JUNE 20TH CRYPTOGRAPHY PROBLEM SET

If someone steals your password, you can change it. But if someone steals your thumbprint, you cant get a new thumb. The failure modes are very different. – Bruce Schneier

Today we will learn about RSA (Rivest-Shamir-Adleman) cryptography. But first we need one more version of Fermat's little theorem. Remember last week we saw that if p is prime and $1 \leq x \leq p-1$ then

$$x^{p-1} \equiv_p 1.$$

We want to find a similar formula when p is not prime.

1. Find the orders of all the elements $1 \leq x \leq n-1$ that are relatively prime to n for the following values of n (remember, $\text{ord}(x \bmod n)$ is the smallest exponent e so that $x^e \equiv_n 1$). Break up the work.

(a) $n = 9$.
(b) $n = 10$.
(c) $n = 12$.
(d) $n = 14$.
(e) $n = 15$.
(f) $n = 22$.

2. Compare the orders of elements you found to $\phi(n)$. Make a prediction relating those two.

3. Assuming your prediction is correct, show that $x^{\phi(n)} \equiv_n 1$ for x relatively prime to n. Make sure everyone in your group understands why this generalizes Fermat's little theorem.

I will prove the above result before we continue onto the next page. See if you can figure out the proof yourself first though.

RSA works like this.

Alice chooses two big primes p, q and computes $m = p \cdot q$ and $\phi(m) = (p-1)(q-1)$. Note there are $\phi(m) = (p-1)(q-1)$ elements relatively prime to m between 1 and m (but only Alice knows that, and it is hard for others to know without factoring m). She also chooses a number e such that

$$\gcd(e, \phi(m)) = 1.$$

Alice computes the multiplicative inverse $d \equiv e^{-1} \bmod \phi(m)$. Notice that $de = 1 + k\phi(m)$. (Make sure everyone in your group see this). Alice can do all this because she knows what $\phi(m)$ is.

Alice now publishes the numbers m and e. Anyone now can send a secure message to Alice. Say x is Bob's message ($x < m$). Bob compute $y = x^e \bmod m$. Alice can decrypt Bob's message by noticing that

$$y^d \bmod m = (x^e)^d \bmod m = x^{de} \bmod m = x^{1+k\phi(m)} \bmod m = x \cdot (x^{\phi(m)})^k \bmod m = x$$

Let's try it in practice.

1. Say Alice chooses the two primes $11, 17$. Then $m = 187$ and $\phi(m) = 160$. Alice also chooses the number $e = 99$. If Bob chooses to send the message made up of the number $x = 7$ to Alice, what should he send? (You may want a calculator or a phone to help do this one).

2. Now take the role of Alice, compute the number d (the multiplicative inverse of e modulo $\phi(m)$). Pretending you only know the value $y = x^e \bmod m$, compte $y^d \bmod m$ and see if you really got the x you started with.

3. You are now Eve. You notice that Alice published $m = 77$ and $e = 23$. Bob then sent the message consisting of two numbers $y_1 = 54, y_2 = 69$. Figure out what message Bob sent.

Each team should choose two two digit primes pq and make their own public keys (m, e). Publish these keys on the whiteboard and see if you can send other teams a message.

4. Points to speedy decryption.

5. Crack some of the other team's messages (and public keys). Points!