(x) and the secret keys required by the user and the receiver.

## Step-3

Solve f(x) = ASCII value of the text message. Cipher text is given by root of this equation.

## Step-4

Encrypted data is shown by array of solution of equations.



# Decryption Approach

### Step-1

Put the values of array into the function to get the values of x.

### Step-2

This value of f(x) is equal to the ASCII value of the text message.

### Step-3

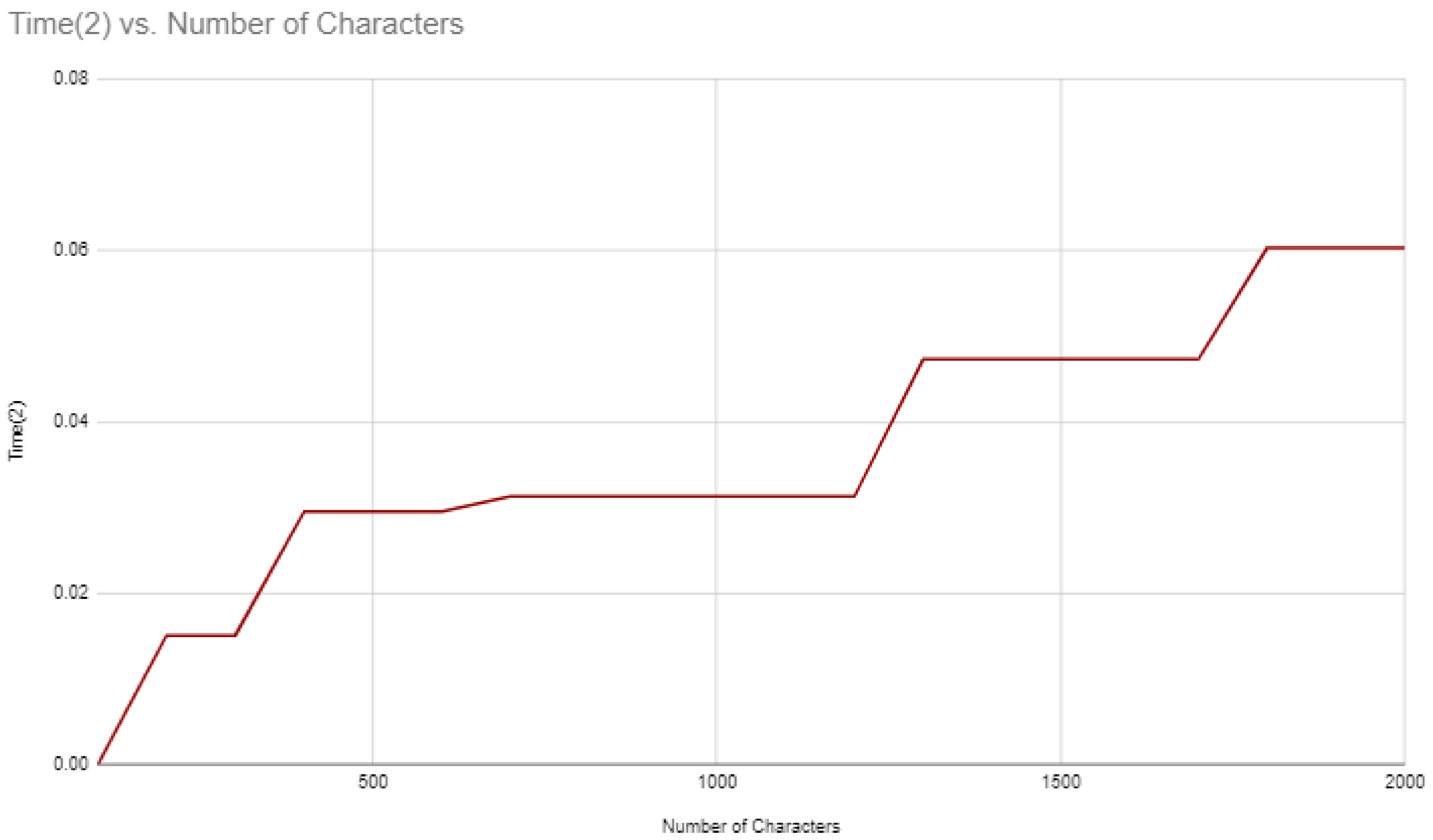
Eventually, from this we can get the original massage.

