СПЕЦИЈАЛНИ КУРС - *ZERO KNOWLEDGE PROOF*

пример испита

1. (5 поена) Објаснити ЗК доказ припадности скупу (тј. да знате тајну која је лист у Мерклеовом дрвету чији је корен (*root*) јаван податак).

2. (5 поена) Објаснити како функционише аритметизација у *PLONK*-у.

3. (5 поена) Нека је дато коначно поље F_p, где је $p = 113$. Нека су дати полиноми $p(x) = 2x^4 - 4x^3 + 4x^2 - 4x + 2$ и $q(x) = x^3 - x^2 + x - 1$. Израчунати вероватноћу да се случајним избором броја из коначног поља F_p погоди заједничка нула полинома p и q.

4. (7.5 поена) Написати *Circom* код за коло којим се проверава да ли особа за дату јавну вредност Посејдон хеша зна број чијим се хеширањем добија та вредност.

5. (7.5 поена) Никола и Милица играју игру "Потапање бродова". Да би се обезбедила поштена игра, а да се притом не открију информације о позицији бродова, неопходно је да се приликом сваког покушаја уз одговор пошаље и ЗК доказ. Подразумева се да је излаз из кола 1 ако је погођен брод, а 0 ако није погођен.

   Објаснити зашто наредни *Circom* код за генерисање ЗК доказа избацује грешку при компилацији и исправити га да буде тачан.

```
include "circomlib/mux1.circom";

template PotapanjeBrodova(N) {
signal input tabla [N][N];
signal input ii;
signal input jj;
signal output odgovor;
signal pogodak;
component polje = Mux1();
for(var i=0; i<N; i++)
{
    for(var j=0; j<N; j++)
    {
        if(i==ii)
        {
            if(j==jj)
            {
               polje.c[0]<==0;
               polje.c[1]<==1;
               polje.s <== tabla[i][j];
               pogodak <== polje.out;
            }
        }
    }
}
odgovor <== pogodak;
}

component main {public [ii, jj]} = Tabla(5);
```