MATH 314 Spring 2018 - Class Notes

11/07/18

Scribe: Cole Bauer

Summary: Cracking RSA.

- If Eve wants to crack RSA, she has to find the decryption exponent "d"

- $n = pq$
- e Encryption Exponent for the encryption m, $m^{\varphi}(mod(n))$
- $d \equiv e^{-1} mod^{\varphi}(n)$ (You have to know the p and q in order to find this.)
- Eve has to factor n in ordert to get "d". What is the best way to do that?

1. If p and q have size 150 digits, trial division is not feasible
2. If we try to divide n by numbers up to around $sqrt(n)$ this table takes O($sqrt(n)$) time.

- FACTORING TRICK: If we find numbers x and y, where x $\neq y$ (mod (n)) and x $\neq -y(mod(n))but$x$^2 \equiv mod(n))$ then d = gcd(n,x-y) is a non-trivial factor of n. Why is this?

- Suppose $x^2 \equiv y^2(mod(n))/x^2 - y^2 \equiv 0(mod(n))$

So, n — $x^2 - y^2$

$(x + y)(x - y)$

n — $(x + y)(x - y)$

So since n divides this product if d = gcd (n, x-1)=1, then n has to divide (x+y). This means that x+y=0(mod(n)) which means x $\equiv y(mod(n))$

If the gcdd(n, x-y) = n then n divides (x-y) but that means x-y $\equiv$ 0nd x $\equiv y(mod(n))$

If we can find x and y with $x \neq + - y$ and $x^2 \equiv y^2$ mod(n)), we win

First we try to use this trick:

- Pick numbers x(mod(n))

- Randomly square them
- Take the remainder mod(n)
- If we land on a square, we win

How long does this take? How hard is it to find a square? What is the probability that a random number (mod(n)) is a square?

How many of the numbers [1,n] are squares? $\sqrt{n}$, the probability is $\sqrt{n}/n = 1/\sqrt{n}$

This takes about $\sqrt{n}$ steps with running time O($\sqrt{n}$)

DIXONS FACTORIZATION ALGORITHM (QUADRATIC SIEVE):

- Pick numbers (mod(n)) call this x
- compute $c = x^2 mod(n)$ remainder when x^2 is divided by n
- Try and factor c into small prime factors using trial division (small prime factors meaning B $\sim e^{\sqrt{logn}}$)
- If all small prime factors of c are less than b, we keep (x,c) otherwise throw it away and keep going.
- Call numbers with only small prime factors (smooth) $46 = 2 * 23$ not smooth because 23 is a big prime, smooth must have all prime factors $<$ "d"
- Repeat this until we have $\Pi(B)$ many pairs (x,c) — $\Pi(B) \Longleftarrow$ (equals the count of how many primes up to B)

Make a matrix where each column is a prime number up to "b" and each row corresponds to a "c" then entry in position (c,p) is the number of times that "p" divides "c". Each row gives the factorization of "c" into primes up to "b". THis matrix has more rows than columns. Linear algebra implies there has to be a collection of rows that sum to give all even entries.

This means that you can multiply the c's from these rows gives a number where every prime occurs at an even number of times (a square)! Let c1, c2...ck be these rows and x1, x2...xk corresponding values of x

Let X= $x1^2$, $x2^2$ ... $xk^2 = x^2$ — Y = c1, c2 ... ck = y^2

- $x^2 \equiv X \equiv Y \equiv y^2 (mod(n))$

- usually $x \neq y(mod(n))$ so we win

  This runs in $O(e^{\sqrt{logn}})$ How does this compare to $\sqrt{n} = n^{1/2}$

  Compare $e^{\sqrt{logn}}$ with n^c and $logn^d$

  - $ln(n^c) = c * ln(n)$
  - $ln(\sqrt{e}^{ln(n)}) = \sqrt{l}n(n)$
  - $ln((ln(n))^d) = d * ln * ln(n)$
  - $O(e^{\sqrt{log(n)}})$ is between polynomial and exponential growth