ENEE 457
Dining Cryptographers Class Exercise

1. Assume there are three dining cryptographers, P_1, P_2, P_3. Each wants to broadcast a message m_1, m_2, m_3, but at most one party can successfully broadcast a message in each round. Assume the parties have agreed to run the protocol for several rounds. At the beginning of each round each party flips a coin. If it is heads, the party broadcasts a message. If it is tails the party does not broadcast its message. Explain what each party should broadcast in each round. On average, how many times will the parties need to run the protocol for each message to be broadcast? How will the parties know when all three messages are broadcast

Solution: First, let's assume we can tell when a message is successfully broadcast. Then the number of rounds it takes to successfully broadcast all three messages is around 8. This is because some party successfully broadcasts in a given round with probability 3/8 (one party gets heads and two get tails). So in expectation, it takes 8/3 rounds for the first party to broadcast. For all three parties to successfully broadcast, it takes less than 3*8/3 = 8 rounds.

Now, let's go back to seeing how to tell if a message is successfully broadcast. A party broadcasting a message will prepend k blocks to its message, each block is chosen at random from {01, 10, 11}. If any of the first k blocks of the received message are set to 00, then the parties know the message was *not* successfully transferred. Otherwise, they assume it was. The probability that 2 or 3 parties are simultaneously broadcasting but none of the k blocks are set to 0 is $\left(1-\frac{2}{9}\right)^k$. This decreases exponentially so becomes negligible for sufficiently large k