Math 4981 Spring 2021
Cryptography HW 4
Due Thursday, February 11

1. Let Ω be a (finite) probability space, and let E, F, G be events.

   (a) Prove that $P(E \cup F) = P(E) + P(F) - P(E \cap F)$.

   (b) Prove that $P(E \cup F \cup G) = P(E) + P(F) + P(G) - P(E \cap F) - P(E \cap G) - P(F \cap G) + P(E \cap F \cap G)$.

2. Suppose we have two boxes. Box A contains three blue balls and four red balls; box B contains five blue balls and two red balls.

   (a) We choose a box at random (50% chance of each box), and then pick a ball out of it at random. What is the probability that the ball is blue?

   (b) Suppose we choose a box at random, draw out a random ball, and the ball is blue. What is the probability that the box we chose is box A?

3. Suppose we have two boxes. Box A contains three blue balls and three red balls; box B contains six blue balls and zero red balls.

   (a) We choose a box at random and then choose a ball at random. What is the probability the ball is red?

   (b) Suppose we choose a box at random, draw out a random ball, and the ball is red. What is the probability that the box we chose is box A?

   (c) Suppose we choose a box at random, draw out a random ball, and the ball is blue. What is the probability that the box we chose is box A?

   (d) How does this relate to the slogan "absence of evidence is not evidence of absence?"

4. For cryptographic purposes, we often need to generate large prime numbers. In practice, we generate a random number, test whether it's prime, and repeat until one of the numbers passes our tests. But it's also difficult to determine for sure whether or not a number is prime, so we use a much faster test that has a chance of giving the wrong answer.

   One specific prime test is the Miller test. Every prime number will pass the Miller test; a composite number has a $\frac{1}{4}$ chance of passing the Miller test. (It's actually less than that, but $\frac{1}{4}$ is a good upper bound.)

(a) If we pick a random 100-digit number, it has about a $\frac{1}{230}$ chance of being prime. Suppose we choose a random 100 digit number, and then use the Miller test and it passes. What are the odds that our number is prime?

(b) We can repeat the Miller test with different "bases" to get independent chances of success. Thus if we try the Miller test k times, a prime number will pass all of them, while a composite number will pass all of them with probability $\frac{1}{4^k}$. Suppose our random 100-digit number passes five Miller tests. What are the odds that it's prime?

(c) How many Miller test would our number have to pass to reach a 99% chance of being prime?

5. Compute the expected value of the random variable X if:

(a) The values of X are uniformly distributed on the set $\{0, 1, 2, \ldots, n-1\}$

(b) The values of X are uniformly distributed on the set $\{3, 6, 11, 15, 22\}$

(c) The values of X follow a binomial distribution with $n = 5$ trials and probability of success $p = .6$.

(d) The values of X follow a binomial distribution with n trials and probability of success p.

6. Which of the follinwg random variables should be given a uniform distribution, and why?

(a) X is the roll of one die.

(b) X is the number of heads obtained in ten coin tosses.

(c) X is the number of coin tosses it takes to get one head.

(d) X is the birthday of a randomly chosen person.

7. Suppose X is the random variable associated to rolling two (six-sided) dice and adding them together. Give an explicit description of the probability density function $f_X(x)$, and graph the probability density function f_X and cumulative density function F_X associated to X.

8. Consider a cipher with three keys, three plaintexts, and four ciphertexts, given by:

	m_1	m_2	m_3
k_1	c_2	c_4	c_1
k_2	c_1	c_3	c_2
k_3	c_3	c_1	c_4

Suppose all keys are equally likely, and the messages have probability $P(m_1) = 2/5, P(m_2) = 2/5, P(m_3) = 1/5$.

(a) What is the probability of each ciphertext?

(b) Compute $P(c_1|m_1), P(c_1|m_2), P(c_1|m_3)$. Can you tell if the ciphertext has perfect secrecy from this calculation?

(c) Compute $P(c_2|m_1), P(c_3|m_1), P(c_4|m_1)$. Can we combine this with the previous answer to tell if the cipher has perfect secrecy?

(d) Compute $P(k_1|c_3), P(k_2|c_3), P(k_3|c_3)$.

9. We proved in class that if a cryptosystem has perfect secrecy, then $\#\mathcal{K} \geq \#\mathcal{M}$. Give an example of a cryptosystem with $\#\mathcal{K} = \#\mathcal{M} = \#\mathcal{C} = 3$ that has perfect secrecy, and show explicitly that it has perfect secrecy.

10. Suppose $\#\mathcal{M} = \#\mathcal{C}$. Prove that for a fixed key $k \in \mathcal{K}$ and a fixed ciphertext $c \in \mathcal{C}$, there is a unique plaintext $m \in \mathcal{M}$ such that $e(k, m) = c$. (Hint: this is a counting argument using the fact that e_k is 1-1).