

Primes & Crypto

Probability testing

prime numbers are frequent

 $\pi(x) = \# \text{ of primes from } 1 \text{ to } x$

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

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} \rightarrow 1$$

 \rightarrow need prime testing to find random primes \rightarrow fraction of primes in 1 to 10^{250}

$$\frac{10^{250}}{250 \ln 10} \approx \frac{10^{250}}{690}$$

$$\left(\frac{1}{690} \right)$$

~~also throw out~~ multiples of 5, 3 early

Find a (random) prime approach

 \rightarrow Pick a random # from 1 to 10^{250}

TEST if prime

yes \rightarrow return prime (big, most #s $> 10^{240}$)

else repeat

Baseline

test if prime up to \sqrt{n} not prime $\Leftrightarrow \exists$ a prime factor $\leq \sqrt{n}$
(prime factorization)

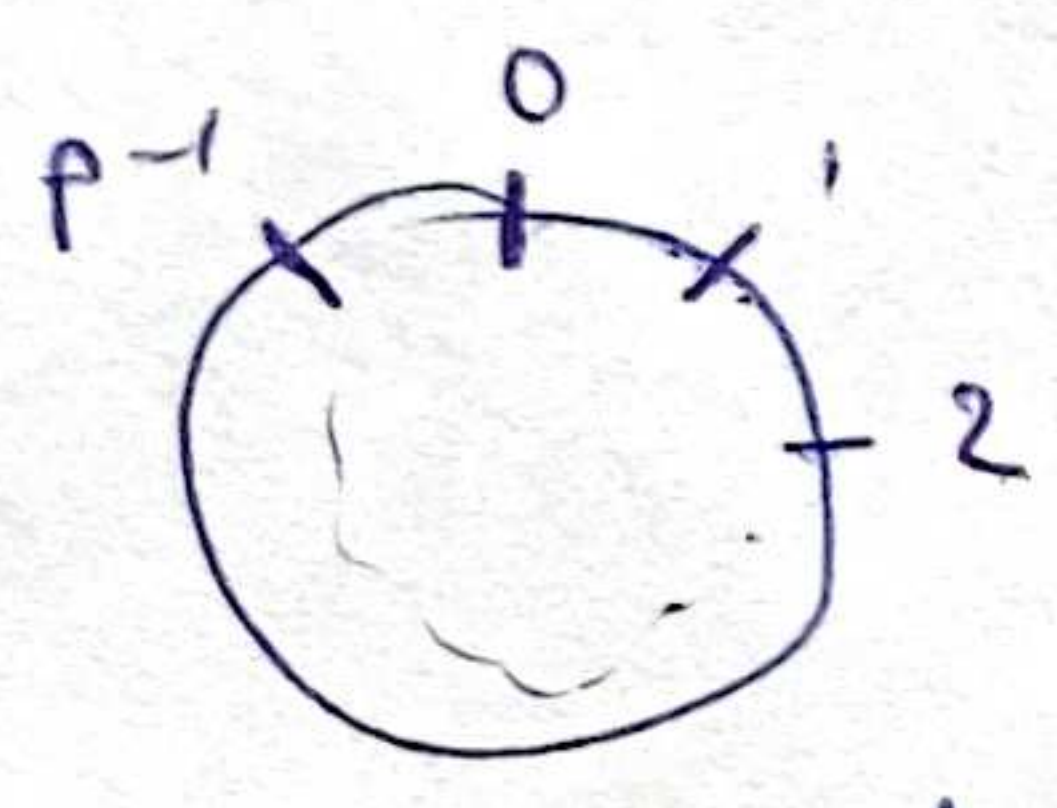
! exponential in # of digits, bits (representation size)

$$\sqrt{10^{250}} = 10^{125}$$

we want $O(\log n)$ alg, based of # of digits/bits
 \uparrow
bits

$\text{mod } p$: remainder when divided by p

$x = y \text{ mod } p$: remainder of x is equal to remainder of y after dividing by p .



multiplicative inverse: $a \neq 0 \text{ mod } p$, then $\exists a^{-1}$, s.t. $aa^{-1} = 1 \text{ mod } p$

ex: $5^{-1} \text{ mod } 7 = 3$, $4^{-1} \text{ mod } 7 = 2$, $6^{-1} \text{ mod } 7 = 6$

Fermat's little theorem

$$a^{p-1} = 1 \text{ mod } p$$

for p prime, $1 \leq a < p$

Proof (part 1)

