Randomized Primality Testing

Fermat's Little Theorem

Let N be a prime number, then for all $1 < a < N$

$$a^{N-1} \equiv 1 \mod N$$

(Implicit: a and N are relatively prime)

$$Z_N^+ = \{1, 2, \dots, N-1\}$$

Z_N^+: Positive remainders

Let $x \neq y$, $x, y \in Z_N^+$

Then $ax \not\equiv ay \mod N$

If we multiply $x \neq y$ by a, i.e. $ax \neq ay$ then $ax \neq ay$

$$Z_N^+ \cdot a = \{1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (N-1) \cdot a\} = Z_N^+$$

Just a permutation of elements

$$Z_5^+ = \{1, 2, 3, 4\} \qquad a = 2$$

$$Z_5^+ \cdot a = \{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, 4 \cdot 2\}$$

$$= \{2, 4, 1, 3\}$$

If $x \neq y$, then $ax \not\equiv ay \mod N$

Proof: Assume to the contrary that

Proof: Assume to the contrary that

$$ax \equiv ay \bmod N$$

$$\Rightarrow ax - ay \equiv 0 \bmod N$$

$$\Rightarrow a(x-y) \equiv 0 \bmod N$$

we know that $a \neq 0$

$$\Rightarrow x - y = 0$$

$$\Rightarrow x = y$$ ⊗ contradiction!

$\Rightarrow$ assumption is wrong

$$\Rightarrow ax \not\equiv ay \bmod N$$

$Z_N^+ = Z_N^+ \cdot a$ simply a permutation of Z_N^+

$$Z_N^+ = \{1, 2, \ldots, N-1\}$$

$$\prod Z_N^+ = 1 \times 2 \times 3 \times 4 \cdots \times N-1$$

multiply all element of Z_N^+ $= (N-1)!_0$

$$Z_N^+ \cdot a = \{1 \cdot a, 2 \cdot a, \ldots (N-1)a\}$$

$$\prod Z_N^+ \cdot a = (1 \cdot a) \times (2 \cdot a) \times (3 \cdot a) \cdots \times ((N-1) \cdot a)$$

$$= a^{N-1} \cdot (N-1)!_0$$

$$a^{N-1} (N-1)!_0 \equiv (N-1)!_0 \bmod N$$

$(N-1)!_0$ is relatively prime to N

$1 \times 2 \times 3 \times \cdots N-1$

$\Rightarrow ((N-1)!_0)^{-1}$ must exist

$\Rightarrow \left((N-1)!\right)^{-1}$ must exist

multiply by the inverse on both sides

$$a^{N-1} \equiv 1 \mod N$$

$n = \log_2 N$

$O(n^3)$ time primality testing!

Is Prime (N):

Pick a randomly, such that $1 < a < N$

let $z = a^{N-1} \mod N$ ←

if $z = 1$

return true | Prob of error $\leq 1/2$

else

return false | Certain

Repeat k times

$P(\text{error}) \leq \left(\frac{1}{2}\right)^k$

Carmichael: pseudo prime

If N is not a prime, but N is a carmichael number

then $\forall$ a relatively prime to N

$$a^{N-1} \equiv 1 \mod N$$

1st carmichael #

$N = 561 = 3 \cdot 11 \cdot 17$

If N is composite and N is not carmichael

$\exists$ a such that, with a relatively prime to N

$$a^{N-1} \not\equiv 1 \mod N$$

then in this case we can have no more than $N/2$ value that pass the fermat test

Let b be any other number $1 < b < N$

let $b^{N-1} \equiv 1 \mod N$ } b passes the fermat test

then $(a \cdot b)$ will not pass the test

$$(a \cdot b)^{N-1} = a^{N-1} \cdot b^{N-1} \mod N$$

$$= a^{N-1} \mod N$$

$$\neq 1$$

for every b that passes fermat test,

$\exists (a \cdot b)$ that does not pass the test

$N-2$ choices

at most $\frac{N-2}{2}$ can pass the test

$\leq \frac{1}{2}$

Miller-Rabin Primality

IsPrimeMR(N):

(0) If N is even & not 2, return false, else return true

(1) pick a randomly $1 < a < N$

(2) // we need to compute $a^{N-1} \mod N$

$N-1 = u \cdot 2^t$ e.g.: $560 = 35 \cdot 2^4$

$N-1$ even

// we need to compute $\left(a^u\right)^{2^t} = a^{N-1}$

$N = 561$

$N-1 = 560$

560	2
280	2
140	2
70	2
(35)	

(3) Compute $z = a^u \mod N$ $\leftarrow O(n^3)$ time

If $z \equiv 1$ then return true

If $z \equiv 1$ then return true

// start squaring for at most t times

$O(n^3)$ time overall

// while squaring make note of the first time we encounter a 1

$z = a^u \bmod N$ ← $z \neq 1$

for $i = 1, 2, \ldots, t$

$z = z^2 \bmod N$ ← $O(n^2)$

If $z = 1$ and prev z is not $N-1$ then return False

Carmichael test

Return True

$P(\text{error}) \leq 1/4$

$t \cdot n^2 \leq n^3$

$a^u = 1$

$(a^u)^{2^t} = (1)^{2^t} = 1$

If we encounter a 1 while squaring and prev value was not $N-1$, the N must be composite

$z_p \neq 1$ ← prev value

let $z = (z_p)^2 \equiv 1 \bmod N$

If $z_p = -1 \equiv N-1 \bmod N$

$(-1)^2 = 1$

$\Rightarrow$ z_p is a non-trivial square root of 1

$z_p^2 \equiv 1 \bmod N$

$z_p \neq 1, \; z_p \neq -1$

$z_p^2 - 1^2 \equiv 0 \bmod N$

$(z_p + 1)(z_p - 1) \equiv 0 \bmod N$

$\Rightarrow (z_p + 1)(z_p - 1) = N \cdot t$

$\Rightarrow$ $z_p + 1$ divide N

or $z_p - 1$ divide N

$\Rightarrow$ z_{p-1} divide N

$\Rightarrow$ N is not a prime

Primality Testing ✓

Generating Large Prime numbers ?

