CS 161 – Computer Security
Instructor: Tygar
13 October 2015

Homework 5 Answer Set

Notes

- Homework 5 is due on 13 October 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- Please keep your answers brief
- Submit this homework using Gradescope.

Please start the answer to each question (including subquestions) on a new page

1. Show a man in the middle attack on the following authentication protocol:

   $A \rightarrow S$: A, B, Na
   $S \rightarrow A$: $A, B, \{A, Na, Kab\}_{Ka}, \{B, Na, Kab\}_{Kb}$
   $A \rightarrow B$: $A, B, \{B, Na, Kab\}_{Kb}$

2. For questions 2 and 3, use the web site https://blockexplorer.com. For question 2, examine block 378741.
   a. How many transactions are there in this block?
   b. The block reward is 25 BTC, but how much in total did the miner who found this block receive for doing so? What accounts for the discrepancy?
   c. Look at the fourth transaction (the third after the coinbase transaction). How many inputs and outputs are there? What is the most likely explanation of why the recipients did not receive the same amount?
   d. What is the sum of the inputs? What is the sum of the outputs? What are the first six characters of the address of the recipient of the difference between (inputs – outputs)?
3. Examine block 378732.
   a. What is unusual about this block? What is the most likely reason that this unusual occurrence happened?
   b. What nonce did this miner find?
   c. On average, how many hashes would you expect a miner to need to try to find this particular nonce?
   d. Look at all the transactions that the miner who mined this block has received (state the precise time (in PDT) that your figure is accurate as of – which should be a time between 10/13/15 and 10/20/15). Roughly how much is this in US dollars? How has this miner managed to receive so many bitcoins in transactions?