Cryptography 2/28

Reagan Shirk

February 28, 2020

???

- $\Pi(n) = \#\{p \leq n \mid p \in prime\}$
- $\Pi(n) \approx \frac{n}{\log(n)}$
- Factoring in $\mathbb{Z}$ is hard but factoring in $\mathbb{F}_2[x]$ is easy
- In $\mathbb{F}_{p^n}$, the number of multiplicative generators is:

$$\frac{\phi(p^n - 1)}{p^n - 1}$$

Block Cipher

- Random substitution, while very safe, makes your codebook too big
- You can do a permutation cipher to make the codebook smaller but it's not all that safe tbh
  - Your keyspace is $n!$ and your ciphertext space is $|\Sigma|^n$
  - You can create a permutation matrix, where the inverse of the matrix is the decryption of the message
    - **I'll try to remember to upload a picture of this at some point**
- You also have a linear cipher/hill cipher
  - $\overrightarrow{c} = A\overrightarrow{m}$
  - This is encryption, A is invertible $\iff$ $\det(A)$ is a unit
  - plaintext and chiphertext spaces are Σ^n, the keyspace is...? Σ^{n^2}?