Cryptography 1/13

Reagan Shirk

January 13, 2020

Number Theory

- Why is number theory important to cryptography?
- Whole numbers, integers, rational numbers, algebraic numbers, prime numbers
  - Prime Numbers
    - Every even number $n \geq 4$ is a sum of two prime numbers:

      $$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 12 &= 5 + 7 \\ 16 &= 13 + 3 \\ &= 5 + 11 \end{aligned}$$

    - This is the **Goldback Conjecture**
    - This is hard to prove, all of number theory is like this
  - You're looking for a problem that fits this description:
    - The problem can be described in one page
    - Understandable by a high school student
    - Answer can be verified easily and you know the answer
    - Nobody can solve it in 1000 years
      - This type of problem that is useful in Cryptography- the answer you know is easily verified but no machine, no matter how powerful, can solve it for 1000 years

        ```
        p = next_prime(108342708501349583427642962044395871435602984436)
        q = next_prime(213409843572345092348572435130958345780342623445)
        n = p * q
        ```
      - `n` is still calculated very quickly even though p and q are incredibly large. However, you can't find `n!` in a reasonable amount of time