Recap of RSA protocol:

Bob:

1. Chooses 2 n-bit random primes p & q.
   HOW?
   - Detail in this lecture
2. Chooses e where $\gcd(e,(p-1)(q-1)) = 1$,
   by trying $e = 3, 5, 7, 11, 13, \ldots$
3. Let $N = pq$
4. Bob's public key is (N, e).
5. Their private key is $d \equiv e^{-1} \bmod (p-1)(q-1)$.

Alice: To send message m to Bob:

1. Looks up Bob's public key (N, e).
2. Computes $y \equiv m^e \bmod N$
3. Sends y to Bob

Bob: 1. Receives y & decrypts using
$m \equiv y^d \bmod N$.

Why does it work?

Fermat's Little Th'm.: For prime p, for all a where $\gcd(a,p)=1$, then

$$a^{p-1} \equiv 1 \bmod p$$

Euler's theorem: For all N, all a where $\gcd(a,N)=1$,

$$a^{\phi(N)} \equiv 1 \bmod N$$

where $\phi(N) = \#$ of $b \in \{1,2,\ldots,N-1\}$ where $\gcd(b,N)=1$.

Note, for prime p, $\phi(p)=p-1$ so this gives

For primes p & q, $\phi(pq)=(p-1)(q-1)$.

Consider d & e where $de \equiv 1 \bmod (p-1)(q-1)$

Thus, $de = 1 + k(p-1)(q-1)$ for integer k.

Therefore, $\left(m^e\right)^d \equiv m \times \left(m^{(p-1)(q-1)}\right)^k \equiv m \bmod pq$

for m where $\gcd(m,pq)=1$.

If $\gcd(m,pq)>1$ then can crack this key.

How to generate random primes?

Generate a random n-bit number r &
check if its prime. If it is prime then
it is a random prime so output it.
If it is not prime, then repeat

$$\Pr(r \text{ is prime}) \approx \frac{1}{n}$$

("Primes are dense")

$\Rightarrow O(n)$ rounds in expectation.

Let $T = 10n \ln n$.

$$\Pr(\#\text{rounds} > T) = \Pr(\text{all } T \text{ rounds fail})$$
$$= \left(1 - \frac{1}{n}\right)^{10n\ln n} \leq \left(e^{-\frac{1}{n}}\right)^{10n\ln n} = \frac{1}{n^{10}}$$

So $O(n \log n)$ rounds with prob. $\geq 1 - \frac{1}{n^{10}}$

How to check if a number x is prime?

If x is prime, then by Fermat's Little Theorem,

for all $a \in \{1, \ldots, x-1\}$,

$$a^{x-1} \equiv 1 \bmod x$$

What about composite x?

Say $a \in \{1, \ldots, x-1\}$ is a Fermat witness if

$$a^{x-1} \not\equiv 1 \bmod x$$

Every a where $\gcd(a,x) > 1$ is a Fermat witness.

Why? Let $d = \gcd(a,x) > 1$.

$a = id$ & $x = jd$ for integers i, j.

Then, $a^{x-1} \bmod x = r$ where

$$a^{x-1} = kx + r$$

$$r = a^{x-1} - kx = d(\text{some integer})$$

Can factor d from a^{x-1} & x

So r is a multiple of d

& $r \neq 1$ since $d \neq 1$.

Hence, every composite x has ≥ 2 Fermat witnesses.

But these ~~a~~ a where $\gcd(a,x) > 1$ already yield a factor of x.

Thus, say a is a <u>trivial</u> Fermat witness if $\gcd(a,x) > 1$ & $a^{x-1} \not\equiv 1 \bmod x$.

What about <u>non-trivial</u> Fermat witnesses?

This is a where $\gcd(a,x) = 1$ & $a^{x-1} \not\equiv 1 \bmod x$.

Some composites have no nontrivial Fermat witnesses

Called Carmichael numbers.

~~Relatively~~ rare, smallest ones are 561, 1105, ...

Let's ignore Carmichael numbers for now.

Hence, we can assume every composite x has ≥ 1 nontrivial Fermat witness.

Lemma: If x has ≥ 1 nontrivial Fermat witness then $\geq \frac{1}{2}$ of the $b \in \{1, 2, \ldots, x-1\}$ are Fermat witnesses.

Proof: Fix a which is a nontrivial Fermat witness, so $\gcd(a,x)=1$ & $a^{x-1} \not\equiv 1 \bmod x$.

Let $B = \{ b \in \{1, 2, \ldots, x-1\} : b^{x-1} \equiv 1 \bmod x \}$

↖ bad set

Let $G = \{ g \in \{1, \ldots, x-1\} : g^{x-1} \not\equiv 1 \bmod x \}$

↖ good set.

