Cryptography 2/19

Reagan Shirk

February 19, 2020

Polynomial Ring over Finite Field ($\mathbb{F}_2$ in particular)

	$\mathbb{Z}$	$\mathbb{F}_p$[x]
Cardinality	Infinite	Infinite
	primes	irreducibles
	$\frac{\mathbb{Z}}{p} \approx \mathbb{F}_p$	$\frac{\mathbb{F}_2[x]}{(f(x))} \approx \mathbb{F}_p n$
	XCGD, CRT	XGCD, CRT
Factorization	Hard	Easy
	Security	Error-correcting code

AES

- Bytes $\iff \frac{\mathbb{F}_2[x]}{x^8+x^4+x^3+x+1}$
- Most of the lecture has been him doing stuff on Sage, tbh I have no idea what's happening and haven't had an idea of what's happening since Friday of last week
  - I'm totally lost. Someone halp

Don't know what this is pertaining to...oops

- For every prime p and every $n \in \mathbb{Z}^+$, there is a field of p^n elements and it is unique
- For every finite field $GF(p^n)$, there exists a multiplicative generator
- $p =$ characteristic of the field
  - If you add elements p times, you'll get 0 (or at least 1? I couldn't tell what he said)