Review questions. (These will not be graded and need not be turned in. However you should make sure you are comfortable answering these questions.) In all the following, we roll three independent, fair dice and let the results be $X_1, X_2, X_3$.

- What is $\Pr[X_1 \in \{3, 4, 5\}]$?
- What is $\Pr[X_1 = X_2]$?
- What is $\Pr[X_1 = X_2 = X_3]$?
- What is $\Pr[X_1 = X_2 | X_2 = 6]$?
- What is $\Pr[X_1 = X_2 = X_3 | X_2 = X_3]$?
- What is $\Pr[X_1 + X_2 = X_3]$?

Graded questions. (Please turn in the answers to these questions. Grading will be done by choosing a random subset of the questions, and grading the answers to those questions for all students.)

1. Exercise 1.2.
2. Exercise 1.3.
3. Exercise 1.6.
4. (*) Let $p_1, p_2$ be two independent, uniformly generated passwords, each 4 characters long. Say $p_1$ is encrypted using the shift cipher, and an attacker sees the resulting ciphertext. What is the probability (taken over choice of $p_1, p_2$, and the key used for encryption) that the attacker can conclusively determine that $p_1$ was encrypted? (Assume the attacker knows $p_1, p_2$.) Repeat for the Vigenère cipher with a period of 2, a period of 3, and a period of 4.
5. Exercise 2.1.
6. Exercise 2.2.
7. Exercise 2.3.
8. Exercise 2.4.