MA202 Course Project - Project Title and Problem Statement

Group Members:
Shreyshi Singh (19110032)
Xhitij Choudhary (19110044)
Ayush Anand (19110074)
Siddhi Surawar (19110170)
Somesh Pratap Singh (19110206)

Project Title: An enhanced cryptographic technique combined with steganography, to enhance Network Security System, using Newton's Method

Problem Statement:

Cryptography is not a new concept. Rather, it has been in use for thousands 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. It does not only mean hiding information. Rather it is a set of techniques which can be implemented to code a data, send it to the intended receiver, and should be easily unpackable by them.

With the dawn of the Information Age, development of hacking techniques and sensitivity of data, security has become more important than ever. The most basic cryptography consists of a coded message and a key to decode it. Depending on whether the encryption key is same as the decryption key or not, cryptographic algorithms are divided into two parts - Secret Key Cryptography (or Symmetric Key Cryptography) and Public Key Cryptography (or Asymmetric Key Cryptography).

Steganography is also a method to encrypt data. Confused with cryptography many times, the difference between them is that steganography conceals data in a non susceptible way, so that it goes undetected. For instance, hiding the data in a normal looking image or file. The same is not true for cryptography, where encrypted data's existence is confirmed, but unknown. Due to the extra protection, steganography is a more preferred and implemented technique.

Many encryption algorithms already exist for Network Security. Our project aims to implement a symmetric encryption-decryption algorithm which is developed using steganography and the encryption and decryption is done using Newton's Method (also known as Newton-Raphson Method). The encryption is done using the concept of one way function (closely related to one-one function, but not the same) and then finally steganography is used to finally encrypt it.

Mathematical Concept (the update)

In the context of computer science, one-way functions are functions that are easy to compute (finding f(x) at a given x), but it is difficult to obtain the image of a random input. The words 'easy' and 'difficult' are in relation to a computing entity, 'easy' meaning cheap enough for a legitimate user, and 'difficult' meaning expensive for any malicious agent. So naturally, one-way functions provide a solid method to encode messages in cryptography.

Another important property is that, if *f* is a one-way function, then it is difficult to invert, but if we know the inputs and outputs, we can easily verify whether they are accurate or not.

In numerical analysis, the Newton Raphson method is one of the fastest methods to converge to a root of a given function. Beginning with a guess value (say x_o), we compute the tangent at $f(x_o)$ and the x where the tangent crosses the abscissa, is our new x_o (set x_o = x where the tangent is 0). When our $f(x_o)$ is 0, or sufficiently close (say 0.000004), we stop the computation.

Our plan to implement this is:

Algorithm for encryption

1. Read the input to be encoded, get the ASCII values for each of its characters.
2. Take a polynomial function from the receiver using DSS technology, subtract the ASCII values from the polynomial and set it to 0 to get the polynomial equations.
3. Solve the polynomial, and store the solutions in an array.
4. Encrypt the array (we have not explored the details of it, yet.)

Algorithm for decryption

1. Read the encrypted file
2. Take the values, and store them in an array
3. Put the values in polynomial function and get the functional values
4. Convert the values back to text

An example

1. Let's say the encrypted message is 'MATH'. We get the ASCII values of each letter (M=077, A=065 and so on).
2. Send the request and get a one-way function. Let us assume our one-way function is $f(x) = 3.5x^3 - 2.7x - 17$. (This is our secret/private key).
3. Solve the equation for each ASCII value.
   First letter is M, so solve f(x) - (ASCII of M) = 0, that is f(x)-77=0.
   The solution for this is x=3.0805. Store these solutions in an array.
   HERE IS WHERE WE USE NEWTON RAPHSON METHOD. The method is very fast on computers, hence it is efficient to implement.
4. Encrypt the array.
5. Decryption can be done by putting the solutions back in the secret key.
   That is, the receiver receives a value of 3.0805. So, f(3.0805) = 77.99585 which is rounded off to 77 which corresponds to M.

The challenges we face are the details of the encryption and decryption, which we need to work upon.

We will propose an algorithm to implement it. The algorithm will be simple and secure, with the key concept being the encryption using one way functions with Newton's method.

References:

[1] A. Ghosh and A. Saha (2013). A Numerical Method Based Encryption Algorithm with Steganography. R. Bhattacharyya et al. (Eds) : ACER 2013, pp. 149157. CS & IT-CSCP