Fall 2022 CIS 3362 Final Exam Part A – Odds and Ends (12/9/2022) Solutions

1) (5 pts) In the description of the birthday paradox in class, a subproblem solved was of the form: given k people in a room, what is the probability that each of them have a different birthday. In solving this problem, it was assumed that each of the 365 birthdays is equally probable, and the multiplication principle was applied: the probability that each subsequent person's birthday was different than all the previous was multiplied to the total result. Consider a similar problem where there are 200 Venetian days in a year, but it's twice as likely that someone is born in the first 100 days of the year than the last 100 days. Thus, the probability of being born on a single day in the first half of the year is 1/150 and the probability of being born on a single day in the second half of the year is 1/300. (Yes, these 200 numbers add to 1!) In attempting to figure out the probability that all of k Venetians in a room have different birthdays, explain why the basic multiplication principle does not work.

The first Venetian you ask might have a common or less common birthday. So when determine the probability that the second Venetian you will ask has a different birthday than the first, it could either be $\frac{299}{300}$ OR $\frac{149}{150}$. The multiplication principle in probability ONLY works if the probability of an event occurring in a given situation is always the same. In the regular birthday problem, no matter what the first person's birthday is, the probability the second person has a different birthday is $\frac{364}{365}$, thus we are allowed to multiply our running tally by this fraction.

Grading: Largely all or nothing. It's a clear principle that is violated. Partial credit may be given for poor explanations that seem to hint at the idea.

2) (5 pts) Consider using Quantum Cryptography (as described in class) to allow Alice and Bob to exchange a sequence of secret bits. In the scheme described in class, Bob is supposed to randomly guess which reader to use. Consider a situation where instead of making a random selection, Bob decides to alternate readers (horizontal, diagonal, horizontal, diagonal). Why might this prevent Alice and Bob from exchanging a sequence of secret bits?

It's not unusual to imagine a situation where Eve guesses some sort of pattern like this and tries to do the same thing as Bob. If she does, then Eve will never be detected, because for every bit that Bob uses the correct reader, he will get the correct answer and Alice and Bob will conclude that no one was listening!

Grading: Again, largely all or nothing. Key is understanding that the randomness is what prevents Eve from making the same guess as Bob, and that if Eve is able to guess the same as Bob, she will go undetected.