Let $S = \{1, 2, \dots, p-1\}$
 $aS = \{a1, a2, \dots, a(p-1)\}$

ex: $p=7, a=3$
 $\{1, 2, 3, 4, 5, 6\}$

$\downarrow \cdot a$
 $\{3, 6, 9, 12, 15, 18\}$

$\downarrow \text{mod } p$
 $\{3, 6, 2, 5, 1, 4\} \checkmark$

Prove $aS = S \text{ mod } p$
by contradiction, pick two elts in aS ,
suppose $ai = aj \text{ mod } p$

multiply by a multiplicative inverse a^{-1}
since $ai = aj \text{ mod } p$ and $a^{-1} = a^{-1} \text{ mod } p$

$$\Rightarrow aa^{-1}i = aa^{-1}j \text{ mod } p \text{ (modular arithmetic)}$$

$$\Rightarrow i = j \text{ mod } p$$

\Rightarrow contradiction

the only way to have two elements in aS s.t.

$$ai = aj \text{ mod } p$$

is to multiply i and j by a \square , where

$$i = j \text{ mod } p$$

BUT, there are no such two elements in S

\Rightarrow \square for all i in aS \square

$ai \neq aj \text{ mod } p$
and there $p-1$ such elts
and none is $0 \text{ mod } p$ (p is not in any operation)

$$\Rightarrow aS = S \text{ mod } p$$

\hookrightarrow is not a factor in prime factorization of any elts

Proof (part 2)

$$\prod_{x \in S} x = \prod_{y \in aS} y \pmod p$$

since S and aS are the same products of their elts are the same mod p

by modular arithmetic

$$(p-1)! = a^{p-1} (p-1)! \pmod p$$

$$(p-1)! = a^{p-1} \underbrace{(p-1)!}_{\text{no factor } p} \pmod p$$

no factor p

$\Rightarrow \neq 0 \pmod p$

\Rightarrow has a multiplicative inverse

multiply by inverse (modular arith.)

$$1 = a^{p-1} \pmod p$$

Fermat test

- given $p > 2$

- compute $2^{p-1} \pmod p$

$= 1 \rightarrow$ prime \times NO
 $\neq 1 \rightarrow$ composite \checkmark YES

Potential fix? \rightarrow NO
try different a 's

$$3^{p-1} \\ 5^{p-1}$$

Carmichael #'s (n)

$$a^{n-1} = 1 \pmod n$$

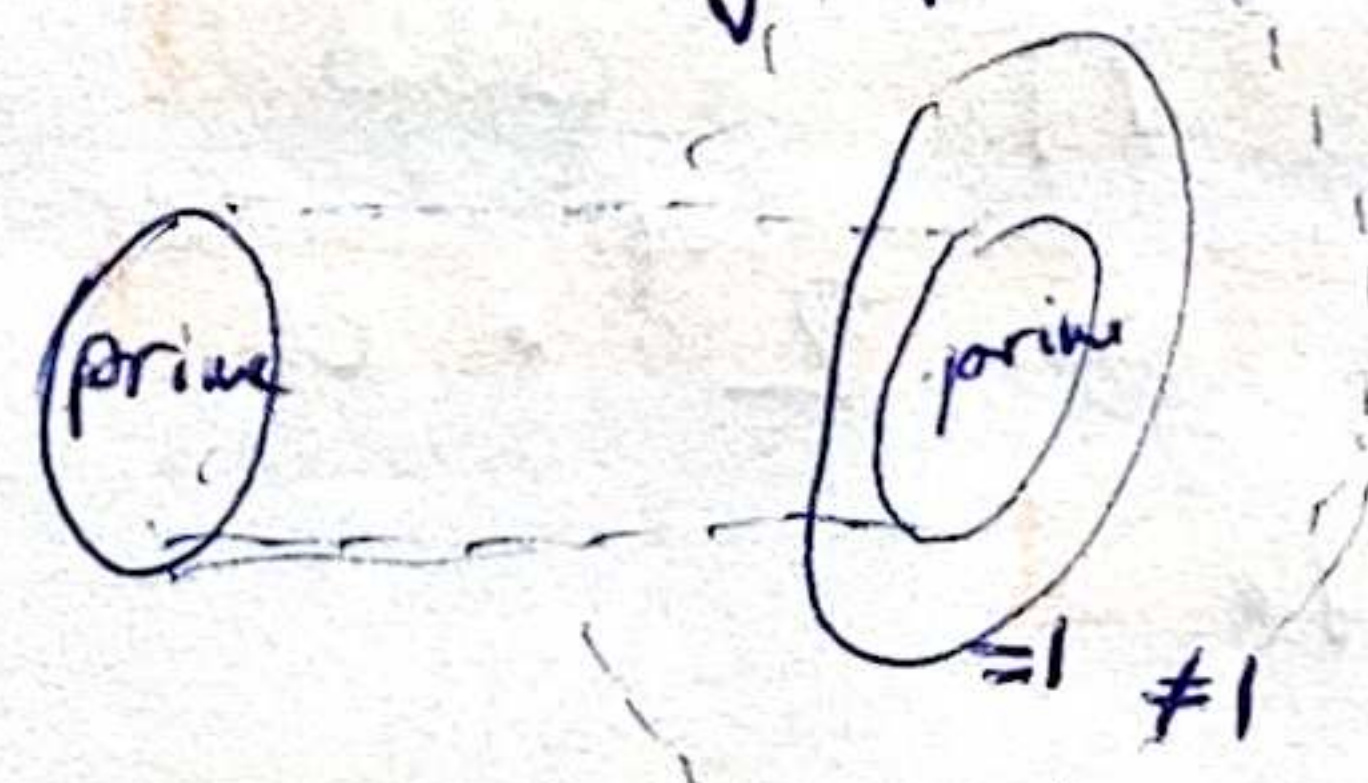
$\forall a$ where a, n do not share a factor

