

СПЕЦИЈАЛНИ КУРС - *ZERO KNOWLEDGE PROOF*

септембар 1

1. (5 поена) Дефинисати completeness и soundness у контексту ЗК доказа.
2. (5 поена) Објаснити шта је проблем дискретног логаритма и зашто је он важан за сигурност ЗК доказа.
3. (5 поена) Објаснити аритметизацију у контексту ЗК доказа.
4. (7.5 поена) Никола поседује број индекса који је јединствен за сваког студента на факултету. Факултет је објавио Merkle стабло свих важећих бројева индекса. Никола жели да докаже да је његов број индекса део тог стабла, али да га не открива јавно. Написати Circom коло које Николи омогућава да докаже припадност свог броја индекса Merkle стаблу.
5. (7.5 поена) Ивана жели да учествује у онлајн квизу. Организатори захтевају да кандидат поседује најмање 18 година, али не и да открије своју годину рођења. Ивана је већ комитовала своју годину рођења тако што ју је хеширала и поставила на блокчејн. Написати Circom коло које Ивани омогућава да пружи ЗК доказ да је старија од 18 година без откривања датума рођења.