Visualization of Encryption

Vibha Pandurangi

November 14, 2016

Abstract

For my project, I want to explore cryptography and the visualization of different encryption methods through graphics using VPython and, if time permitting, JavaScript. First, I will explore ancient cryptography, including the Caesar Cipher method and the Vigenre cipher. At this point, I look to creating a visualization of these two ciphers by creating spinning wheels to display the encryption shifts. Then, I would like to delve further into more modern encryption methods, like public-key encryption. The way I am able to create the graphics to present the visualizations may evolve and thus, this part of my project is currently flexible to best fit the encryption methods I study since this project has not been attempted previously.

1 Proof-of-Concept and RTICA

For my initial proof-of-concept, I want to be able to visualize a basic shift encryption. The Caesar Cipher shift is a simple ancient encryption method that utilizes shifts to code the messages. For example, the String "ABCDEF" with a shift value of three would become "DEFGHI". Negative shift values can be used to decrypt the messages, as using a shift value of -3 on "DEFGHI" would result in the String "ABCDEF". Although this method of encryption was once considered to be secure, it can now be seen now that the Caesar Cipher can easily be broken. First, I would prove that I can create a Cipher code so that will be the first part of my proof-of-concept. Then, for the second part of my proof-of-concept and my real-time interactive computer animation, I would like to visualize this shift encryption using wheels that would display input, allow the user to select a shift value, spin, and display an output value.

2 Caesar Cipher and other forms of ancient encryption

The Caesar Cipher was used by Julius Caesar to communicated secret military messages, and has since then, been a very well-known but simple form of encryption. The cipher can now easily be broken through the use of the brute force attack, since there are only 25 possible shifts that can be implemented in the Caesar Cipher. However, the Caesar Cipher's basis of alphabetic shifts are not extinct; instead, the concept has been implemented into various other encryption methods. For example, the Vigenére cipher uses a polyalphabetic cipher instead of a singular value shift. In this particular method, a word is selected as a key (instead of a numerical shift value as in Caesar) and a A-Z by A-Z table is used to create the cipher. If time permits after creating the Caesar Cipher RTICA, I would like to begin working on a visualization of the Vigenére cipher. Similarly, to the Caesar visualization, I would like to depict this cipher in the same way with the spinning wheels.

3 Public key encryption

Public key encryption is the use of public and private keys to encrypt information. Public key encryption is asymmetric, meaning that two different keys must be used to encrypt and decrypt information. If someone were to send confidential information, they would encrypt it using the recipient's public key, which would then be decoded using only the recipient's private key. This is the area of my project that I would look to do more research on in order to figure out a method of visualizing different methods of public encryption. Mathematically, the basis of public key cryptography is one way functions, which are functions that can be easily computed but their inverses are more difficult to compute.

The most common type of public key encryption is RSA, which uses prime factors are the one-way function (or the private key). The key-pair is a large number n (the product of two prime numbers) as the public key and a derivative of one of the factors of n as the private key, making this RSA encryption very secure. One option to portray the security of the RSA encryption is to allow the user to input a value for the modulus, n (the multiple of p and q), and the program to output all the possible values of p and q. Then the program would allow the user to develop their own example

of simple public and private keys, input a message, and deliver an encrypted output. I am still researching a visualization or graphical representation of this concept.

In terms of mathematics, I am looking to understand the mathematics behind different encryption algorithms, starting from simple ancient shifts and working toward public key cryptography. In terms of graphics, I would like to create different ways to visualize encryption methods, through the turning wheels and perhaps interactive graphs. I would be using VPython while working on this project, and time permitting, will look to translate to Javascript/HTML.

4 Purpose

The purpose of my project is to allow the user a better understanding of how encryption works through a visual depiction of it as this as very little presence on the internet. While coding my cipher in my CS 125 class, it was difficult for me to code the shifts because I could not visualize it effectively. With my project, I look to making it easier for the user to understand the Caesar cipher by allowing them to see the shifts, both in the encoding and the decoding process. The long-term purpose of my project in terms of the study into the public key encryption part of my project is to deepen my understanding of encryption, and using this knowledge, try and create a visualization or graphic to depict RSA encryption. Overall, I would like my project to help the user understand both ancient and RSA encryption, through text and visualizations. For future developments of my project, I would like to see the visualization of the Vigenére ciphers as well as an expanding the concept of visualization in RSA encryption.

5 Timeline

October 28: Caesar Cipher completed

November 4: Vigenre implemented

November 9: Seminar

November 9-23: Further research on public key encryption for ideas on visualization, working on completing RTICA, and writing up the paper on the public key encryption theory.