Homework Assignment # 8

Due Date: Wednesday, November 8

In the first few problems we will study some of the properties of cyclic groups. We will only consider the multiplicative group of the $Z_p^\star$ which is of outstanding importance for many public-key schemes.

1. Determine the order of all elements of the multiplicative groups of:

   (a) $Z_5^\star$

   (b) $Z_{13}^\star$

   Create a list with two columns for every group, where each row contains an element a and the order $\text{ord}(a)$.

   (Tip: In order to get familiar with cyclic groups and their properties, it is a good idea to compute all orders "by hand", i.e., use only a pocket calculator. If you want to refresh your mental arithmetic skills, try not to use a calculator whenever possible, in particular for the first two groups. This is not a requirement.)

2. We study now the groups from the problem above.

   (a) How many elements does each of the multiplicative groups have?

   (b) Do all orders from above divide the number of elements in the corresponding multiplicative group? (Property 3 in the theorem from the lecture.)

   (c) Which of the elements from Problem 1 are primitive elements?

   (d) Verify for the groups that the number of primitive elements is given by $\phi(|Z_p^\star|)$. (Property 1 in the theorem from the lecture.)

   (e) Verify for all elements a of $Z_p^\star$ that $a^{|Z_p^\star|} \equiv 1 \bmod p$, with $p = 5$. (This property is usually referred to as "Fermat's Little Theorem" or "Fermat's Theorem".)

3. This problem deals with the subgroups of the groups introduced in Problem 1.

   (a) How many subgroups does each of the groups from Problem 1 have? Exclude the trivial subgroup which only consist only of the element 1. What is the cardinality (i.e., number of elements) of each subgroup? You may want to, but don't have to, draw a diagram for each of the groups circling the subgroups.

   (b) For each subgroup found above, give the complete multiplication table. That is, a square table which describes the multiplication of all subgroup elements with each other.

   (c) For each subgroup found above, provide all primitive elements. Under which condition are all elements of a subgroup, with the exception of 1, primitive elements?

4. Write a program which determines the order of an element of $Z_p^\star$. The program also should give special notice if an element is primitive. The inputs are the field element a and the prime p. Remember to perform a modulo reduction after every arithmetic operation. Determine the order of the following elements a in Z_p:

   (a) $p = 3571, a = 2, 4, 2048$

   (b) $p = 12553, a = 2, 5, 5300$

   Which elements are primitive? (In the next problem we will discuss methods for finding the order of an element that are more efficient than the straightforward approach that you are supposed to implement here.)

5. In practice it is important to be able to find primitive elements for the Diffie-Hellman key agreement protocol and many other public-key schemes based on the DL problem. In this problem we will discuss the computational complexity of this task.

   (a) What is the complexity (given by the average number of steps needed or in big-O notation) for the program implemented in Problem 4? Is this approach feasible for real-size Diffie-Hellman key agreement implementations?

   (b) Do you have any suggestions how we can improve the tests to be performed dramatically? You don't have to provide a complete algorithm, but rather sketch an idea on which an improved algorithm can be based. Hint: Use one of the properties of cyclic groups that we discussed.

6. Compute the two public keys and the common key for the Diffie-Hellman key agreement scheme with the parameters $p = 467$, $\alpha = 2$, and:

   (a) $a_A = 3$, $a_B = 5$

   (b) $a_A = 400$, $a_B = 134$

   (c) $a_A = 228$, $a_B = 57$

   In all cases, perform the computation of the common key for Alice *and* Bob. This is also a perfect check of your results.

7. We design now another Diffie-Hellman key exchange scheme with the same prime $p = 467$ as in Problem 6. This time, however, we use the element $\alpha = 4$. The element 4 has order 233 and generates thus a subgroup with 233 elements. Compute K_{AB} for

   (a) $a_A = 400$, $a_B = 134$

   (b) $a_A = 167$, $a_B = 134$

   Why are the session keys identical?

8. (This problem requires creativity!) We saw in the lecture that the Diffie-Hellman protocol is as secure as the Diffie-Hellman problem which is probably as hard as the DL problem in the group $Z_p^\star$. However, this only holds for passive attacks, i.e., if Oscar is only capable of eavesdropping. If Oscar can manipulate messages between Alice and Bob, the key agreement protocol can easily be broken! Develop an active attack against the Diffie-Hellman key agreement protocol with Oscar in the middle being able to alter messages.