Cryptography 1/17

Reagan Shirk

January 17, 2020

Last Time

- Bit complexity - very important in cryptography
- Easy and hard - the gap between easy and hard is *huge* in cryptography
  - You want the right people to have easy access, the wrong people to have hard access
- Size of representations - an integer has a size
  - N = integer, n = size
  - $n = log_2(N)$
  - You want to make sure that your algorithm is polynomial in n, not N

Multiplication

- Mathematically, we look for $M \times N$
  - This algorithm is v bad when the numbers are big, you end up with an exponential time algorithm
- What is the better algorithm?
  - Long multiplication - easy to implement in binary
  - The binary numbers have n bits, so the complexity is $O(n^2)$
  - Why is it n^2?
    - With binary numbers of length n, the result will be length $2n$ and you will have to perform n number of operations, and somehow this comes to n^2
      - Ohhh because each operation requires $O(n)$ so you have n operations that require n time and end up with n^2 overall
- There's also a divide and conquer method called Karatsuba that has $O(n^{1.585})$
- FFT is even better with $O(nlog^2(n))$
- We want to get to $O(n)$ in the future but we haven't gotten there yet
- We've gone over multiplication and addition, what next?
  - Not subtraction, it's the same as addition
  - Division? You can do long division, it's an $O(n^2)$ algorithm that's very similar to multiplication
- This is all if you use binary, what if you use something else? Like messages
  - You can convert the message into a binary number

Base Change

- Turn decimal into binary, etc
- We have to do this in our homework
- Base 26 because of the alphabet
  - Divide number by 26
- ASCII - unicode

Primes and Divisors

- Unique factorization: an integer can be written uniquely as a product of primes, up to reordering, I still don't entirely understand this
- Divisors:
  - a is a divisor of n if there exists a k in $\mathbb{Z}$ such that $n = ak$
    - This is denoted as $a|n$
    - If two integers do not divide, it's written as $n \nmid a$
- Theorem (we should be able to prove):
  - If $a|b$ and $b|c$, then we conclude that $a|c$, assuming that $a, b, c \in \mathbb{Z}$
    - This shows that division is transitive
  - If $a|b$ and $b|a$, then we conclude that $|a| = |b|$
  - If $a|b$ and $a|c$, then we conclude that $a|b + c$
- Proof of third theorem:
  - *I'll post a picture, I don't wanna type all that LaTex*
- Aside: In sage, if you need the set notation for something, it's just the letter twice
  - i.e. $\mathbb{Z} = ZZ$
- No idea what he's talking about but I'll write it down
  - In general, you can factor a number n into $n = P_1^{e_1} \cdots P_n^{e_n}$, which means the number of divisors of n is $2(e_1 + 1)(e_2 + 1) \cdots (e_n + 1)$