Homework 1

Use cases

In your teams, think of some use cases of zero knowledge proofs
What problems are there when using zkps in real world situations, such as providing an identity application for use in airports.

Maths Introduction

Some modular arithmetic

1. Working with the following set of Integers S = {0,1,2,3,4,5,6,7,8}

   What is
   a) 4 + 5 = 9 mod 9 => 0
   b) 3 x 5 = 15 mod 9 => 6

2. For S = {0,1,2,3,4,5,6,7,8}
   a) Can we consider 'S' and the operation multiplication to be a group ? YES
   b) Can we consider 'S' and the operation division to be a group ? NO

Background Material

Zero Knowledge podcast - Eli Ben-Sasson
Intro to ZKPs