Zelong Li
24569650
Discussion 102
TA: Qi Zhong
CS161 Homework 5

1.

Let M be the man in the middle. Let K_m be the secret key of M (only S and M know it).

A → M: A, B, Na

M → S: A, M, Na

M → S: M, B, Nm

S → M: A, M, $\{A, Na, Kam\}_{Ka}$, $\{M, Na, Kam\}_{Km}$

S → M: M, B, $\{M, Nm, Kmb\}_{Km}$, $\{B, Nm, Kmb\}_{Kb}$

M → A: A, B, $\{A, Na, Kam\}_{Ka}$, $\{M, Na, Kam\}_{Km}$

A → M: A, B, $\{M, Na, Kam\}_{Km}$

M → B: A, B, $\{B, Nm, Kmb\}_{Kb}$

Now, A only knows Kam, the session key between A and M and B only knows Kmb, the session key between M and B. However, both A and B think they are communicating with each other. Thus, when communicating, A will encrypt its message with Kam and B will encrypt its message with Kmb. And, M will be able to know all the messages.

2.

a. There are 444 transactions in this block.
b. 25.07264926 BTC. There is a discrepancy due to transaction fees. For large size transactions, there are transaction fees. When a new bitcoin block is created, information of all transactions is included in the block, and the user who created the block collects the corresponding transaction fees.
c. There is one input and two outputs. The recipients did not receive the same amount of bitcoins because one recipient is the actual recipient, and the other one is for the change. Specifically, when an output of a transaction is used as an input of another transaction, the amount of bitcoins should be spent entirely. When this amount is higher that what the owner wants to spend, a new address is created for the change of this transaction.
d. The sum of inputs is 8.81701738 BTC, and the sum of outputs is 8.81612307 BTC. The first six characters of the address of the recipient of the difference between inputs and outputs are 1M5hoG.

Reference:
https://en.bitcoin.it/wiki/Transaction_fees
https://en.bitcoin.it/wiki/Change

3.

a. There is only one transaction in block 378732, which is the coinbase transaction. It is most likely that there are no transactions between previous block and this block.
b. 2933092036
c. $(60813224039.440346 \times 2^{256})/(0xffff \times 2^{208}) \approx 2.612 \times 10^{20}$ hashes
d. Oct 19 16:07, 27904.38865027 BTC, or 7372897.57 USD. This miner may have a stronger computational power; this miner could have a mining pool that many computational powers collectively solve this block.