FNCE 385/885 Assignment 2: Blockchain Cryptography

Due: 3:30 pm, Wed Nov 30, 2016

In this assignment you will perform some basic cryptography work. You will have some direct experience of working with Hash and getting to know what Hash does.

We need to work with R package *digest*.

You will start with creating a key, and then try to sign some messages using that key. Then you will check if three messages are signed by the correct party. Finally, you will have a sense on how BitCoin mining works.

We will also provide a function to calculate (x^d)module(y), when x^d is fairly large.

Part 1: Create Keys

Recall how public and private keys are created in class. Suppose that $p = 7$, $q = 23$, and $e = 13$.

a) What is the public key?

b) Let d be the *smallest positive interger* which can be used to create the private key. What should the private key be?

You are expected to get the private key using R: a loop with some conditions can do that. The correct d lies in range [55,65].

Part 2: Sign a message

Use the *private* key you generate above, sign a message: 12.

Your result should be one number only.

Part 3: Check if a message is authentic

Suppose you receive the following three messages

1. Message1: $[10, 24]$; signed message: $[210, 453]$.
2. Message2: $[11, 30]$; signed message: $[519, 370]$.
3. Message2: $[12, 16]$; signed message: $[12, 594]$.

They all share the same public key, which is obtained in Part 1.

Which of these three, if any, are authentic? provide your reasoning.

Part 4: Mining BitCoin

In this part we will generate proof-of-work, similar to what Bitcoin miners do.

Specifically, suppose that you receive a message: "2017", and you work with Hash function *md5*. Find a number x attached to "2017" such that after the transformation with the Hash function your output starts with *at least* three 0's (zero). To reduce the amount of work, you can start with $x = 1000$.

In R, the command of calculating md5 Hash function is digest(x,algo = "md5"), where x is the message to be transformed. The command for combining strings is paste(c(x, y),collapse=""), where x and y are two different strings.

Part 5: Think about mining BitCoin (BONUS)

In this part you will try to think about a strategy of mining BitCoins. Remember that, a BitCoin miner tries to find some strings attached to original message such that the new message after Hash calculation starts with k zeros.

a) Suppose you have several opponents who have similar computational ability to you, and they all start with some number (say 0) and then try different numbers according to some

ordering rule $(0, 1, 2, 3, \dots)$. In order to compete against them, what might be you best choice of number to start with?

b) Suppose you happen to find that there is another smart guy who uses your strategy in a), what should you do? Suppose again that, each time you get a new strategy, some new smart guy enters the game and uses your newly-developed strategy, what will you do?

c) What might be miners' strategies of choosing numbers for trials in equilibrium?