CS70 In Simpler Terms - Note 10

written by Kevin Liu cs70.kevinmliu.com

August 1, 2017

1 RSA

- Encrypt message x: $E(X) = x^e \pmod{N}$, $N = pq$ (large primes)
- Decode $m = E(x)$: $D(m) = m^d \pmod{N}$, where d is the M.I. of e $\pmod{(}p-1)(q-1) \Rightarrow gcd(e,(p-1)(q-1)) = 1$ ensures that d exists *since e is relatively prime with $(p-q)(q-1)$*
- $D(E(x)) = x \pmod{N} \Rightarrow E$ is a bijection - $x^{ed} = x \pmod{N}$
  Proof:
  - $ed = 1 \pmod{(}p-1)(q-1) = 1 + (p-1)(q-1)k$
  - $x^{ed} - x = x^{1+k(p-1)(q-1)} - x = x(x^{k(p-1)(q-1)} - 1)$
    We are trying to show that the above statement $\equiv 0 \pmod{N}$, because then we will have proven that $x^{ed} \equiv x \pmod{N}$
  - We can do this by showing that x is divisibly by p and x is divisible by $q \Rightarrow$ divisible by pq
    - case 1: x is a multiple of p, in which case we are done
    - case 2: x is not a multiple of p so using FLT
      $x^{p-1} \equiv 1 \pmod{p} \Rightarrow (x^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \pmod{p} \equiv 1 \pmod{p} \Rightarrow$
      $x^{k(p-1)(q-1)} - 1 \equiv 0 \pmod{p} \quad \square$
  - the proof for the case where $q|x$ is analagous

2 Polynomials

- degree d polynomial has at most d roots
- need $d+1$ points to uniquely determine polynomial of degree d
- Lagrange interpolation - used to find a polynomial of lowest degree, given a set of points

  Formula for calculating the final polynomial $p(x)$ of degree d
  $p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$, after constructing $d+1$ polynomials $\Delta_i(x)$

  Formula for finding the individual polynomials, $\Delta_i(x) = \frac{\Pi_{j\neq i}(x-x_j)}{\Pi_{j\neq i}(x_i-x_j)}$

Example: Find the polynomial of lowest degree that passes through the points $(1,1),(2,2),(3,4)$

- $d=2, x_i=i$
- $i=1$, $\Delta_1(x)=\frac{(x-2)(x-3)}{(1-2)(1-3)}$
  * This makes sense because at $x=2, x=3$, $\Delta_1(x)=0$, and at $x=1$, $\Delta_1(x)=1$, so $y_1\Delta(x)=1(1)=1$ which is correct
- $i=2$, $\Delta_2(x)=\frac{(x-1)(x-3)}{(2-1)(2-3)}$
- $i=3$, $\Delta_3(x)=\frac{(x-1)(x-2)}{(3-1)(3-2)}$

3 Finite Fields F_m or $GF(m)$

Restricting the fields to $\pmod{m}$

- x has inverse $\pmod{m}$ iff$gcd(m,x)=1$ so m is prime
- $x \in \{1,...m-1\}$ all have an inverse $\pmod{m} \Rightarrow$ bijection
- How many polynomials are there of degree at most 2 $\pmod{m}$?
  - There are 3 coefficients in a degree 2 polynomial
  - Each coefficient has m values to choose from $\{0,...m-1\} \Rightarrow m^3$ polynomials

  The chart below summarizes the result above:

Polynomials of degree $\leqslant d$ over F_m

Number of points given	Number of polynomials
$d+1$	1
d	m
. . .	. . .
0	m^{d+1}