GeneratePrime (n): n # of bits for the prime

① generate a random n bit number, store it in V

② res = IsPrimeMR(V, k) — $O(n^3)$ — # of repeats

prob(error) $\leq \frac{1}{4^k} \leq \varepsilon$ ← User threshold

③ If res = True return V

else goto ①

# of times we have to repeat?

$O(n)$ Expected # of repeats.

One trial is expected to return a prime with prob $p = 1/n$

Q: how many trials must one do before encountering a prime?

Expected Time : on average

$\pi(x)$: # of primes $\leq x$ ← value

$\pi(x) \approx \frac{x}{\ln x}$

n-bit numbers

$N = 2^n$ largest n-bit number

$\pi(N) \approx \frac{N}{\ln N} = \frac{2^n}{n}$

Q: what is the probability of picking a prime number in the range

$1 \ldots N$

$1 \ldots 2^n$

Q: how many trials before first success, if prob of success $= \frac{1}{n}$

$(2, 3, 4, 5 \ldots \ldots (N)$

success $= \frac{1}{n}$

Ans: geometric random variable

$E[\#\text{ of trials}] = n$

$\frac{1}{n} \cdot n = 1$

$(2, 3, 4, 5 \ldots \ldots \underset{\text{pick at random}}{\textcircled{V}} \ldots \ldots N)$

$P(\text{prime}) = \frac{\#\text{ of prime}}{\text{total \# of value}} = \frac{\pi(N)}{N} = \frac{\frac{N}{\ln N}}{N} = \frac{1}{\ln N}$

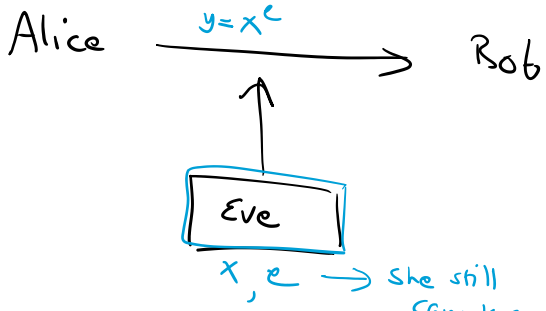
$\simeq \frac{1}{n}$

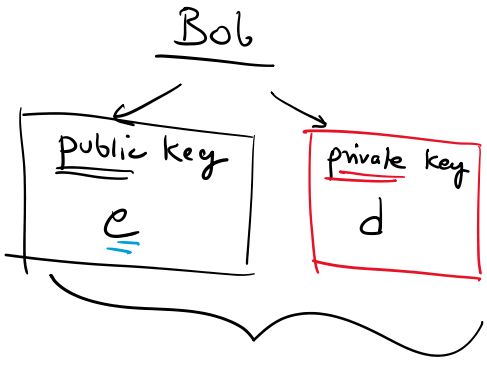
RSA cryptography

↳ Rivest, Shamir, Adleman

public-key cryptography

Integers: x, e, d





① Alice wants to send message x to Bob

$y = \text{Encoding}(x) = \boxed{x^e}$

② When Bob gets the encrypted message y

$X = \text{Decode}(y) = \boxed{y^d} = (x^e)^d = x^{ed}$

Bob: ① generate 2 large random prime numbers $O(n^3)$

(1) generate 2 large random prime numbers $O(n^3)$

p, q

$n = 4096$

$p \approx 2^{4096}$ $q \approx 2^{4096}$

security relies on hardness of prime factorization

(2) $N = p \cdot q$

Knowing N, it is extremely difficult to factorize it into p, q

but it can be done in P time on Quantum Computers

Any small prime # is o/c

(3) Choose e, public key such that it is relatively prime to $(p-1)(q-1)$

(4) Compute d, private key

$d \equiv e^{-1} \mod (p-1)(q-1)$ $O(n^3)$

$e \cdot d \equiv 1 \mod (p-1)(q-1)$ ← Ext Euclid to get $e^{-1} = d$

(5) Bob publishes (e, N) as the public info

(d, N) kept private.

---

1) Alice wants to send x. (Using Bob's public key (e, N))

Encoding $(x) = y = x^e \mod N$

2) Bob decodes y, private key (d, N)

Decode $(y) = y^d \mod N$

$$\text{Decode}(y) = y^d \bmod N$$

$$= (x^e)^d \bmod N$$

---

prove: $x^{ed} \equiv x \bmod N$

$x^{ed} - x$ is divisible by N

$e, d \qquad d = e^{-1}$

$ed \equiv 1 \bmod (p-1)(q-1)$