\rightarrow infinitely many Carmichael #'s

Fermat little theorem

$$p \text{ prime} \\ 1 \leq a < p \Rightarrow a^{p-1} = 1 \pmod p$$

\uparrow only forward direction



$$\text{e.g. } 2^{340} = 1 \pmod p$$

341 not prime

\rightarrow 2 - pseudoprime for Fermat's test

Rabin - Miller Primality test

mod prime (p)

① — no non-trivial root of 1

mod composite (n)

② — there are

e.g. $n=15$

$$4^2 \equiv 16 \equiv 1 \pmod{15}$$

① $x^2 \equiv 1 \pmod{p}$

by mod. arithmetic

$$(x+1)(x-1) \equiv 0 \pmod{p}$$

for $0 \pmod{p}$,

$$x+1 \equiv 0 \pmod{p}$$

or

$$x-1 \equiv 0 \pmod{p}$$

by mod. arithmetic.

$$\Rightarrow x \equiv 1 \pmod{p} \text{ or }$$

$$x \equiv -1 \pmod{p}$$

trivial roots

② $x^2 \equiv 1 \pmod{n}$

multiply with itself to get $1 \pmod{n}$

$$(x+1)(x-1) \equiv 0 \pmod{n}$$

factor of 3

factor of 5

for $n=15$

or vice versa

\Rightarrow non-trivial roots

use Fermat little theorem, and exploit the root property

Test n (odd)

$$n-1 = 2^t \cdot u \quad \leftarrow \text{odd part}$$

compute

rep. squaring ($O(\log n)$)

$$\begin{matrix} a^u \\ \downarrow \\ a^{2u} \\ \downarrow \\ a^{4u} \\ \vdots \end{matrix}$$

$$a^{2^{t-1}u} \equiv \begin{cases} \neq -1 \text{ or } 1 \pmod{n} \\ 1 \pmod{n} \\ -1 \pmod{n} \end{cases}$$

\Rightarrow composite, non trivial root of 1 found

keep going

$$1 \pmod{n}$$

$$-1 \pmod{n}$$

DONE, cannot continue taking roots

$$a^{2^t u} = a^{n-1}$$

$$\text{if } a^{n-1} \not\equiv 1 \pmod{n}$$

\Rightarrow composite by FLT

if $a^{n-1} \equiv 1 \pmod{n}$, look at previous term, square root

Alg.

choose a random $1 < a < n$

run Rabin-Miller

if n is composite

→ return with prob. $\geq 3/4$
(a is witness)

else

→ with $< 1/4$ prob, pass, repeat.

candidate
witness that n is composite (5)

(LT Number theory)

