Homework 1 - Algebra

Foundations of Blockchain Technology and cryptocurrencies

Fall 2019

Sharif Blockchain Lab
Sharif University of Technology
Department of Electrical Engineering

Deadline: Yekshanbeh 1398/7/28 At the beginning of the class

(The Homeworks will be collected at the beginning of the class. After 3 minutes of the class the homeworks will not be accepted.)

Note that questions with the tag "optional" have extra points, but those with the tag "no points" are for your own practice and need not be delivered.

Number Theory

1. (12 points) We know the order of $a \in GF(q)$ is the smallest natural number d such that $a^d = 1$ (according to the defined multiplication in the field).
   i. Prove $d|q-1$.
   ii. Prove that the order of a^r is $\frac{d}{gcd(r,d)}$.
   iii. Prove that the order of $\alpha\beta$ is mn, where $\alpha, \beta \in GF(q)$, m is the order of α, n is the order of β and $gcd(m,n) = 1$.

2. (8 points) Assume $p - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, where p is a prime number. Prove that g is a generator in $GF(p)$ if and only if $g^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}$ for all $1 \le i \le n$.

3. (8 points) Recall the discrete logarithm problem. As it was mentioned in the class, the prime number p is better to be a safe prime (i.e $p = 2q + 1$ where q is a prime number). Why?

4. (**optional**, 10 points) This question might be a bit tricky. Recall the discrete logarithm problem in $\mathbb{Z}_p^*$ which is a hard problem. Lets define function f as $f(x) = g^x \bmod p$ where g is a generator and p is a prime number. Alice is sending you t which is $t = f(y)$ and she is not willing to reveal y. How can she prove she knows the value y without fully revealing it? this concept is really useful!!!

Groups and finite fields

1. a. (3 points) Prove that there is one and only one identity element in any group G.
   b. (3 points) Prove that there is one and only one inverse element a^{-1} for a given element a in any group G.

2. Recall creating a finite field of $GF(p^k)$ (where p is a prime number). Construct a finite field with 9 elements:
   i. (10 points) Write the addition and multiplication tables.
   ii. (10 point) Find one generator and show why it is a generator.

3. (3 points) Groups are not necessarily commutative . ($i.e \quad a * b \neq b * a$) Find one group which is not commutative.

4. (15 points) First prove that any finite field F has at least one primitive root (generator). Then prove that there are exactly $\phi(q-1)$ generators in $GF(q)$.
   Hint: You can use results of the first question in the previous section.

5. (**no points**) Prove that the order of a finite field is always p^k for a prime number p and a positive integer k

Cryptography

1. In this question, we learn more about the Diffie-Hellman key exchange protocol.
   i. (8 points) The protocol explained in the class involved two parties, Alice and Bob. Propose a similar protocol for exchanging a key between Alice, Bob and Carol. Try to minimize the communication needed.
   ii. (8 points) Design a "man in the middle" attack on the protocol discussed in the class, by which an attacker that can modify the messages between Alice and Bob, can learn the messages after the key exchange. (**Optional**) Propose a modification on the key exchange protocol to prevent such attack.