MATH CLUB
PUBLIC KEY CRYPTOGRAPHY

MAY 10, 2020

Number theory background

All numbers considered in thsi assignment are integers.

Theorem 1 (Little Fermat Theorem)**.** *If p is a prime, and a is nto divisible by p, then $a^{p-1} \equiv 1 \mod p$*

We will also need Chinese remainder Theorem

Theorem 2. *If m, n relatively prime, and $a \equiv b \mod m$, $a \equiv b \mod n$, then $a \equiv b \mod mn$*

As a corollary of these results, we have the following (see problem 2):

Theorem 3. *Let p, q be distinct primes. Let k be such that $k \equiv 1 \mod (p-1)(q-1)$. Then for any a, we have*

$$a^k \equiv a \mod pq.$$

Public Key cryptography

In RSA model of public key cryptography, the encoding and decoding is done as follows:

First, a person (call him Bob) chooses a number n which should be a product of two primes $n = pq$. In real life, p, q are chosen so that each is about 100 digits long; obviously, in our examples we will use smaller numbers. He also chooses two numbers d, e such that

$$de \equiv 1 \mod (p-1)(q-1)$$

Pair (e, n) is called the public key; pair (d, n) is called the private key. The public key is made widely known (posted online); the private key (and the numbers p, q) he keeps to himself.

Now if someone (say, Alice) wants to send Bob an encrypted email, it can be done as follows. First, the text message is broken into blocks of fixed length, and each block is converted to a number (call it P) between 1 and n. Next, each such number is replaced by an encrypted number C defined by

$$C = P^e \mod n$$

This sequence of encrypted numbers is sent in an email to Bob.

To decode this, Bob uses his private key: he recovers P from C by using the formula $P = C^d \mod n$ (since $C^d \equiv P^{de} \equiv P \mod n$).

The remarkable thing is that here, different keys are used for encrypting and decrypting. What is more, the only way to recover d from e requires finding $\varphi(n)$ — which in turn requires finding the prime factors p, q. Since n is about 200 digit long, factoring it is extremely hard: at the moment, even the most powerful computers can not do it in reasonable time. Thus, for all practical purposes, even if you know the public key (e, n), you can not find the private key (d, n). Thus, anyone can use the public key to encrypt a message to Bob — but only Bob would be able to read it.

You can find the demo here: `https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html`

This scheme has also many other applications, some of which were discussed in class.

1. Compute $2^{2015} \mod 55$.

2. Prove that if p is prime, then for any $k > 0$, $k \equiv 1 \mod (p-1)$, we have $a^k \equiv 1 \mod p$.

3. Prove Theorem 3

4. (a) Find the inverse of 13 mod 60, i.e. solve $13e \equiv 1 \mod 60$.
(b) If a, b are integers such that $b \equiv a^{13} \mod 77$, then one can write $a \equiv b^e \mod 77$ for $e =?$.

5. Assume that a person uses RSA encoding, with public key $(e = 13, n = 77)$, so the encoding is done by the formula

$$C = P^{13} \mod 77$$

Can you find the key that should be used for decoding?

6. Assume that a person uses RSA encoding, with public key $(e = 7, n = 437)$. Break the encoding, by factoring n and finding d. Use it to decode the following secret message:

426 4 215 1 215

7. Two people want to play "stone, scissors, paper" online. However, none can trust the other.

They could play by mail using the following trick: each writes his answer on a piece of paper, locks it in a strong box, and sends to his partner — but without the key. Only after both receive the boxes, they send each other the key.

Can you think of a similar trick which would allow them to play online, using public key cryptography?