~~if pass 50 times~~

if pass 50 times

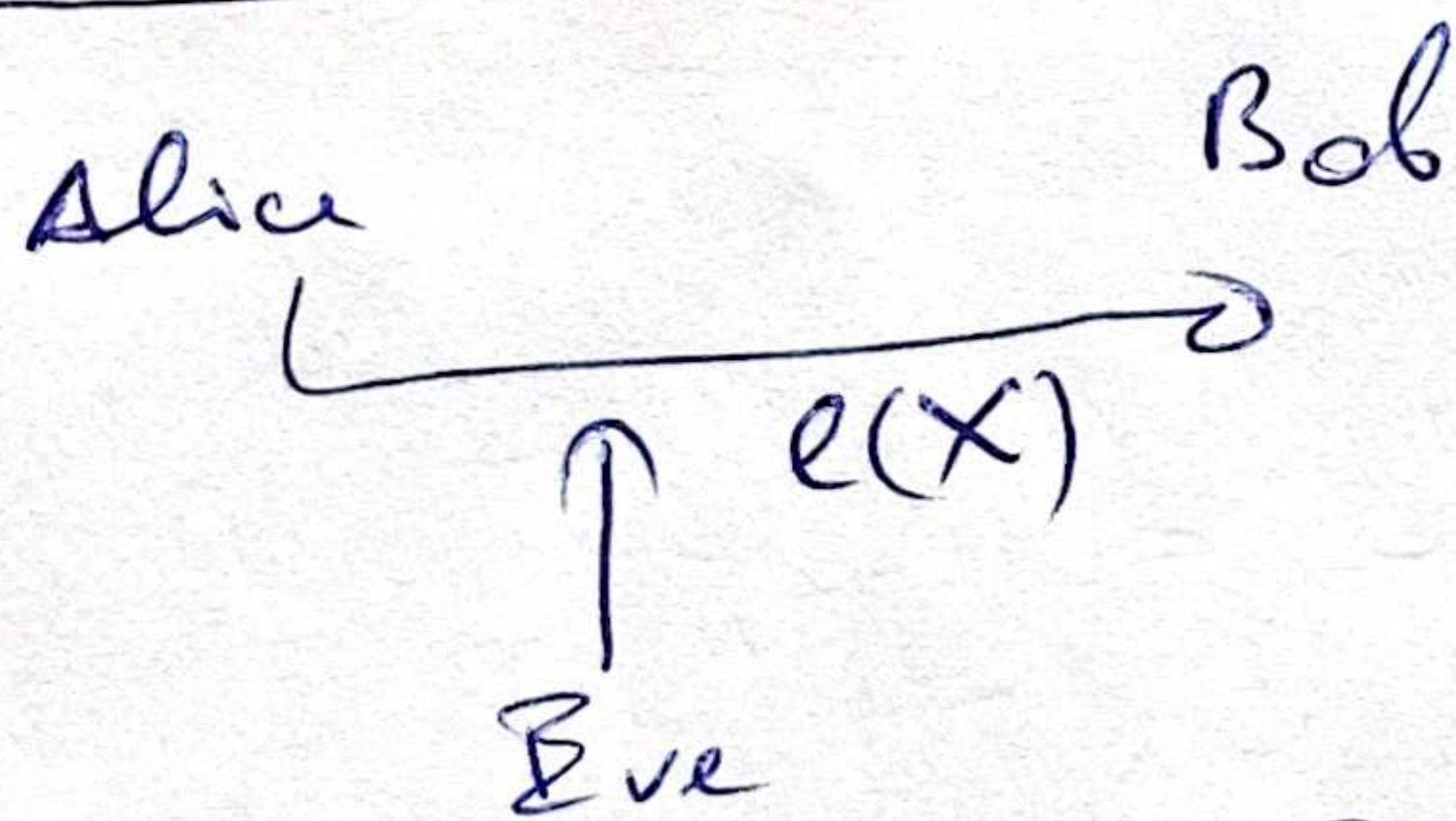
return prime with False positive rate $< 2^{-100}$

$O(\log n)$

no problem with Carmichael #s

there is a de-randomized alg. now, but randomized is efficient

Gen. Crypto Framework



Alice $x \rightarrow e(x)$

Bob $e(x) \rightarrow d(e(x)) = x$

Eve cannot recover x from $e(x)$

e.g. one-time pad

Alice, Bob share a random string r

Alice: $x \rightarrow e(x) = x \oplus r$

Bob: $e(x) \rightarrow d(e(x)) =$

$= e(x) \oplus r$

$= (x \oplus r) \oplus r = x$

0 1 1 0
0 1 0 1
0 0 1 1
0 1 0 1
0 1 1 0

in $e(x)$ each bit is equally likely to be 0 or 1 → no info

① Information theoretic

$\Pr(x \text{ was the message} | e(x) \text{ crossed wire})$

$= \Pr(x \text{ was the message})$

→ $e(x)$ does not change info

② RSA, computational

from $e(x)$, x cannot be computed in

$\leq 2^{50}$ ops

with prob. $1 - 2^{-100}$

problems with one-time pad

$$e(x) = x \oplus r$$

reuse

$$e(y) = y \oplus r$$

$$e(x) \oplus e(y) = x \oplus r \oplus y \oplus r = x \oplus y$$

reuse the random string leaks info

↳ can only use once