CSIT 495/595 - Introduction to Cryptography
Assignment 1

Due: October 27 (Submit in the Class)

Total Points: 45

In this assignment, you will analyze/implement the Cryptographic problems related to prefect secrecy, private-key encryption, MAC, and hash functions discussed in the course. If you have any questions, please post it on the Canvas or contact me during the office hours.

Note that this is an individual assignment. You are free to discuss and share your ideas related to this assignment with other students, however, do not copy. Please solve the following four problems which are from the **textbook** *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell, 2nd Edition, Chapman & Hall/CRC, 2014, unless otherwise specified.

Problem 1: Shift and Perfect Ciphers

(a). Assume a message m is encrypted using the Shift cipher and the resulting ciphertext is as follows?

JBCRCLQRWCRVNBJENBWRWN

What would be the values of m and key k in this case? Please justify your answer. (Hint: you need to do an exhaustive search over 26 possible keys. Extra credit if you write your own code to perform the analysis.) **(10 points)**

(b). Chapter 2, Exercise 2.7. **(5 points)**

Problem 2: Block Ciphers

(a). Chapter 3, Exercise 3.22 **(5 points)**

Problem 3: Message Authentication Code (MAC)

(a). Chapter 4, Exercise 4.8. **(10 points)**

Problem 4: Hash Functions

(a). Suppose you want to verify the integrity of certain files, say system files or software packages downloaded from online. Explain how you can achieve this using MAC and hash functions separately. Also, describe the advantages and disadvantages in using each of this technique with respect to the verification of file integrity. **(10 points)**

(b). Can we use a hash function that is not collision resistant to construct a MAC scheme? Justify your answer. **(5 points)**

What to turn in

1. Please write a report that clearly explains your solutions to the above problems (Note: Please do not simply write down the final answers, i.e., explain your reasoning as well).
2. Please print out all your code, commands and outputs (if any) and attach them in your report.
3. Please submit your report to me in the class on October 27.