3-pass protocol, physical version

- The NYTimes wants to have a way of securely receiving anonymous documents.
- It places a lockable box outside its offices and the anonymous source brings the documents, puts them in the box and puts a lock on the box.
- The editors then go outside and put their own lock on the box.
- Later, the source comes back and removes their lock.
- The editors then take their lock off the box and remove the documents.

3-pass protocol, digital version

- Bob, who wants to receive something securely (and potentially anonymously), chooses a large prime p and publishes it.
- Alice encodes her message as a number $m < p$ and also picks an exponent a, $0 < a < p$ with $\gcd(a, p-1) = 1$. She posts m^a mod p.
- Bob picks his own exponent b, $0 < b < p$ with $\gcd(b, p-1) = 1$ and publishes m^{ab}.
- Alice knows the multiplicative inverse of a mod $(p-1)$ and so she is able to post m^b mod p.
- Bob then uses the multiplicative inverse of b mod $(p-1)$ to determine m.

Primality testing, Fermat

- The simplest primality test uses Fermat's little theorem.
- Fermat in the contrapositive, says that if $0 < a < n$ and $a^{n-1} \not\equiv 1 \bmod n$ then n is not prime.
- Unfortunately, there are composite numbers n such that $a^n \equiv a \bmod n$ for all a. In fact, there are infinitely many such numbers.

Primality testing, Miller-Rabin

Lemma

If $x^2 \equiv y^2$ mod n and $x \not\equiv \pm y$ mod n then n is composite. Moreover, $\gcd(n, x+y)$ and $\gcd(n, x-y)$ are non-trivial factors of n.

- Here is the Miller-Rabin algorithm for determining primality probabilistically:
- Suppose n is odd and greater than 9. Write $n - 1 = 2^k m$ where m is odd.
- Now pick $a < n$ randomly and compute a series b_i for $i = 0, \ldots, k-1$ as follows:

$$b_0 \equiv a^m \bmod n, b_1 \equiv b_0^2 \bmod n, \ldots, b_i \equiv b_{i-1}^2 \bmod n, \ldots$$

- We will guess that n is prime if $b_0 \equiv \pm 1 \bmod n$ or if $b_i \equiv -1 \bmod n$ for any i. Otherwise we will say that n is composite.

Primality testing, Miller-Rabin, cont'd

- Claim: If we say n is composite we will be correct.
- There is at most a 25% chance that if we say n is prime then we will be wrong.
- If we repeat this test many times for randomly chosen a and we always get the answer "prime" then with high probability n is prime.

Primality testing, Agarwal-Kayal-Saxena

- There is a primality test which is completely deterministic and polynomial in the number of digits of the given number.
- The problem is that its known run-time is order n^6 although 6 is not known to be best possible.
- In practice, if one needs to determine primality for a given number, one uses the probabilistic algorithms to see if you can prove it is not prime and then tries a series of special purpose primality tests which are not efficient but are good enough for "small" numbers, say ones with fewer than 1000 digits.