Cryptography 2/17

Reagan Shirk

February 17, 2020

Irredicubles in $\mathbb{F}_2[x]$

- $x^2 + 1$ is reducible
- $x^2 + x + 1$ is irreducible
- $x^3 + 1$ is reducible
- $x^3 + x + 1$ is irreducible
- He wrote $\frac{\mathbb{F}_2[x]}{x^3+x+1}$ on the board and I haven't the *slightest* clue what he's talking about
  - I don't know when the midterm is but I know it's going to kill me
  - $a \equiv x \bmod x^3 + x + 1$
  - Apparently $\frac{\mathbb{F}_2[x]}{x^3+x+1} = \{0,\ 1,\ a,\ a+1,\ a^2,\ a^2+1,\ a^2+a+1\}$
- In general:

$$|\mathbb{F}_p[x] \bmod (f(x))| = p^{deg(f)}$$

- Inverse of $(a + 1)$
  - $\gcd(x^3 + x + 1,\ x + 1)$
  - You do this by doing long division, I wrote it down so I'll try to remember to upload a picture
  - $(x^3 + x + 1) = (x^3 + x)(x + 1) + 1$
  - Inverse of $(a + 1) = a^2 + a$
- If $f(x)$ is irredicuble, then $\left|\left(\frac{\mathbb{F}_p[x]}{f(x)}\right)^*\right| = p^{deg(f)} - 1$
- p is a characteristic of the finite field
- Something in sage?
  - F2x.=GF(2)[]