Week 2: Written Reflection

In this week 2, we covered Classical cryptography where some simple cryptosystems like shift and substitution cipher were discussed. I learned that classical cryptography is based on the mathematics and depends mostly on computational difficulty of large number. In this cryptography the plaintext is converted into ciphertext for the purpose of transferring sensitive data through insecure communication. There is a concept of key that is used to encode or decode the message and key should be kept secure. Classical cryptography has basically two types of techniques which are symmetric and asymmetric cryptography. In symmetric cryptography, there is only one key that is used for both encryption and decryption. In asymmetric cryptography, there is public and private key where sender encrypts using public key and receiver decrypts the encoded text using private key. Also, I learned about the cryptoanalysis techniques. I was intrigued by this theory as we make assumption that intruder knows about the technique which is being used to encode. There are different techniques of cryptoanalysis and I was more intrigued with known plain text attack as in this type of attack the intruder has both plaintext and ciphertext. While trying to attempt the solutions for the shift cipher, I understood that shift cipher encryption depends solely on the shift of the alphabets. For example, let's say if we want to shift for A to E, then correspondingly, we will have to change for B to F and so on. Here the shift key will be 4 and each and every letter would be shift on the same way. For Z, it would be D as we don't have any alphabets after Z so we just repeat and count from the beginning.

Furthermore, while going through the chapter, I understood about substitution cipher where there is no key mentioned as previous encryption methods and key is randomly given to the alphabets that is ranging from 1 to 26. Also, for one alphabet we can only issue another one alphabet. For instance, if we give A to E then we cannot issue A to B as A has already been issued to E. For decrypting this type of encryption, it takes some time and frequency letters and probability of occurrence take vital role in this decryption. Let's say if there is a cipher text ARADDSDWDWDER, then we first find out the frequency of letters and guess the key that is being replaced with that. Probability of occurrence takes vital role in this decryption method as in the sentence, E is most repetitive so, we issue E to the highest frequency alphabet in our cipher text.

While studying about Vignere Cipher, it is complex type of Caesar cipher where the letter frequency won't be fixed as Caesar cipher. The simple frequency analysis as substitution cipher won't work in this type of encryption as highest frequency letter E can also be represented by various letters in various points in the message which will be hard to decipher with simple frequency analysis. While encrypting this type of cipher, the alphabets are written out 26 times in different rows which is also called as Vignere table. Studying Hill cipher, I recapped about matrix multiplication as the letters will be given respective numbers ranging 0 to 25 and after multiplying, we, modulo it by 26 and the result will be the ciphertext. The weakness of this cipher was if the attacker has both plain text and cipher text.

While doing the assignment, I am really new into python and into programming field so, I believe along with learning new Cryptographic theories. I learned about different theories which had its own advantages and disadvantages. There were more mathematic and arithmetical expressions and I had hard time understanding the concepts but was able to get through them step by step. I came to know about various terms like Kasiski test, congruency theory which I did not know before. Google Collab was also a new thing for me. I also learned about GCD, relatively prime number to find out the modulo and many more. The chapter was difficult as we also had to program the solutions in python which was a new thing for me. Overall, I feel more comfortable about basic cryptographic theories and with Cryptoanalysis. I am able to gain a lot of knowledge while studying and trying to solve the assignments but it is somewhat complex to solve in python and I am trying till now as I had never studied about this before.