Cryptography 2/10

Reagan Shirk

February 10, 2020

Chinese Remainder Theorem

- Let $m_1, \cdots, m_n$ be integers such that they are pair wise relative prime
  - Basically, $\forall\ i, j$ where $i \neq j,\ \gcd(m_i, m_j) = 1$
- Then the below congruence system has a unique mod$M$ where $M = \Pi\ m_i$, there is always a solution, and every solution can be found efficiently

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_1 \bmod m_2 \\ &\cdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

- Algorithm for this I guess? More like steps
  - $M_i = \frac{M}{m_i}$
  - $y_i = M_i^{-1} \bmod m_i$
  - $x = \Sigma_i y_i M_i$
- How do we prove the last point above?
  - Calculate $x \bmod m_i$
  - We need to remember from the formula that we have M_i, and if the i in M_i is different than m_i...something happens? Everything else is gone...for some reason
    - M_i is every single one of the $m's$ except for m_i because you divide by it
    - Therefore we can say that $x \bmod m_i = a_i y_i M_i = a_i$
  - This is also somehow relevant

$$\begin{aligned} x_1, x_2 \\ x_1 - x_2 \bmod m_i = 0 \\ \forall\ i,\ m_i | x_1 - x_2 \\ \Rightarrow \Pi\ m_i | x_1 - x_2 \end{aligned}$$

- What is this? I don't know
  - $\frac{\mathbb{Z}}{m\mathbb{Z}} = \frac{\mathbb{Z}}{m_i\mathbb{Z}} \bigoplus \frac{\mathbb{Z}}{m_r\mathbb{Z}} \bigoplus \cdots \bigoplus \frac{\mathbb{Z}}{m_n\mathbb{Z}}$