# Live Demonstration

Let us see how some plain text can be encrypted and decrypted using a python code!

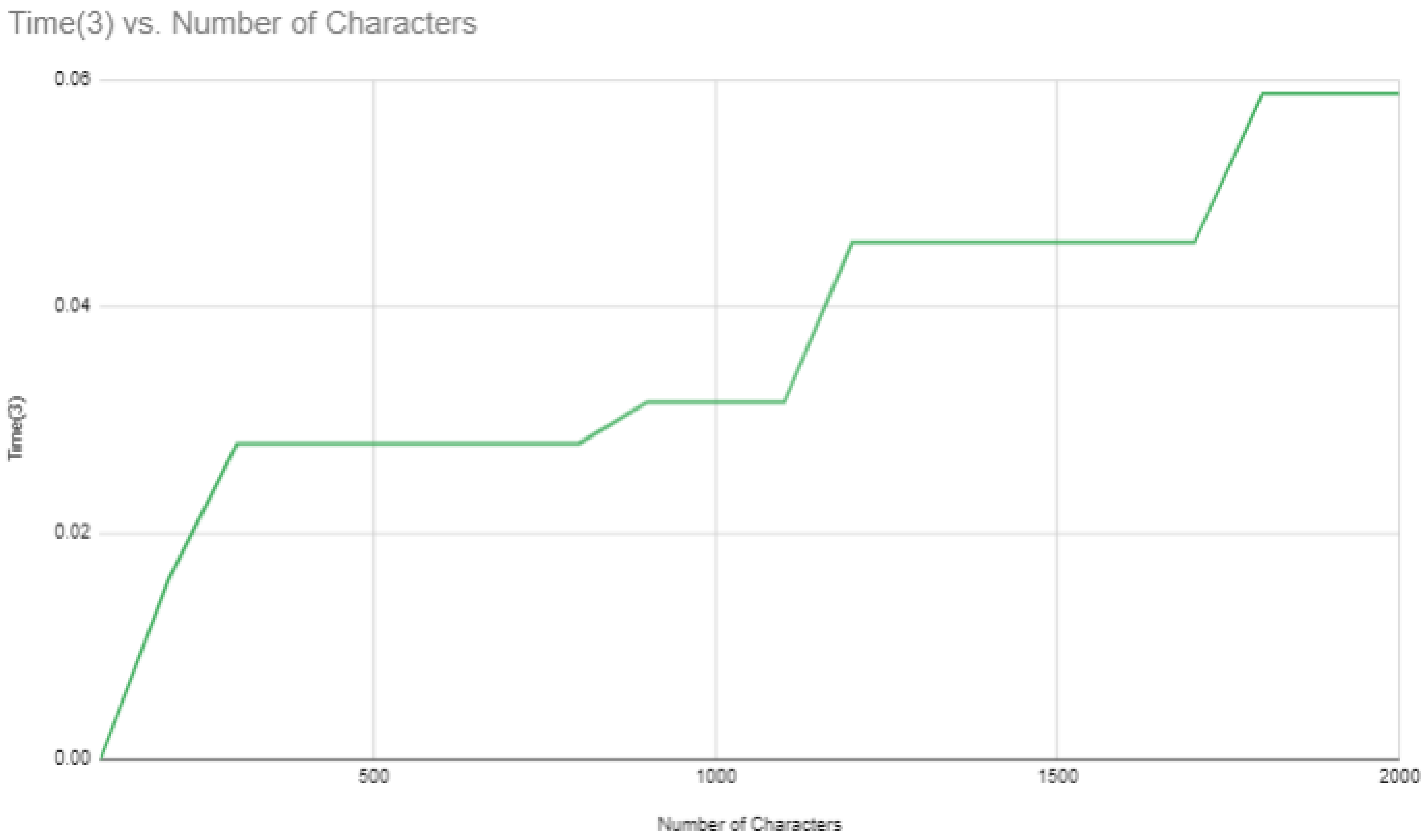
# Results obtained

## Bisection Method



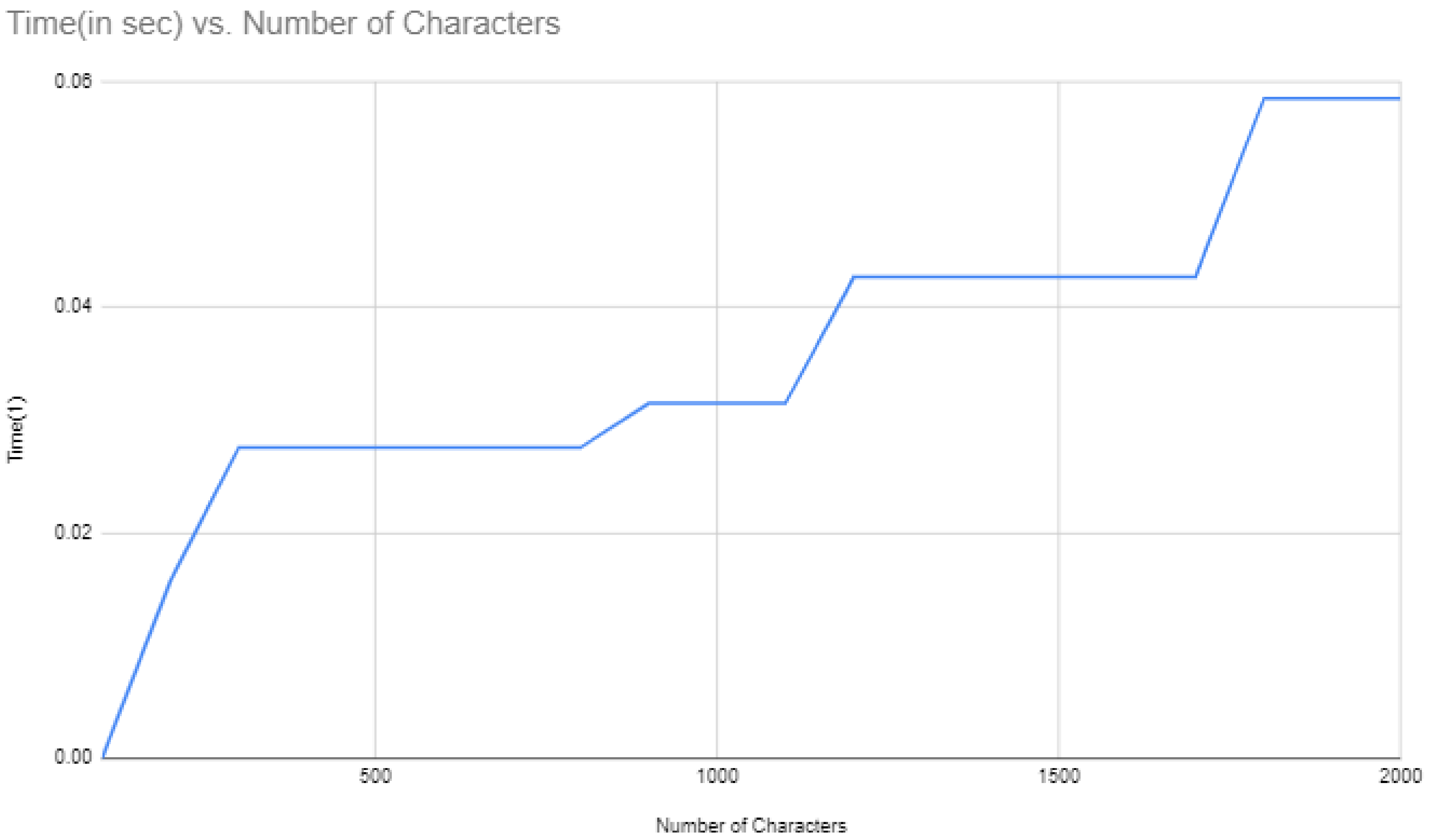
# Results obtained

## Newton-Raphson Method



# Results obtained

## Secant Method



# Conclusions

- The results of the comparison show that the Newton-Raphson method and Secant method are quite efficient, while methods like the Bisection method do not work very efficiently for a larger length of text.

- It can be very well observed that Secant and Newton's methods take very less time and very less iterations for encrypting the same text message.

- The results we obtained hold with our general expectation that the Newton-Raphson method and the Secant's method takes lesser time to converge.

# THANK YOU FOR LISTENING!

*Hope you liked the presentation!*