Recap from last class:

Fermat's little theorem:

For prime p, for a where $\gcd(a,p)=1$,

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

Generalization: **Euler's theorem:**

For any N, for 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 $\gcd(b,N)=1$

For prime p, $\phi(p) = p-1$

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

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

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

then for a where $\gcd(a,pq)=1$,

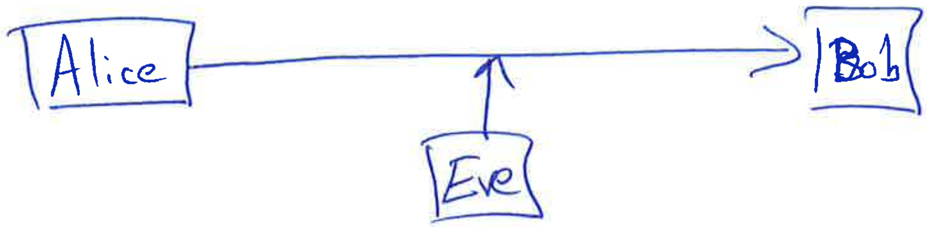
$$(a^d)^e \equiv a^{de} \equiv a^{1+k(p-1)(q-1)} \equiv a \times \underbrace{\left(a^{(p-1)(q-1)}\right)^k}_{\equiv 1 \text{ by Euler's thm.}} \equiv a \bmod pq.$$

In fact, $\boxed{\text{for all } a,\ a^{de} \equiv a \bmod pq}$ ← (See Part I notes for the short proof of this fact)

this is the key to RSA.

RSA = [Rivest, Shamir, Adelman '77]
independently discovered by Clifford Cocks in '74.

Public-key cryptosystem:



Alice has a message m that she wants to send to Bob

Eve can see whatever message is transmitted

Public-key scheme:

Bob publishes a public key (N,e)
Alice uses Bob's public key to encrypt m
Bob uses his private secret key to decrypt.

RSA Protocol:

I. Bob: (1) Bob picks 2 n-bit random primes p & q.
HOW? We'll see in a bit.
n is big, like $n = 1024$ or 2048.

(2) Bob chooses e relatively prime to $(p-1)(q-1)$
by trying $e = 3, 5, 7, 11, \ldots$
and testing $\gcd(e, (p-1)(q-1))$.

Let $N=pq$.

(3) Bob publishes his public key (N,e).

(4) Bob computes his private key:

$$d \equiv e^{-1} \bmod (p-1)(q-1)$$

Using Extended-Euclid algorithm.

(B) Alice: To send message m,

(1) Looks up Bob's public key (N,e)

(2) She computes $y \equiv m^e \bmod N$.

(3) She sends y.

(C) Bob:

(1) He receives y.

(2) He decrypts using:

$$m \equiv y^d \bmod N$$

Use fast modular exponentiation algorithm since d is probably big.

Key assumption: Given N, e, and y it is computationally difficult to determine m.

Natural approach is to factor N to get p & q then one can get $(p-1)(q-1)$ and hence $d \equiv e^{-1} \bmod (p-1)(q-1)$

Potential issues:

- if $e=3$ (or is too small) one needs to make sure that $m^e > N$ otherwise mod N isn't doing anything so to decrypt one can just compute $y^{1/3}$

  To avoid this often "pad" m with random r.

- if send same m to e or more people ~~then~~ (all using the same e) then it can be decrypted (see HW problem).

Generating random Primes:

Primes are dense:

generate a random n-bit number x

Check if x is prime (How?)

if x is prime, output x

else repeat

$\text{Prob}(x \text{ is prime}) \approx \frac{1}{n}$ (Prime number theorem)

Thus, n rounds in expectation.

How to test if x is prime?

If x is prime then for all $a \in \{1, 2, \ldots, x-1\}$,

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

(by Fermat's little theorem)

What about composite x?

Say $a \in \{1, 2, \ldots, x-1\}$ is a Fermat witness if:

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

(such an a proves that x is composite)

For composite x, for a where $\gcd(a,x) = d > 1$ then: $a^{x-1} \bmod x = a^{x-1} - kx$ for some integer k

$$= d\left(\frac{a^{x-1}}{d} - k\frac{x}{d}\right)$$

So $a^{x-1} \bmod x$ is a multiple of d.

Thus, such an a is a Fermat witness.

So composite x have ≥ 2 Fermat witnesses but are there Fermat witnesses which are not divisors of x?

<u>Lemma</u>: if x has ≥ 1 Fermat witness a where $\gcd(a,x) = 1$ then at least half the $b \in \{1, 2, \ldots, x-1\}$ are Fermat witnesses.

<u>Carmichael number</u>: composite x where every a where $\gcd(a,x) = 1$ has $a^{x-1} \equiv 1 \bmod x$.
(So no non-trivial Fermat witnesses and this lemma doesn't apply.)

Carmichael numbers are rare.

Smallest ones are 561, 1105, 1729, ...

Ignoring Carmichael numbers we have a primality testing algorithm:

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) a) if for all i we have $a_i^{x-1} \equiv 1 \bmod x$ then output "x is prime"
else output "x is composite"

For prime x, we always output "x is prime"

For composite x & not carmichael,

$$\Pr(\text{output } x \text{ is prime}) \leq \frac{1}{2^\ell}$$

"false positive"

How to deal with Carmichael numbers

For x, N, if $x^2 \equiv 1 \bmod N$ then x is a square root of $1 \bmod N$.

Note $x = 1$ & $x \equiv -1 \equiv N-1 \bmod N-1$ are always square roots of $1 \bmod N$.

if x is not ± 1 then it is a <u>nontrivial</u> square root of $1 \bmod N$.

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

So to show that x is composite we'll find a nontrivial squareroot of $1 \bmod x$.

To see the claim:

note $x^2 \equiv 1 \mod p$

hence $x^2 = 1 + kp$ for some integer k.

thus $x^2 - 1 = (x-1)(x+1) = kp$

Since p Divides kp it must also divide $(x-1)$ or $(x+1)$.

hence $x - 1 \equiv 0 \mod p$ or $x+1 \equiv 0 \mod p$

$x \equiv 1 \mod p$ or $x \equiv -1 \mod p$.

For odd x, $x-1$ is even so we can factor the largest power of 2 and get:

$x - 1 = 2^t u$ where u is odd.

Recall Fermat's test: check if $a^{x-1} \stackrel{?}{\equiv} 1 \mod x$

we'll compute $a^{x-1} \bmod x$ by
first computing $a^{u} \bmod x$
then doing repeated squaring

So we'll get the sequence:

$$a^{u} \bmod x$$
$$a^{2u} \bmod x$$
$$a^{2^2 u} \bmod x$$
$$a^{2^3 u} \bmod x$$
$$\vdots$$
$$a^{2^t u} \bmod x$$

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

if $a^{x-1} \equiv 1 \bmod x$ then look at the 1st i where $a^{2^i u} \equiv 1 \bmod x$

check if $a^{2^{i-1} u} \equiv -1 \bmod x$

if not then we have a nontrivial square root of $1 \bmod x$

So we know x is composite.

<u>Claim:</u> For at least $\frac{3}{4}$ of the $a \in \{1, 2, \ldots, x-1\}$, they provide a nontrivial square root of 1 mod x for this algorithm.