Want to show $|G| \geq |B|$.

Define a map $f: B \to G$ so that it's injective,

this means each $b \in B$ maps to a unique $g \in G$,

so if $b, b' \in B$ with $b \neq b'$ then $f(b) \neq f(b')$.

Let f be $f(b) = ab \bmod x$

for $b \in B$, note $f(b) \in G$.

Why? $f(b) = ab \bmod x$

thus, $f(b)^{x-1} \equiv a^{x-1} b^{x-1} \equiv a^{x-1} \not\equiv 1 \bmod x$

Since we assumed a is a Fermat witness

Now suppose for $b, b' \in B$, where $b \neq b'$,

$f(b) = f(b') \Rightarrow ab \equiv ab' \bmod x$

Since $a^{-1} \bmod x$ exists b/c $\gcd(a,x) = 1$

then $b \equiv b' \bmod x$

∎

Hence, by the lemma, if x is composite & not Carmichael then $\geq \frac{1}{2}$ of the $b \in \{1, 2, \ldots, x-1\}$ are Fermat witnesses.

Primality testing alg. for n-bit x:

1. Choose $a_1, a_2, \ldots, a_\ell$ randomly from $\{1, 2, \ldots, x-1\}$.
2. For $i = 1 \to \ell$,
   compute $a_i^{x-1} \bmod x$.
3. If for all i, $(a_i)^{x-1} \equiv 1 \bmod x$
   then output "x is prime"

   If $\exists i$ where $(a_i)^{x-1} \not\equiv 1 \bmod x$
   then output "x is composite"

For prime x, alg. always outputs prime.

For composite x which is not Carmichael,

Prob. alg. outputs "x is prime" is $\leq 2^{-\ell}$

So <u>false positive</u> probability is $\leq 2^{-\ell}$

How to deal with Carmichael numbers?

For x, N, if $x^2 \equiv 1 \bmod N$ then

x is a square root of $1 \bmod N$.

$x \equiv 1 \bmod N$ & $x \equiv -1 \bmod N$

are always square roots of $1 \bmod N$,

any other one is a <u>nontrivial</u> square root of $1 \bmod N$.

<u>Claim:</u> For prime p, no nontrivial square roots of $1 \bmod p$.

<u>Proof:</u> Consider x where $x^2 \equiv 1 \bmod p$.

thus, $x^2 = 1 + kp$ for integer k.

$$x^2 - 1 = kp$$

$$(x-1)(x+1) = kp$$

Since p divides RHS it also divides LHS so either p divides $x-1$ or $x+1$.

hence, $x - 1 \equiv 0 \bmod p$ or $x + 1 \equiv 0 \bmod p$

$x \equiv 1 \bmod p$ $\quad$ $x \equiv -1 \bmod p$.

So $x \equiv 1$ or $x \equiv -1 \bmod p$. ∎

To prove N is composite it suffices to find a nontrivial square root of $1 \bmod N$.

For composite $N \Rightarrow N$ is odd

so $N-1$ is even

let ~~N~~ $N-1 = 2^t u$ where u is odd

↖ take out as many factors of 2 as possible.

Fermat's test: check if $a^{N-1} \stackrel{?}{\equiv} 1 \bmod N$

for random a.

Let's do by repeated squaring.

Compute: $a^u \bmod N$

then $a^{2u} \bmod N$

$a^{4u} \bmod N$

$\vdots$

$a^{2^t u} \bmod N$

$\| \; a^{N-1}$

if $a^{N-1} \not\equiv 1 \bmod N$ then we know N is composite by Fermat's little theorem.

Suppose $a^{N-1} \equiv 1 \bmod N$

go back to the 1st point where $a^{2^i u} \equiv 1 \bmod N$

then $a^{2^i u}$ is a square root of $1 \bmod N$

is it non-trivial?

if it's $\not\equiv -1$ then it is.

For every composite N,

$\geq \frac{3}{4}$ of $a \in \{1, \ldots, N-1\}$

Provide a nontrivial sq. root of $1 \bmod N$ in this manner.

Example: $N = 561$.

$N - 1 = 560 = 35 \times 2^4$

try $a = 8$. (note $\gcd(8, 561) = 1$)

$8^{35} \equiv 461 \mod 561$.

$8^{2 \times 35} \equiv 463 \mod 561$

$8^{2^2 \times 35} \equiv 67 \mod 561$

$8^{2^3 \times 35} \equiv 1 \mod 561$

$8^{2^4 \times 35} \equiv 1 \mod 561$

67 is a nontrivial square root of 1 mod 561.