6.857 Homework	**Problem Set 2**	# 2-1 Secret Sharing
Changping Chen		
Peinan Chenn		
Skanda Koppula		March 3, 2015

(a) We can give only A and B shares of the secret and then require that there must be 2 out of 2 parties to construct the secret in a Shamir secret sharing scheme.

(b) Assuming we have some combination of gates that take inputs and outputs the secret if the inputs are correct, we will start our definition of our scheme by working top down starting from the output. Starting from the output, whenever there is an OR gate, we make it so each input of the OR gate will construct the same secret, which is also the output secret. Whenever we see an AND gate, we give each of the inputs of the gate a different share that is also itself a secret and make it so that we need shares equal to the number of inputs of the AND gate to produce the output secret with Shamir secret-sharing. Each input to an AND gate has its own secret (its share), different from that of the other inputs to that AND gate as well as the output. The input to the AND gate needs to determine its own secret before it can provide an input to the AND gate. In other words, we make each AND gate a N out of N gate and make it so that each input to the AND gate needs to construct its share since the share is also a secret. For each T out of N gate, we use Shamir secret-sharing. Part c will illustrate how this scheme works with an example.

(c) We make it so both inputs of the OR gate will construct the same secret. So, Professor Rivest gets the secret and ((2 out of 3 TA's) AND (10 out of 20 students)) will be able to construct the same secret. We then make the AND gate a 2 out of 2 Shamir secret-sharing gate and give both inputs a share which is also a secret. In this case, (2 out of 3 TA's) will be enough to reconstruct S1 and (10 out of 20 students) will reconstruct S2. Where S1 and S2 are secrets, S1 is not S2, and S1 and S2 are the shares that together will reconstruct out original secret. Then, we use Shamir secret-sharing for both (2 out of 3 TA's) and (10 out of 20 students) such that (2 out of 3 TA's) will reconstruct the secret S1 and (10 out of 20 students) will reconstruct the secret S2.

6.857 Homework	**Problem Set 2**	# 2-2 Hash Functions
Changping Chen		
Peinan Chenn		
Skanda Koppula		March 3, 2015

6.857 Homework	**Problem Set 2**	# 2-3 Cryptocurrency
Changping Chen		
Peinan Chenn		
Skanda Koppula		March 3, 2015