

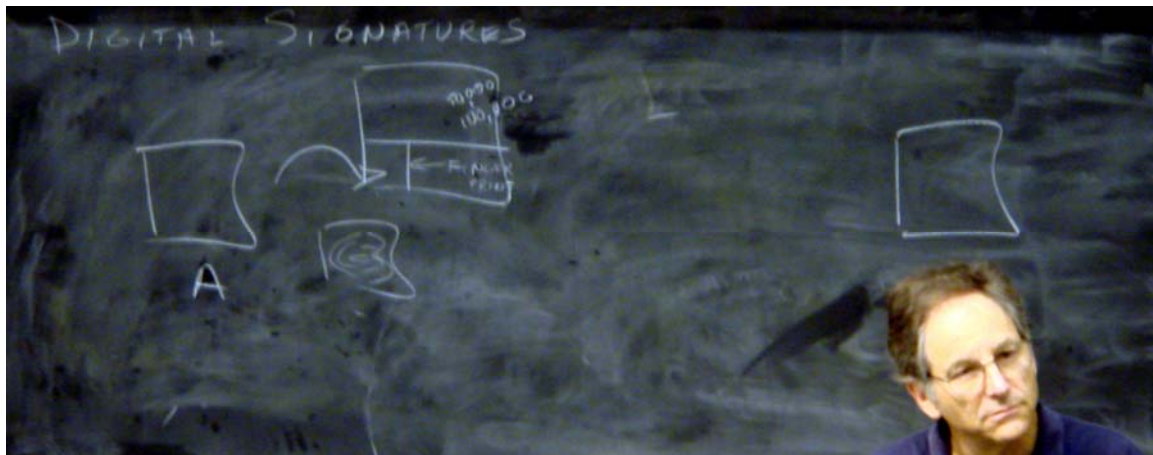
Quiz 2 will be on Monday, April 9th, in class. It will cover homeworks 6, 7, and 8.

We have seen how RSA solves the key distribution problem. Note that in RSA, the keys d and e are symmetrical (in particular, $P_A(S_A(m)) = m$). So either of them could be used as part of the public key, and the other as the private key. This leads to RSA being a doubly public key cryptosystem (if it cannot be broken in polynomial time).

This property allows RSA to be used in another context, one that has not traditionally been associated with cryptography: digital signatures.

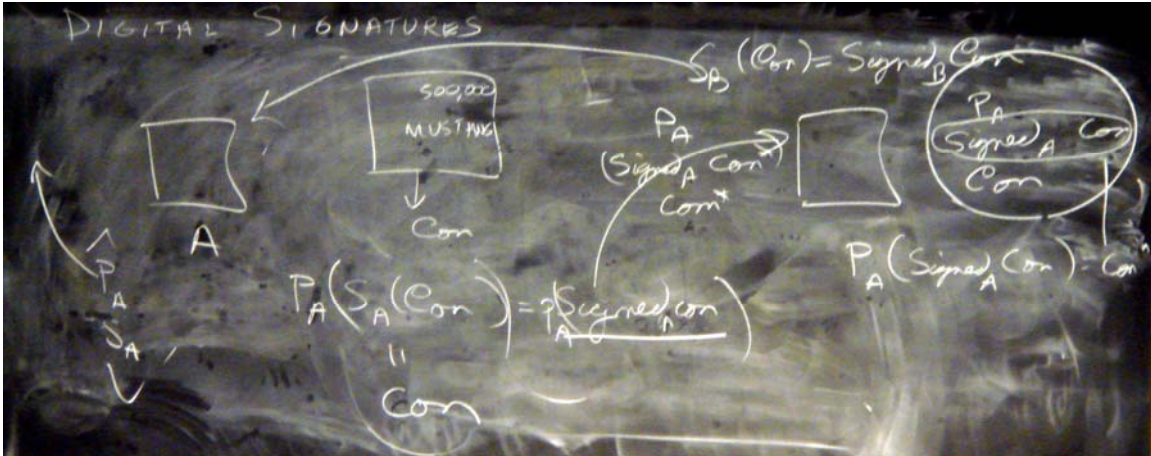
Digital signatures:

A digital signature is the analog of a signature at the bottom of a contract. When you sign a contract, you place your unique seal on a particular agreement. To be able to do so on the internet, it is not sufficient to just use some digital piece of information because digital information can be easily copied exactly, so one could sign other documents with your signature, and change the contract you agreed to.



RSA:

Alice and Bob come to an agreement and write up a contract Con . Alice signs this contract with her private key by computing $S_A(Con) = Signed_A Con$, and sends that to Bob. Bob signs the contract with his private key by computing $S_B(Con) = Signed_B Con$ and sends that to Alice. Now each of them can use the other's public key to make sure the data they signed is in fact the original contract ($P_A(S_A(Con))=Con$), but without the other person's private key they cannot modify and then sign a new contract. The only one who can sign a contract with a private key is the owner of that private key.



Other problems that RSA, or RSA spin-offs can help solve:

Poker on the Internet:

You can make sure the dealer is not cheating in dealing cards.

Zero-knowledge proof:

I can prove an important theorem and prove to you that I have the proof, without ever telling you a single bit of information about the proof, except that it exists. This allows an incredibly exquisite control over information.

