JUNE 22ND CRYPTOGRAPHY PROBLEM SET

The purpose of computing is insight, not numbers! – R. W. Hamming

We will discuss a variant of RSA which can be used for a different purpose. Authentication. In this case we are not trying to encrypt information. We are trying to demonstrate that the real person created it. We begin by reminding ourselves how RSA works.

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 (she published these a while ago).

Alice writes a message. Probably not encrypted. She signs it by saying that:

I Alice wrote this message. The number y encrypts to x. (Here x is a number which depends on the text of the message[1]).

For example, you could take the text, turn it into a number k in some way (maybe break it up into blocks, then multiply/add those blocks together in some pattern), and compute $k^f \pmod m$ where f is some other number that is publicly known. There are lots of other ways to generate x as well, x is called the *hash of the message*.

The point is, it is very hard for someone else to figure out what y is, it is as hard as decrypting x (because it is decrypting x).

1. However, it is easy for Alice to figure out y. Figure out how Alice does this as a group. Write down the procedure.

2. How can you (Bob) verify that Alice really was the author of the message?

[1]Let's talk about Hash functions.

3. Use the number $m = 143$, and specified $e = 7$. The following messages were digitally signed but only some are authentic. Figure out which are authentic.

- Hash = 5, Signature = 125
- Hash = 98, Signature = 100
- Hash = 50, Signature = 9
- Hash = 50, Signature = 72

4. Find a fake signature to sign the Hash = 10 for the $m = 143$ and $e = 7$ above.

5. Find the correct signature for the incorrectly signed Hash's from 3.

We will play a game where you get to race to see who can authenticate the signatures fastest. We will use $m = 187$ and $e = 11$.