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