CS 2, Spring 2018

Tyler Furreboe

February 8th, 2018

Dr. Gurka

Public Key Cryptography

The goal of cryptography is to be able to send secret information between two computers over the internet, what makes this hard, however, is the internet is public and open, so every device on the internet can intercept this data being carried from router to router, but what prevents other computers to be able to recognize this information are public and private numbers.

Essentially, here’s how cryptography works, on your personal computer, there is a private key – and on your friend’s computer he also has a private key. Now, spoken out loud across the open internet is the public-private number (The public number, 2 to the power of the private number: Like so, PPN = 28 = 3) and public numbers (Say, 11 and 2). What happens, is that you will take your public number, 2, and use it to exponentiate your private number 8, with a clock size of the other public number, 11, which gives you a public private number of 3, because (PPN = 28 = 3 (clock size 11)). On your friend’s computer, the same process occurs, his computer will take the public number 2, and use it to exponentiate his private number 9, with a clock size of the other public number 11, which gives him a public private number of 6, because (PPN = 29 = 6 (clock size 11)).

Now what happens, is that your computer takes your friend’s public-private number 6, and exponentiates it against your private number, 8. So (your shared secret = 68 = 4 (clock size 11)) and your friend’s computer does the same except with your public-private number, so he will get (friend’s shared secret = 39 = 4 (clock size 11)).

Typically, in practice the numbers are much, much larger – but the process is essentially the same, the reason nobody else can get this information is because they’ll never be able to get the correct results by mixing their own number into the equation, since they’ve already been mixed… Any extra “mixing” the outside computer attempts to do, will only produce inaccurate results.

The article didn’t say this, but there is a current issue that I know of with this cryptography algorithm, the issue being with the new era of computing, Quantum-Computers. These computers have shown to be able to decrypt almost any RSA encrypted messages, rendering cryptography in the Quantum-Computer age, essentially useless.

Overall, cryptography has been a major success, it has helped the internet turn into what it is today, to allow online payments, conversations, the ability to save and secure private documents, it’s provided a great secure way to handle information across the internet.

I would probably implement this algorithm if I were to create a login on a website or if I needed to accept someone’s credit card information, as it is important those message stay secured.