Cryptography 2/14

Reagan Shirk

February 14, 2020

Polynomials over Finite Fields

- Something about being hardware friendly
- What is a finite field?
  - $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$
  - $\mathbb{F}_2 = \{0, 1\}$
  - $\mathbb{F}_2[x] = \{$polynomials in x with coefficients in $\mathbb{F}_2\}$