Homework #4

Due: March 5, 2024 **Points:** 100

Questions

1. (*10 points*) With the exception of the break-the-glass policy model, the hybrid modes we have studied do not discuss availability. What unstated assumptions about that service are they making?

2. (*30 points*) Consider the systems Louie and Dewey in Section 9.2.4.

   (a) Suppose the sends and receives for the buffers are non-blocking. Is the composition of Hughie, Dewey, and Louie still noninterference-secure? Justify your answer.

   (b) Suppose all buffers are unbounded. Is the composition of Hughie, Dewey, and Louie still noninterference-secure? Justify your answer.

3. (*25 points*) Consider again the algorithm in Figure 9–7. The power used is another side channel for most instantiations of this algorithm. Explain how this side channel works. How might you add sufficient noise to it to render it unusable?

4. (*20 points*) A company develops a new security product using the agile programming[1] software development methodology. Programmers code, then test, then add more code, then test, and continue this iteration. Every day, they test the code base as a whole. The programmers work in pairs when writing code to ensure that at least two people review the code. The company does not adduce any additional evidence of assurance. How would you explain to the management of this company why their software is in fact not "high assurance" software?

5. (*15 points*) Prove that for $n = 2$, $H(X)$ is maximal when $p_1 = p_2 = \frac{1}{2}$.

[1] In the book, this is called "extreme programming"