Nicole Robles
CYEN 489 - 001
Introduction to Cryptography

Encryption Scheme Project

When considering this project, many ideas ran through my head. Initially, I debated whether I should begin with a symmetric or an asymmetric system, and from then on, I attempted to tie in different areas of study into cryptography. I wondered if any of my engineering courses could be used as a basis for an encryption scheme.

My first trial was attempting to tie in some of statics and mechanics of materials into mathematics, since there was uniqueness in the properties of each metal. A complex encryption scheme could be built around different statics problems, where the placement of the materials is given, but only both Alice and Bob know the forces and/or the type of metal the arrangement required. After much deliberation, this proved to be unfeasible since it was not easily reversible, and both parties would have a difficult time calculating the numerous unknowns of each arrangement. Having exhausted most of the encryption possibilities in statics, I shifted to my mathematics courses of study.

In the search for mathematical patterns, I moved to the study of the Fibonacci sequence. I wondered if there could be an encryption scheme built around the well-known sequence, since its numbers increased in value rapidly. In order to convert the sequence into an encryption scheme, I used the familiarity with moduli I gained from this course (Cryptography) in order to study the sequence differently. Choosing a low prime in order to see the results easier, I created a table based on the results, shown below.

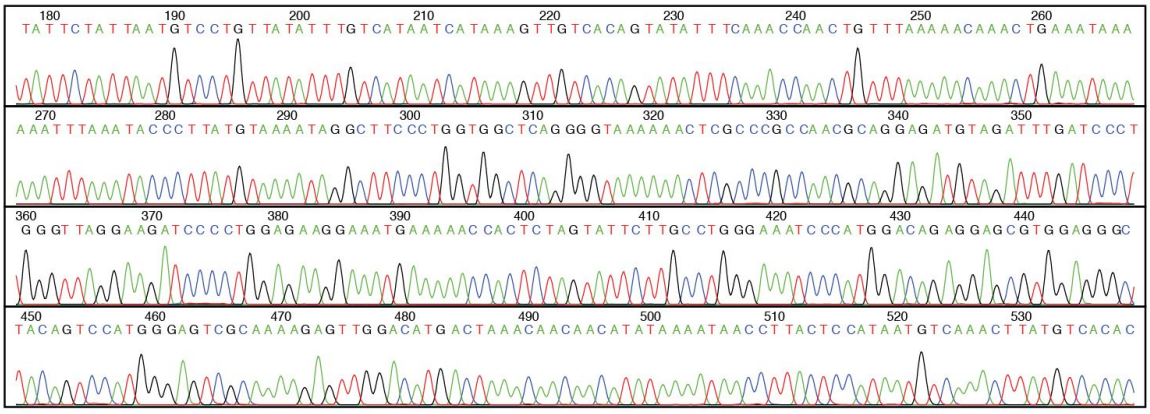
Fibonacci Sequence	Fibonacci in Modulus 3
0	0
1	1
1	1
2	2
3	0
5	2
8	2
13	1
21	0

34	1

Quickly, I realized there was a pattern arising. The sequence seemed like a repeating key that could be used to encrypt a secret message. I theorized that with large enough modulus, the sequence would be more difficult to decipher, and thus bring a unique structure that could be used to hide information. The Fibonacci sequence is known to all, so if Alice and Bob wanted to share sensitive information without Eve listening in, they could choose a shared modulus and encrypt their information using the Fibonacci sequence modded by that specific number.

However, after considering the security of the scheme I created, I came to the realization that the Fibonacci scheme could be cracked with brute force algorithms. Since the Fibonacci sequence is widely-known, the only unknown variable in the encryption scheme would be the shared modulus. If Eve would be intercepting the communication between Alice and Bob, she could listen for the shared modulus to be discussed and promptly crack the cipher. If Eve was not able to intercept the communication, in case Alice and Bob had discussed the shared modulus and agreed upon it verbally, Eve could still set up scripts on her computer to compute every single modulus of the FIbonacci sequence, and eventually crack the message.

Disappointed in these findings, I moved to yet another disciplinary course of study: biology, focused on genetics. In the search for uniqueness, I thought about how the DNA of every human is unique and can be used to identify people involved in crimes. I began to theorize how DNA could be used in order to hide information, and thought about how DNA is composed of 4 different bases: adenine (A), cytosine (C), thymine (T), and guanine (G). These four bases could then be transferred into binary: 00 for A, 01 for C, 10 for T, and 11 for G. This led me to create an asymmetric encryption system using those binary values.



