Week 5: Written Reflection

In chapter 4, I have learned about what is block and stream cipher. I found out that both were the ways of encrypting the data. They both used symmetric encryption algorithms which I learned in previous chapter where only one key is used to both Encrypt and decrypt. If you encrypt the data or plain text in chunks or blocks it is Block Cipher. I researched more that Block uses chunks to get cipher text of the same size which is generally 64 to 128 bits. It is done by using the plain text and key bits and in the other hand, Stream Ciphers don’t do that. They just generate pseudorandom bits from the key provided and encrypt the plain text by using that along with XOR operation.

Other day after that, further down I was intrigued by Differential Cryptanalysis as I had studied only about Cryptanalysis before and I was more curious to found out the difference between them. Form what I learned, this type of cryptanalysis is mainly used in block cipher but can also be used for Stream and Cryptographic hash functions. Generally, it can also be called as a chosen-plaintext attack. We use the x-or value thinking that the attacker has large number of data sets or inputs. All the text are encrypted with the same keys, and we try to decrypt using the same key for all the plaintexts. So, let’s say if there is a plain text attack then it is a disadvantage. I also learned in depth about DES which is a block cipher. We encrypt the data in 64 bits in this and we use the same algorithm for both encryption and decryption following the key to be 56 bits. After further studying about DES, I got to know that the 64-bit plain text goes into initial Permutation (IP) which is given by LPT and RPT which goes through the keys and both are again permuted, and we get ciphertext from it. However, let’s say if the keys are a split into two half and if we swap them, they might give us the same result if there is 0 and 1 continuously. Also, there is Sei weak keys where the output might be same from the S-Boxes when different inputs are there in permutation. So, later there is a replacement for DES and AES came which has the block length of 128 bits and keys can be 128,192,256 bits. The main advantage for this can be as it can be implemented in both hardware and software. Let’s imagine if you are using 128 bits key then you will need 2 to the power 128 tries to break them which makes it hard to crack. But the problem for this type of algorithm is that every block is always encrypted in same format, and it is hard to implement AES in software.

Also, I gained additional knowledge about the ways of operation. I learned more about the following seven modes of operation: counter mode (CTR mode), output feedback mode (OFB mode), cipher feedback mode (CFB mode), cipher-block chaining MAC (CCM mode), and Galois/counter mode (GCM). Padding oracle attack was also discussed in some detail in this chapter. I learned that an attacker can send ciphertexts that have been altered to the oracle and track its responses by using a padding oracle attack. This allows the attacker to finally retrieve the entire plaintext and gradually deduce details from it. The ciphertext is modified somewhat throughout the attack, and then it is sent to the padding oracle to check the validity of the padding. By evaluating the oracle's responses, the attacker can ascertain whether the padding is accurate and utilize this information to infer specifics about the plaintext. These modes of functioning, I discovered, offer both advantages and disadvantages. In some circumstances, OFB and CTR are more effective, although ECB is more open to attack. I learned about stream ciphers, a sort of symmetric-key encryption that creates a keystream to encrypt data, in the other part titled "Stream cipher." Also, authors described numerous stream ciphers, outlining both their advantages and disadvantages as well as the underlying theoretical ideas.

Also, I learned how stream ciphers are used in practice and how vulnerable they are to different kinds of attacks. Overall, the chapter served as an invaluable resource for understanding the symmetric-key encryption technique by providing a thorough overview of block ciphers and stream ciphers. Also, the theoretical aspects of encryption are simple to comprehend, but the mathematical examples are difficult to grasp. I have also learned something about SPN where there is S box (Substitution) and P box (Permutation). This box is used to get cipher text. The ciphertext is generated usually by transforming input bits into output bits. Till now, I have not learned about this in full depth, but I will do it. Till now I have understood about X-OR operation and how it works, Block and Stream Ciphers, basic about AES and DES and Differential Cryptanalysis. I believe I am learning in depth about how cryptography is performed and there are a lot of things that goes in while doing those things. I hope to get more knowledge on the mathematical aspect as I can easily understand the concept but it takes a bit more time to understand the theorems and examples.