Voting:

We can make sure that all votes are anonymous and that the count is correct.

In our discussion of RSA, we spoke about using a polynomial time algorithm to check for a number's primality. However, this algorithm has been around for only five or so years. Here's the history of the primality problem:

Sieve of Eratosthenes 276 BC - 194 BC)

http://en.wikipedia.org/wiki/Sieve_of_Eratosthenes

Step 1: Write down all the numbers starting with 2.

Step 2: Circle the first number not yet circled or crossed out and cross out every number after it that is divisible by it.

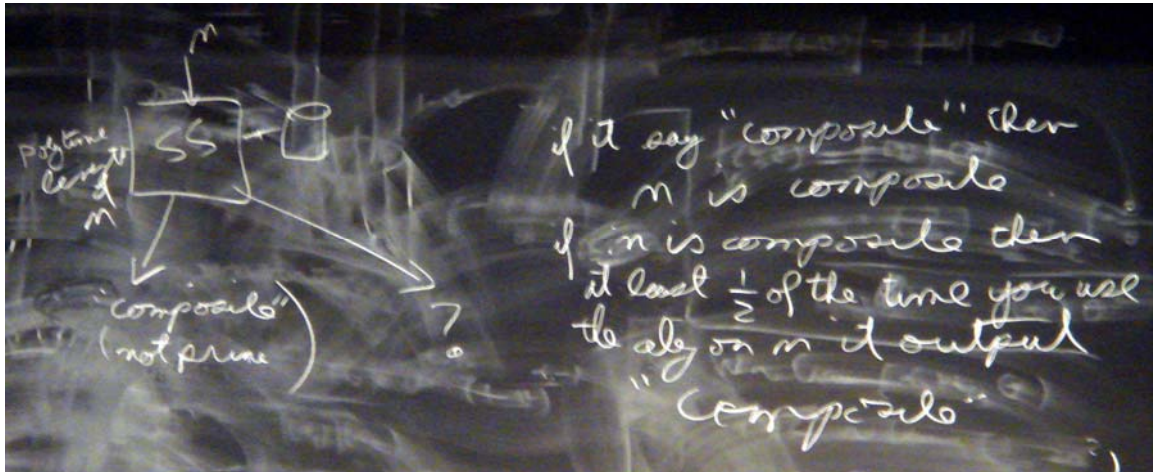
Step 3: Goto step 2.

The prime numbers end up circled. This algorithm takes $O(2^n)$ time.

Then Fibonacci (1170 or 1180 – 1250 AD) came up with an algorithm that runs in $O(2^{n/2})$ time.

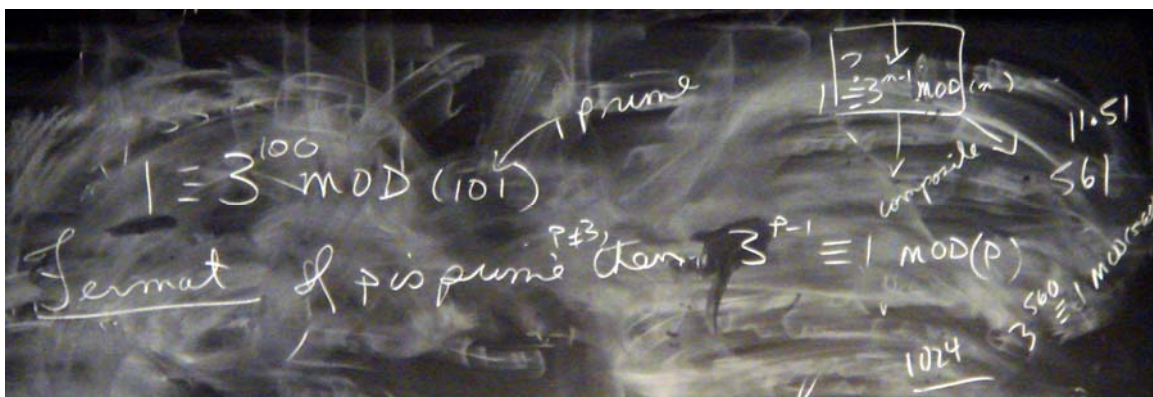
Fibonacci's algorithm was the best known until 1970s, when Solovei and Strassen came up with a randomized algorithm that, in polynomial time, either said the input was composite or that it did not know. It guaranteed that if it said the input was composite, then the input was in fact composite. If the input was in fact composite, it said that it did

not know the answer no more than $\frac{1}{2}$ the time. Thus you could execute the algorithm a large number of times, say 100 times. If it ever said that the number was composite, then you knew for sure that it was composite. However, if it always said that it did not know, then with probability $\frac{1}{2}^{100}$ the number was composite and with probability $1 - \frac{1}{2}^{100}$ it was prime!



Then there was an algorithm that with probability no more than $\frac{1}{2}$ said it didn't know, and otherwise answered whether the number of prime or composite, so with arbitrarily high probability, you could know for sure that the number was prime.

Also, Fermat said that for all primes p other than 3, the following holds $1 \equiv 3^{p-1} \pmod{p}$. This observation could be adopted into an algorithm by picking random numbers and checking if the above holds. If it doesn't, the number is composite. If it does, the probability that it's prime is very high (composite numbers with the above property are extremely rare).



Next time, recursive function theory.