Class Notes 4/13

Logan Smith

May 8, 2020

RSA: Pulbic Key Cryptography (Alice has public key. She tells everyone, people send her message that only she can decrypt)

she picks 2 large random prime p q
n=pq
she picls an e
gcd(e,(p-1)(q-1))=1
her public key is (n,e)
alice computes $\varphi(n) = (p-1)(q-1) andusesthistofind$
$d \equiv e^{-1}(mod \varphi(n))$

Using Euclid's Algorithm

Bob can send Alice a message m<n

He computes c $\equiv m^e(mod \varphi(n))$

TO decrypt Alice computes c$^d(modn)$
$sinceed = 1(mod\varphi(n))$
$ed = 1 + k\varphi(n)$
$soc^d \equiv (m^e)^d = m^{ed}$
$\equiv m^{1+k\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k(modn) \equiv m(modn)$
$soalicecandecrypt$

If eve knows n why can't she use this to decrypt bob's message?
The decryption function is:
D(y)=y$^d(modn)$
$Evehastofindd$
$d \equiv e^{-1}(mod\varphi(n))$

Eve cannot compute this without knowing $\varphi(n)$. So eve need to know $\varphi(n)$. If she can factor n=pq, then eve could break RSA (find d) but factoring is hard(no one knows a fast way to do it for big n).

Maybe she could find $\varphi(n)$ some other way?

Claim: Computing $\varphi(n)$ is equally as hard

If you found a way to compute $\varphi(n)$ you could use it to find p and q (factor n). How do you do it?

Suppose you manage to learn $\varphi(n)$

know $\varphi(n) = (p-1)(q-1) = pq - p - q + 1$
$n - \varphi(n) + 1 = p + q$
Use quadratic formula to find p q:
$x^2 - (n - \varphi(n) + 1) + n = 0$
$x^2 - (p+q) + (pq) = 0$
This factors as

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

$= \frac{n - \varphi(n) + 1 + \sqrt{(n - \varphi(n) + 1)^2 - 4(1)(n)}}{2(1)}$
Since factoring is hard it is hard find $\varphi(n)$ or d
Test if n is prime. Trial division test if n is divisible by any number $\sqrt{n}$ (really slow)

Fermat primality test: Fermats little theorem: If n is prime and $1 \leq a < n$ then $a^{n-1} \equiv 1 (mod n)$ steps: (repeat 10 times) pick a random $a < n$ if $a^{n-1} \equiv 1 (mod n)$
return composite
else return "probably prime"
drawbacks:
lots of psuedoprimes(false primes)
carmichael numbers (fermat's test always lies)
too many mistakes for RSA
Solovay Strassen Test:
Use jacobi symbols $(a, n) = \{$ 1 if n is prime and $a \equiv x^2 (mod n)$
-1 if n is prime and $a \not\equiv x^2 (mod n)$
If n isnt prime the symbol doesn't tell us if a is a quadratic residue
Theorem(Euler)
If n is prime and $a \leq a < n$ then $(a, n) \equiv a^{\frac{n-1}{2}} (mod n)$

steps: repeat 10 times pick a random a<n
if $(a, n) \not\equiv a^{\frac{n-1}{2}} (mod n)$ return composite else return probably prime

why is solovay strassen better?
if n is composite, there is always some a which shows this using solovay strassen no carmichael 's in fact if n is composite then atleast 1/2 of the choices for a tell it is composite

if we do this test N times the probability of getting probably prime everytime when the number is composite is at most $\frac{1}{2}^n$