CS 5490/6490: Network Security – Fall 2016
Homework 3
Due by 11:59 PM MT, Wednesday September 21st 2016

- **cs5490 = 33 points, cs6490 = 42 points**
- **No cheating will be tolerated. No copying from the Internet is allowed.**
- **No extensions will be granted.**
- **The code for programming questions and the output files must be submitted using the *handin* utility. The rest of the homework should be submitted through Canvas.**

Question 1:

(a) (*2 points*) Problem 1, Chapter 5, page 143.

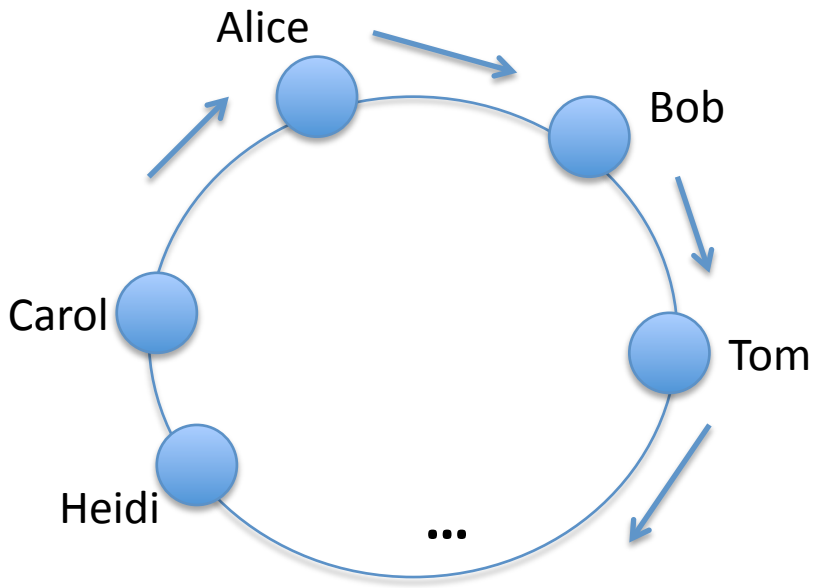
(b) (*3 points*) Problem 8, Chapter 6, page 183.

(c) (*2 points*) Suppose that <7, n_1>, <7, n_2>, <7, n_3>, <7, n_4>, <7, n_5>, <7, n_6>, and <7, n_7> are the public keys of network nodes R1, R2, R3, R4, R5, R6, and R7, respectively. Assume that n_1, n_2, n_3, n_4, n_5, n_6, and n_7 are very large and also relatively prime. A node S sends the same message *m* to R1, R2, R3, R4, R5, R6, and R7 using their respective public keys. An adversary uses the Chinese Remainder Theorem to find $m^7 \bmod n_1n_2n_3n_4n_5n_6n_7 = 410338673$. What is *m*?

Question 2 (Diffie Hellman Key Establishment):

(a) (*2 points*) Encrypting the Diffie-Hellman value with the other side's public key prevents the person-in-the-middle attack. Why is this the case, given that the attacker can encrypt whatever it wants with the other side's public key?

(b) (*2 points*) Consider n network nodes placed in a ring such that each node can only transmit to its nearest neighbor in the clockwise direction. A node can forward messages meant for other nodes in the ring. Each node wishes to establish a separate Diffie Hellman secret key with every other node in the network. Devise an efficient method to achieve this task. Describe your method.



Question 3 (Euclid's Algorithm) ***3 points*****:** Use the Euclid's algorithm described in Section 7.4 of the textbook to show that the numbers 173 and 1013 are relatively prime. Find the values of u and v by drawing a table similar to the one in Section 7.4. What is the multiplicative inverse of 173 modulo 1013? (Note: Remember to include your table in your homework.)

Question 4 (Zero Knowledge) ***9 points*****:**

(a) (*6 points*) Design your *own* zero knowledge proof system for interactive authentication using the ideas presented in Section 6.8 of the textbook. You must present arguments to show that your scheme is secure. (You can find a long list of NP-complete problems in the book by Michael Garey and David Johnson.)

(b) (*3 points*) Transform your scheme into a zero knowledge signature scheme and also show that your signature scheme is secure.

Question 5 (Programming Question) ***10 points*****:** Write a program (in C, C++, C#, Python, or Java), call it EXPO, to efficiently exponentiate big numbers modulo n as described in Section 6.3.4.1 of your textbook. Your program should take three positive numbers as input, one representing the number m, another representing the exponent d to which m is raised to and the third being n. Write client server programs (in C, C++, C#, Python, or Java) using TCP sockets where the client (Alice) and the server (Bob) perform a Diffie Hellman exchange. Use your EXPO program (or function call) to compute the Diffie Hellman numbers. Let g = 1907, p = 784313, S_A = 160011 (Alice's secret), and S_B = 12067 (Bob's secret). Turn in your programs and the output using *handin* (directory HW3). Your ouput must show the numbers sent by Alice and Bob for the Diffie Hellman exchange as well the shared key after the exchange.

Question 6 (Required for cs6490 students, extra-credit for cs5958 students) *9 points*: Read the following paper – "Secret Key Extraction from Wireless Signal Strength in Real Environments," by Premnath *et al*, IEEE Transactions on Mobile Computing, 2012 (http://eng.utah.edu/~cs6490/readings/paper_tmc_secret_key_accepted_version.pdf).

(a) (*2 points*) Briefly describe the properties of the wireless channel between a pair of wireless nodes that enable these nodes to extract a symmetric/secret bit sequence?

(b) (*2 points*) What is the similarity between the secret key extraction presented in this paper and the Diffie-Hellman cryptosystem?

(c) (*3 points*) In this paper, the authors have evaluated secret key extraction in different types of environments. Which type of environment is best suited for secret key extraction? Why?

(d) (*2 points*) What is predictable channel attack? Which settings are more vulnerable to predictable channel attack? Why?