CS 2800: Discrete Math Sept. 23, 2011

Lecture

Lecturer: John Hopcroft *Scribe: June Andrews*

Review

See previous lecture notes.

Public Key Encryption

We are going to build up to RSA encryption. To do that, we need explain the general framework for encryption decrpytion and build up more understanding about primes.

Let us say we have an algorithm that works for everyone and can be indiviualized by a pair of random numbers. The algorithms works by, given E a process for encoding a message, m, and D a process for decoding m:

$$D(E(m)) = m$$
$$E(D(m)) = m.$$

We have to personalize the algorithm (ie, not everyone can have exactly the same E and D, otherwise everyone could read everyone else's messages and that is not very good encryption). We can personalize the algorithm by have everyone generate 2 large primes, p and q, say on the order of 10^{50}. Now, we make $p * q$ public, but keep p and q private. You would think if you knew pq, you could easily find p and q, however, the problem of factoring a large number into its two large prime factors is in fact very hard. So hard, it is considered impossible.

Now, with these primes we can Bob can produce his own version of the encryption/decryption algorithms, E_b and D_b. Bob makes E_b public and keeps D_b private. The process of Alice sending Bob a message is as follows:

1. Alice creates m and looks up Bob's public E_b
2. Alice sends Bob, $E_b(m)$
3. Bob receives $E_b(m)$ and decrypts it with $D_b(E_b(m)) = m$.

That was straight forward. However, Bob doesn't really know whether or not Alice was the one sending the message. Eve could have sent $E_b(m')$, where m' said she was Alice. But because Alice is the only one that knows her personalized decryption algorithm D_a, she can sign the message, so that Bob knows Alice sent the message. Alice can send $E_b(D_a(m))$. And Bob can read Alice's message by computing $E_a(D_b(E_b(D_a(m)))) = E_a(D_a(m)) = m$. Of course, when Bob first reads Alice's message it is just a bunch of random 1's and 0's. Bob needs to know to look up Alice's public key in order to apply E_a to the message. This can be achieved by Alice sending the message "*Hi Bob, It's Alice, find my public key* $+m$." Now Eve can not fake being Alice - only Alice could have sent a message, that when E_a was applied to it, the message produce an understandable phrase. This is because D_a is public or private?

Of course, encryption is a one up game. Hackers find a way to read encrypted messages, coders find more secure encryptions, and vice versa. Now that we have described the basics of RSA, the next step up for the hackers is to guess the message, compute $E_b(m)$ and see if they guessed the message correctly. If you know the format of the message, guessing a message is easier than you think.

1 Euler's ϕ function

Definition 1. *Let $\phi(n)$ be the number of positive integers less than or equal to n that are relatively prime to n.*

In particular this means, $\phi(1) = 1$, and $\phi(8) = 4$, since $1, 3, 5, 7$ are the only positive integers less than or equal to 8 that are relatively prime to 8.

Corollary 2. *If p is prime, then $\phi(p) = p - 1$.*

Proof. If p is prime, then p is relatively prime to every number less than it, which is $p - 1$ numbers. □

Let us check a way to calculate $\phi(n)$. If p and q are two different primes, then $\phi(pq) = (p - 1)(q - 1)$. We first consider all the numbers that are not relatively prime:

$$\begin{gathered} q, 2q, 3q, \ldots, (p-1)q \\ p, 2p, 3p, \ldots, (q-1)p. \end{gathered}$$

With a quick check you can convince yourself that all the numbers we have listed are unique, less than pq, but most importantly, that no number less than pq that is not relatively prime to pq has not been listed. Hence:

$$\begin{aligned} \phi(pq) &= pq - 1 - |\{q, 2q, \ldots, (p-1)q\}| - |\{p, 2p, \ldots, (q-1)p\}| \\ &= pq - 1 - (p-1) - (q-1) \\ &= (p-1)(q-1) \end{aligned}$$

Theorem 3. *Euler's Theorem: If $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$*

A useful corollary follows.

Corollary 4. *If p is prime and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \mod p$.*

For a quick check, ask yourself what the 1-line proof of this corollary is.

We can use this corollary to test whether or not n is prime. Let us choose p at random. Now, choosing a relatively prime a, we compute $a^{p-1} \mod p$. If p is prime, the result will be 1. Of course there are a few cases where p will not be prime, but the probability a non-prime number p survives this test is $\frac{1}{2}$. So, if we pick a_2 and rerun the test, the probability a non-prime number p survives both tests is $\frac{1}{2^2}$. In fact, if we run the test 100 times, by picking 100 a's and p survives every test, then p is prime with probability $\frac{1}{2^100}$. Using this method to test whether or not p is prime is very quick. If we guess p to be prime, but find it is not prime, we pick another p' and try p'. By the density of primes the expected number of p's we have to test, before finding a p that is prime is 100. That's not too bad. This is known as the Miller-Rabin Primality Test.

Note: there are some composite numbers that act like primes, ie will surivive all of our tests. These numbers are know as Carmichael numbers.

We now cover the proof of Euler's Theorem:

Proof. Let us define X as the set of all numbers that are relatively prime to n. Recall that this is also the set of all numbers that have a multiplicative inverse mod n. Let us also define $aX = \{ax \bmod n \mid x \in X\}$. We now show that $X = aX$ by showing that $X \subseteq aX$ and $aX \subseteq X$:

To show that $X \subseteq aX$, we want to prove that $x \in X \implies x \in aX$. Consider $a^{-1}x \bmod n \in X$ (we know this because $a^{-1}x$ has a multiplicative inverse mod n, specifically $x^{-1}a$. This means that $a(a^{-1}x) \equiv x \pmod{n} \in aX$.

To show that $aX \subseteq X$, observe that $|aX| \leq |X|$, since the elements in aX are simply the results of an onto mapping from $X \to aX$. Because these sets are finite and we know both that $X \subseteq aX$ and $|aX| \leq |X|$, we can conclude $aX \subseteq X$ (otherwise we'd have a contradiction).

Now that we've shown that $aX = X$, we can see that:

$$\prod_{x \in X} x \equiv \prod_{y \in aX} y \equiv \prod_{x \in X} ax \ (mod\ n)$$

As we stated earlier, every $x \in X$ has a multiplicative inverse, so if we multiply each side of this equality by each x^{-1} corresponding to every $x \in X$, we're left with:

$$1 \equiv \prod_{x \in X} a \ (mod\ n)$$

Because $|X| = \phi(n)$, we've shown that $a^{\phi(n)} \equiv 1 \text{ (mod } n)$

□

Theorem 5. *Fermat's Little Theorem: If p is prime and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \mod p$*

Recall, we can compute a^{p-1} very quickly with repeated squaring.
Midterm this Friday!