MATH 314 Fall 2019 - Class Notes

4/13/2020

Scribe: Daniella Diaz

Summary: In class we learned about RSA.

Notes: Alice picks two random primes p and q. She computes $n = pq$ and picks an e where $gcd(e, (p-1)(q-1)) = 1$. Alice tells everyone (n, e), then secretly uses p and q to compute $e(n) = (p-1)(q-1)$. She then computes $d = e^{-1}(mod\ e(n))$ by using Euclid's Algorithm. Once she computes d, she can forgot about p and q.

d is now Alice's secret decryption key.
To send a message $m < n$, Bob uses Alice's key (n, e) to computer $C = M^e(mod\ n)$. k sends this to Alice...

To Decrypt: Alice computes, $C^d(M^{ed}) = M^{ed}(mod\ n)$

Since, $de = 1(mode(n))$
$de = 1 + ke(n)$

so, $C^d = m^{1-ke(n)}$
$= m(m^{e(n)})^k = 1$ by Euler Theorem
$= m(modn)$

Decryption Function: $D(y) = y^d(mod\ n)$

Since, $d = e^{-1}(mode(n))$, Eve needs to find $e(n)$ so factor n!
Factoring n is equally hard as computing e(n)

$$
\begin{aligned}
\text{Since,}\quad e(n) &= (p-1)(q-1) \\
&= pq - p - q + 1 \\
n - e(n) + 1 &= \cancel{(pq)} - (\cancel{(pq)} - p - q + \cancel{1}) + \cancel{1} \\
&= p + q \\
n &= pq
\end{aligned}
$$

$$
\begin{array}{ccc}
a & b & c \\
\downarrow & \downarrow & \downarrow
\end{array}
$$

$x^2 - (n - e(n) + 1)x + n$
$= x^2 - (p+q)x + pq = (x-p)(x-q)$

Now, Quadratic Formula: $p, q = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

$= \frac{(n-e(n)+1) \pm \sqrt{(n-e(n)+1)^2-4n}}{2}$

$\therefore$ *Computing* e(n) *allows us to factor* n = 99

Trial Division: $\sqrt{n}$

If n has x bits then the trial division $n \approx 2^x$

This is $2^{x/2}$ steps too slow!

Use Fermat's Primality Test: If n is prime then,

$a^{n-1} = 1(mod\ n)$ for all a not divisible by n but,

-Lots of false positives

-Carmichael numbers

Solovay-Strasser Primatlity: using Jacobi Symbols,

$$(\frac{a}{n}) = \begin{cases} 1, & \text{if } n \text{ is prime and } a = x^2 (mod\ n). \\ -1, & \text{if } n \text{ is prime and } a \neq x^2 (mod\ n). \end{cases} \tag{1}$$

Theorem (Euler) if n is prime and α is not divisible by n then $(\frac{a}{n}) = a^{(n-1)/2} (mod\ n)$

Steps:

Pick random $a < n$

if $(\frac{a}{n}) \neq a^{(n-1)/2} (mod\ n)$

return "composite"

repeat 10 times

return "probably prime"