Exploring Elliptic Curve Digital Signature Algorithm (ECDSA)

Thomas Harper

January 14, 2024

Abstract

These are simply my notes on ECDSA, sufficient to complete the RareSkills ECDSA coursework.

1 Introduction

ECDSA is based upon the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP is the problem of finding k given kP where P is a point on an elliptic curve. The ECDLP is believed to be hard, and so ECDSA is believed to be secure.

2 Elliptic Curves

An elliptic curve has the following form:

$$y^2 = x^3 + ax + b$$

There are two constants, a and b. The curve is defined over a finite field $\mathbb{F}_p$ where p is a prime number. The curve is also defined over a point at infinity, denoted $\mathcal{O}$.

3 secp256k1

For secp256k1 specifically, a = 0 and b = 7:

$$y^2 = x^3 + 7$$

It is defined over a field $\mathbb{Z}_p$

- $\mathbb{Z}$ is the set of integers
- p is a prime number
  - ➠ $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
  - ➠ $p = 2^{256} - 2^{32} - 997$
  - ➠ $p = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF$
- $\mathbb{Z}_p$ is the set of integers modulo p