CS 478/513: Computer Security

Written Assignment 3
Due: 4/25/22, 11:59 pm
Total points: 100

Please complete the following problems, being sure to explain your conclusions and show your work for all problems. Your solutions must be submitted to Canvas as a PDF file.

This assignment is to be completed individually — plagiarism and cheating are strictly prohibited and are punishable.

Chapter 4:

1. (15 points) This question relates to the Diffie-Hellman secret exchange mechanism. Suppose that Alice and Bob want to derive a shared key and have agreed on a prime $p = 17$ and generator $g = 3$. Alice's private exponent $a = 9$ and Bob's private exponent $b = 5$.
   (a) Alice sends Bob $g^a \bmod p$, and Bob sends Alice $g^b \bmod p$. Show the computation of each of these values.
   (b) Show that Alice and Bob will both obtain the same shared secret from the transmitted values. Compute that secret.
   (c) Suppose that Trudy attempts a Man-in-the-Middle attack on Alice and Bob's key exchange. Trudy has private exponent $t = 7$. Show the process of the attack. Show the values that Trudy sends to Alice and Bob, and compute the shared secrets that she establishes with each of them.
2. (10 points) This question concerns the RSA asymmetric cipher. Suppose Bob uses $e = 7$ and $N = 221$ for his public key.
   (a) Bob wants to encrypt the plaintext $M = 2$ with his public key. What vulnerability is the ciphertext susceptible to? Demonstrate that Trudy can recover the plaintext without Bob's private key.
   (b) The security of RSA is derived from the difficulty of factoring large numbers. In this case, N is relatively small. Factor N into the primes p and q, and find Bob's private exponent d.
3. (10 points) Textbook problem 7.

Chapter 7:

4. (21 points) Complete Problem 7 (a, b, c) from the textbook.
5. (24 points) Complete Problem 10 (a, b, c, d) from the textbook.
6. (20 points) Complete Problem 26 (a, b) from the textbook.