1. **On the ThreeBallot voting system.** Suppose there are 3 candidates vying for a position: Alice, Bob and Carol. Each of the three ballots then consist of 3 candidates. We can encode a vote using a 3-bit string. For example, if a voter shaded Alice and Bob, we encode it as 110; if the voter shaded Bob and Carol, it would be 011. Thus, every voter’s 3-ballot can now be encoded by three 3-bit strings; e.g., the ballot in Figure 10.15 of your book is (100, 010, 101).

   a. For our purposes, we shall represent each valid 3-ballot by three 3-bit strings that are ordered lexicographically. For example, the ballot in Figure 10.15 will be represented as (010, 100, 101). List all the valid 3-ballots for this setting.

   b. To have some individual verification, the system tells the voter to pick one of the three ballots arbitrarily. A copy of the ballot is then made and given to the voter as a “receipt”. The voter can then verify from the public bulletin posted at the end of the election that this particular ballot was processed correctly. Thus, the voter is assured that his/her vote was correctly counted with a probability of $\frac{1}{3} = 33.33\%$. A reason why a voter is only allowed to choose one ballot as a receipt is because a single ballot can never leak information. That is, if the voter shows his/her receipt to another person, that person will have no idea how the voter voted.

   For each of the valid 3-ballots you’ve listed in part (a), determine if there are two ballots that can used as a receipt so that these two ballots will still not leak any information. If so, this means that the assurance probability for the voter can increase to $\frac{2}{3} = 66.66\%$.

   c. Graduate students: describe mathematically the 3-ballots that can have 2 receipts where no information is leaked. That is, what properties should these 3-ballots have?

2. These days, a DoS attack is more likely a distributed one where the computers involved are either part of a botnet or volunteered to be part of a botnet. In the press, the attack is often described as “a large number of computers sending traffic to particular server/ website causing the latter to go down”. Investigate one such attack that has taken place in 2011 or 2012 and find out as much as you can about the particulars of the attack. For example, does it resemble a SYN Flood, a Ping Flooding, etc.? If not, what technique was involved? How was the attack stopped?

3. C-5.4

4. C-5.6

5. Graduate students: C-5.8