Cryptography III

Want to make a billion dollars? Just factor this one number!

3082010a0282010100a3d56cf0bf8418d66f400be31c3f22036ca9f5cf01ef614de2eb9a1cd74a0c344b5a20d5f80df9a23c89

10c354821aa693432a61bd265ca70f309d56535a679d68d7ab89f9d32c47c1182e8a14203c050afd5f1831e5550e8700e008f2

a7229b75688baf129fedbfa7d6a32bc150c047978d948443a0996aad472f62914e4987b7c274bc30beb8603d1a17e7a1c7cc10

941f726e62cca735018c861f55a7ca23c94e223a2586d1b8971b24dd50574939803ac131d0b133613dc2da3e7f2a58114e79ab

3da6dfa8f89f8061739f557686e11a8d59b7917166dc7d2a68dc7ba044a54cdcb02fcfb66b8104d7b29d2cb23dcf20a28ddc62

9b79683c7cf2525facff0203010001

Math Circle

January 28, 2018

Today we are going to conclude our discussion about cryptography by talking about public key cryptography, and the extremely famous algorithm by Ron Rivest, Adi Shamir and Leonard Adleman, the RSA algorithm. Before we get there, let's motivate the need for public key cryptography at all.

1. As we talked about over the last two weeks, symmetric encryption schemes, like one-time padding, can be pretty awesome. As long as you and the person that you want to communicate have a shared secret key that you only use once, one-time padding is totally unbreakable. What if you don't have a secret key and you want to communicate?

   (a) Isn't this exactly what the Diffie-Hellman key exchange did? Describe in words (as precisely as you can remember) what Diffie-Hellman does. You don't have to explain the math operations, you can use the color analogy if you wish.

(b) One problem with Diffie-Hellman is that is susceptible to what is called a man-in-the-middle attack. To talk about what it is, it helps to lead up to it. Suppose that you lived in the good(?) old days and wanted to mail your friend Bob a check in the mail. The mail is picked up at your house and moved by your mailwoman Eve. You don't totally trust Eve. You trust her enough to deliver the mail (eventually), but not enough to not try and snoop around while the mail is in transit. Suppose that a long time ago you and Bob shared blueprints to make a unbreakable lock, and a key to open said lock. How can you send your check to Bob without the risk of Eve fiddling with your check?

(c) Now suppose that you and Bob never shared those blueprints all of those years ago. How could you two use Diffie-Hellman to agree upon a secret blueprint that only you two know over the mail?

(d) When you are doing the key exchange with Bob, how do you know that the messages that you are getting are really from Bob, and not Eve?

(e) One way that Eve could ruin you and Bob's plan to send messages is to lose/destroy everything that both of you try and send. This is true, but if it was happening then you would be able to figure out that Eve was messing with you mail, and sue her! Eve doesn't want to get sued, and so wants to mess with your mail without you or Bob ever realizing it. How could she hijack your key exchange so that both you and Bob think that you're doing a legitimate exchange with the other person, but in fact you are doing a key exchange through Eve?

(f) The word 'authenticate' means to show that something is true, or genuine. If you and Bob had a way of authenticating your messages, how could you two prevent Eve from doing the above?

(g) Without authentication, how can you and Bob know that you are being hoodwinked? How can you stop it?

Hopefully the above problems illustrated a shortcoming with Diffie-Hellman. It works when you know that your messages aren't being tampered with, but if your messages could be changed by a third party, it may be totally insecure.

Now let's talk about public key cryptography. You know what time it is, time for another video! Today's video is called 'Public Key Cryptography: RSA Encryption Algorithm' from the channel 'Art of the Problem.'

`https://www.youtube.com/watch?v=wXB-V_Keiu8`

2. As usual, let's go through some of the things said in the video, but go through them a little bit more slowly...

(a) Just to make sure that you were paying attention (and do that you remember) let's go with the lock/key analogy again. Alice has a the blueprints for creating a lock and a corresponding key. She can send the blueprints to anyone she wants. If Bob wants to send Alice a secret message, what should Alice send Bob? What should Bob do?

(b) And what should Alice do if Alice wants to send Bob a message?

(c) Typically the blueprint to the lock is called the public key, and the blueprints to the lock's key the private key. Why are both of these called a key, if one of them is a lock?

3. Ok, now let's talk about what hard even means

   (a) In the video the author said that it's 'easy' to multiply two numbers, and 'hard' to factor them. In your opinion, what do you think that he meant when he said 'easy' and 'hard'?

   (b) Compute $59 \cdot 83$, as well as $73 \cdot 79$ and $107 \cdot 101$.

   (c) Now, try and find the prime factors of 8051 *Hint, there are two. **Hint, this is probably a problem that you should try and solve as a table.

(d) Let's say that first I ask you to multiply two 3 digit numbers, and then two 6 digit numbers, then two 12 digit ones (I won't! Don't' worry!) estimate how much more time it would take every time I doubled the digits. Don't just say 'a lot longer,' try and estimate how much longer. Would it be twice as long? 4 times? 10 times? 100 times?

(e) Same question if I asked you to factor a 3 digit number, a 6 digit one, a 12 digit one etc...

(f) You might think that a good method to factor numbers quickly would be to just have a huge list of all of the primes, and just go through them one by one! There is a very famous theorem called the Prime Number Theorem that says that the number of primes less than a number x is approximately $\frac{x}{\ln x}$. This is **very** difficult to prove, but for now just take it as fact. Suppose that you wanted to have a list of all primes with fewer than, say, 50 digits. How long would your list have to be? What about all primes with 300 digits?

4. Alright, now let's return to that function Φ, the prime counting function. Remember, we define $\Phi(n)$ to be the number of numbers less than n which are coprime to (that is, have no factors in common) to n.

   (a) Prove that if n is prime, then $\Phi(n) = n - 1$. *Hint, this should be really easy. If it's hard you're barking up the wrong tree.

   (b) Prove that if $\Phi(n) = n - 1$, then n is prime. *Hint, this proof should be a little different then the last problem. Still easy though.

   (c) **Prove that for relatively prime** m, n $\Phi(n \cdot m) = \Phi(n)\Phi(m)$.

(d) Compute $\Phi(n)$ where n are three numbers that you got in problem 3.b), as well as 8051.

(e) If for any natural numbers m, n where $m < n$, $m^{\Phi(n)} \equiv 1 \bmod(n)$ if true, show that for any k it is also true that $m^{k\Phi(n)+1} \equiv m \bmod(n)$

(f) **Once you choose the value for e, you need to choose d so that $de \equiv 1$ mod$(\Phi(n))$. How can one compute d given e?**

5. Finally let's return to the problem of authentication.

   (a) **One property of RSA is that you would swap the public and private keys, and nothing would change. Use this fact and show how, in our first example, Alice could authenticate a message, that is she could prove that a message definitely came from her.**

   (b) **How can Alice and Bob use this authentication technology to beat Eve?**