Joshua Brown

9 Algorithms ch. 9

November 8, 2018

Digital signatures have become the main solution for making payments or transactions online. A digital signature is an electronic signature that encrypts a document with a digital code that is hard to duplicate. Digital signatures use an effective strategy to protect people’s transactions and keeps them from being able forge their signature. Digital signatures consist of three algorithms which include signing with a padlock, signing with a multiplicative padlock, and signing with an exponential padlock.

The signing with a padlock algorithm begins with all persons getting three padlocks as well as three keys. It is important to note that all three of the padlocks and keys are the same for each person (one will be given to the bank). Let’s say Mark owes Martha 100$. Martha then writes a note saying she owes Mark 100$ and places it in her box that is locked with her padlocks. She then gives Mark the box and all she must do is go to the bank, ask for the key, and there she has proof that Mark owes her 100$. The advantage of this algorithm is that you cannot deny authenticity once you have written the note. The problems with this algorithm are that requires cooperation from both parties and it wouldn’t be very difficult to forge.

Instead of using physical boxes and keys, the multiplicative trick uses mathematical objects which are represented digitally. Specifically, the keys are represented as numbers and the clocks as clock arithmetic. Also, instead of writing in plain English, everything will be translated to numbers. Mark will then choose a clock size and choose a number less then his clock size as his numerical pad lock. For Mark to lock his message he will then multiply his message with the pad lock. To then unlock that message, you must multiply the message by the multiplicative key. This process not only verifies a digital signature, but if the message is not the same when you use the multiplicative key, the signature has been forged. The disadvantage of using this algorithm is that you still have a 3rd party. With out the 3rd part Mark could distribute a false key and make the signatures appear invalid.

Building upon the last algorithm, instead of using simple multiplication, we are upgrading to exponents. The algorithm works the same as before, pick a clock size and padlock value, then use a computer to find the key value. When you are trying to unlock the padlock, you use the exponent key and if the results match the signature is authentic. The process is known as the RSA scheme and as of now, it makes it impossible for somebody to reverse the process of creating the clock size and padlock value. The fixes the flaw in the multiplicative algorithm. But it seems even this algorithm has its own flaw. That flaw is integer factorization, and whoever creates a perfect integer factorization algorithm will be able to break any known RSA algorithm.

The main use of digital signatures is for downloading software. If the software is signed your computer unlock that padlock and the software is downloaded. There is no digital signature algorithm that has been confirmed 100% secure and because of that we all must be careful of what software we download. This chapter was very interesting in that I had never heard about digital signatures before and I now know to be careful when downloading software.