ZERO KNOWLEDGE MATH

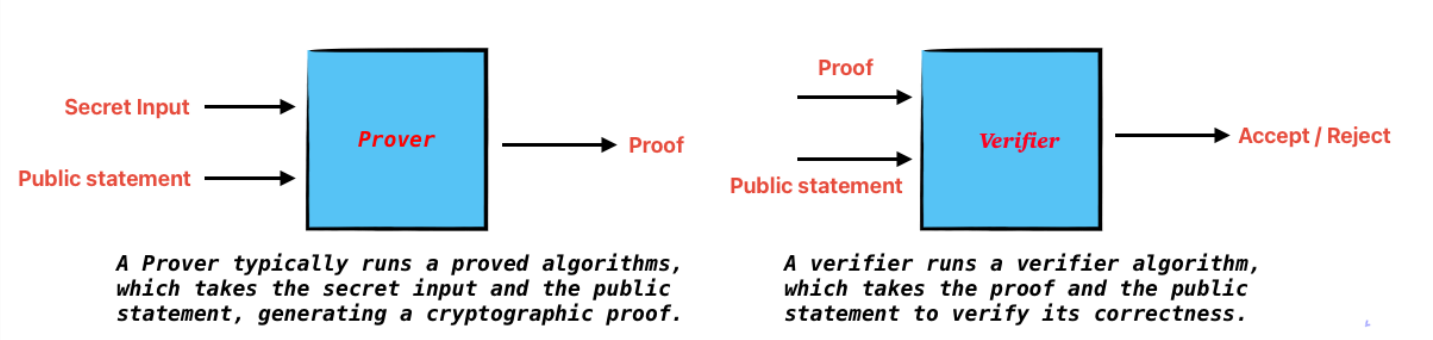
Context for Zero Knowledge:

"Human diginity demands that personal information, like medical and foresnic data, be hidden from the public. But veils of secrecy designed to preserve privacy may also be abused to cover up lies and deceit by institutions entrusted with data, unjustly harming citizens and eroding trust inc entral institutions" -- Starkware.

ZK Overview

What is a Zero Knowledge Proof?

A Zero knowledge Proof is a cryptographic method by which one party called the prover can convince another party called the verifier that the statement is true, without revealing any additional information beyond the validity of the statement itself.



Prover : The ***Prover*** is the party usually an alogiorithm or a program that possess some secret information and that information is called as ***Witness*** and want to prove the knowledge of this secret or the validity of a statement to another party.

Verifier : The ***Verifier*** is a party that can be a program, protocol or smart contract that checks the proof send by the prover and decides whether to accept or reject it.

The Moon Math

There is a lot of math involved that we should learn to understand the Zero Knowledge proofs in depth. As a part of our learning process we will do a lot of problems, paper and pen problems as well as problems in Python.

Modular Arithmetic

Basic Arithmetic contains four operatiosn or functions. Addition, Subtraction , multiplication and division. So the idea of modular arithmetic is to be able to do the four operations using modules.Modules often written as mod refers to the remainder after division of one number by another number.

First lets learn Integer arithmetic and then we will explore modular arithmetic.

Integers : We use $\mathbb{Z}$ as a short descirption for the set of all integers, that is we write integers

$$z = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \tag{1}$$

Integers are also known as whole numbers, that is numbers that can be written without fractional part.There are many other kinds of numbers which are in the image below.