CSIT 495/595 - Introduction to Cryptography

Assignment 2 (Due: Dec 1 - submit in the class)

Total Points: 30

In this assignment, you will analyze the Cryptographic problems related to number theory, key distribution and public-key encryption discussed in the course. If you have any questions, please post it on the Canvas or contact me during the office hours.

Problem 1: Number Theory

(a). Answer the following: (i) What is the size of group $\mathbb{Z}_{11}^*$? (ii) Is 3 a generator of $\mathbb{Z}_{11}^*$? and (iii) Is 2 a generator of $\mathbb{Z}_{11}^*$? **(10 points)**

Problem 2: Key Exchange

(a). Suppose p be a prime number and g be the generator of $\mathbb{Z}_p^*$. Consider a scenario where two users Alice and Bob want to generate a shared key secretly on an open channel using the Diffie-Hellman Key-Exchange Protocol. Let us assume that $p = 11, g = 2$ and say Alice and Bob choose 3 and 8, respectively, as their random input integers in the Diffie-Hellman Protocol. What would be the final key shared by Alice and Bob under this case? Please explain your answer. **(10 points)**

Problem 3: Public-Key Encryption

(a). Describe why textbook RSA is not CPA-secure. A solution often used to address this issue is called Padded-RSA. Please explain how Padded-RSA addresses the issue of textbook RSA? **(10 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 submit your report to me in the class on December 1.