DNA sequence data from an automated sequencing machine

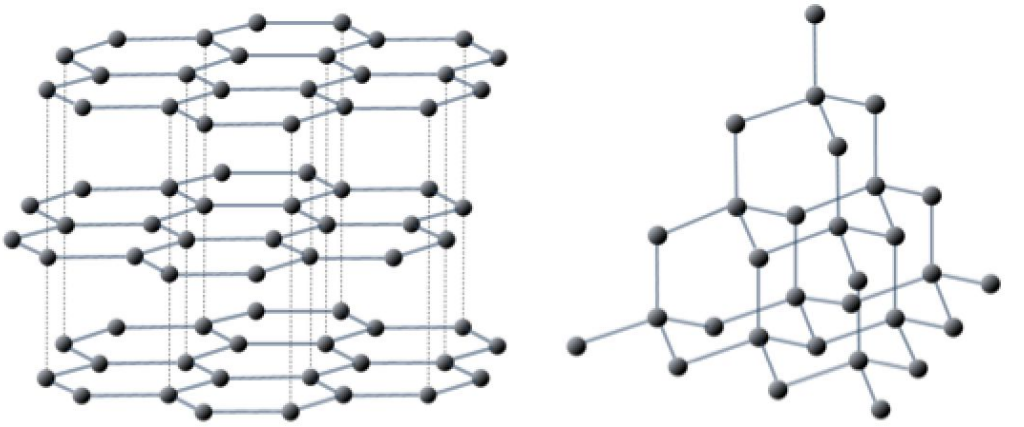
https://www.genome.gov/genetics-glossary/DNA-Sequencing

The DNA system would work like this: Alice would choose a DNA sequence of her liking, look at its arrangement of bases (ACTG), and transfer them to binary in order to create a unique binary string.

She would then choose a random DNA sequence, change it to binary, and AND it with her original binary sequence. The output of the AND would be published, and Bob would be able to see it. Bob would convert his message to binary, and XOR his the encrypted message with the DNA sequence posted by Alice. Bob then sends the XOR to Alice, who would decrypt it by XOR'ing Bob's encrypted message with her unique binary sequence.

However, this system implementation has safety issues with XOR being easily reversible if the ciphertext is acquired. After realizing this, I began considering other types of binary operations such as AND and OR, but they kept producing the same issues. Even though the DNA sequence would be unique each time, since the DNA sequence from Alice would be published and Eve could listen in to Bob's ciphered response, she could extract the hidden message by comparing the two.

Trumped by that discovery, I changed educational disciplines yet again. Uniqueness can be found in chemistry specifically in molecular structures. For example, the carbon atoms in diamond and graphite are organized in distinct patterns. A visual representation can be shown below.



Graphite (solid lines are strong covalent bonds, dotted lines are weak inter-layer bonds)

Diamond (all bonds are strong covalent bonds)

https://opentextbc.ca/geology/wp-content/uploads/sites/110/2015/06/the-lattices-of-graphite-and-diamond.png

Based on the complex molecular structures, I began thinking about how graph theory could be used within them. The unique geometry of molecules could hide information within it as a graph would, and each bond within the molecule could represent the lines connecting vertices in a regular graph theory problem. From my basic understanding of graph theory, the carbon atoms in a molecule could be randomly spread out on a graph, with no connections, and be published by Alice.

Only Alice would know how to connect each of the atoms in order to form the correct molecule. Bob would see the "random" points on the graph, and spread out his message over every single point on the graph, however he chooses. After doing so, Bob would send his plot back to Alice, who could decrypt it with her knowledge of where the carbon bonds are, and properly sum up the message Bob sent. This would trump Eve since she would see the graph Bob spread out his message on, but she wouldn't have the

knowledge of where the atoms tied together in order to make sense of the graph. Only Alice would know how to read the graph, making this a secure asymmetric encryption scheme.

However, I had personal limitations in my knowledge of graph theory.. Though I was not able to go further in depth into the practical implementation of graph theory for this scheme, I believe this maintains to be a feasible option for an advanced encryption scheme, and as I learn more through the rest of my educational career, I hope to be able to fully craft this idea and be able to completely support with mathematical proofs in the future.