Deadlines:

For all Groups: November 1 2022

Grading system:

- 1 problem - 6

- 2 problems - 7

- 3 problems - 8

- 4 problems - 9

- 5 problems and bonus – 10

1. How much should I bet ?

Are you in for some betting ? Let’s play a game. There are some specific rules to this game: A fair coin will be flipped until it falls on its head for the first time. You will be paid $2 to the power of j dollars if this occurs on the jth toss. You are sure to win at least 2 dollars so you should be willing to pay to play this game, but how much ? Few people would pay as much as 10 dollars to play this game. See if you can decide, by simulation, a reasonable amount that you would be willing to pay, per game, if you will be allowed to make a large number of plays of the game. Does the amount that you would be willing to pay per game depend upon the number of plays that you will be allowed ?

2. I bet my life on this one

Are you still in the mood for betting ? Now let’s play something more interesting and serious! Let's try our skill at Russian roulette. Here's the conditions. I only have two bullets in my revolver, which has a 6-slot barrel.Now I put the bullets into the revolver in **adjacent** slots, spin the barrel and hand you the gun. You point the gun to your head. You pull the trigger and ... Click! you're still alive. Congratulations but the game is not over yet. You have to pull the trigger one last time. Now you have two choices. 1 You spin the barrel afterwards you pull the trigger. 2 You pull the trigger without spinning. Luckily you have some time and a computer with you in your bag so you can simulate the current situation such that you can choose the correct choice.

Your assignment is to calculate the probability for both cases and after you've found the probability for the initial conditions you need also to find out what are the probabilities in case the bullets are not adjacent. Now you need to calculate the same probabilities but in case when you have 2 bullets and the gun has a 5 slots barrel. You have to present the result for 8 different outcomes. Good luck staying alive.

3. Tennis

Ana and Dan decided to play tennis only, they changed a rule so that the person who serves continues to do so as long as they win the point. The first player to win 25 points wins the game. Assume that when Ana serves first the probability of winning a point is 0.7 and the probability when Dan serves is 0.5. Estimate, by simulations, the probability that Ana will win the match.

4. Roulette

One of the most popular casino games is roulette. Many people like roulette because it is an easy game to learn and play. Unlike other casino games, roulette doesn't have many complicated rules to follow or strategies to perfect. A regular casino roulette wheel has 38 slots numbered 0, 00, 1, 2, . . . , 36. The 0 and 00 slots are green, and half of the remaining 36 slots are red and half are black. A croupier spins the wheel and throws in an ivory ball. If you bet 20 dollars on red, you win 20 dollars if the ball stops in a red slot, and otherwise you lose 20 dollars. Find the total winnings for a player who makes 1000 bets on red. Another form of bet in roulette is to bet that a specific number (say 18) will turn up. If the ball stops on your number, you get your dollar back plus 35 dollars. If not, you lose your dollar. Write a program that will plot your winnings when you make 500 plays of roulette at a casino, first when you bet each time on red, and then for a second visit to the casino, when you make 500 plays, betting each time on the number 18. What differences do you see in your winnings on these two occasions?

5. Birthday attack

This exercise aims to introduce you to a very basic concept of hashing algorithms, how they work, why they are useful and what are their weaknesses. And along the way you'll pick up the principle behind the flaw of hashing functions.

Do you remember at some lesson I explained to you about the **birthday paradox** that was used creating **birthday attack**. Now you're gone make the **birthday attack** with the **md5**

hashing algorithm. Your task ahead is to find collisions for this algorithm, (only for the first 40 bits of the hash, aka first 10 hex characters).

You have to write a small program that would eventually find a collision for the first 40 bits generated by the **md5** algorithm.

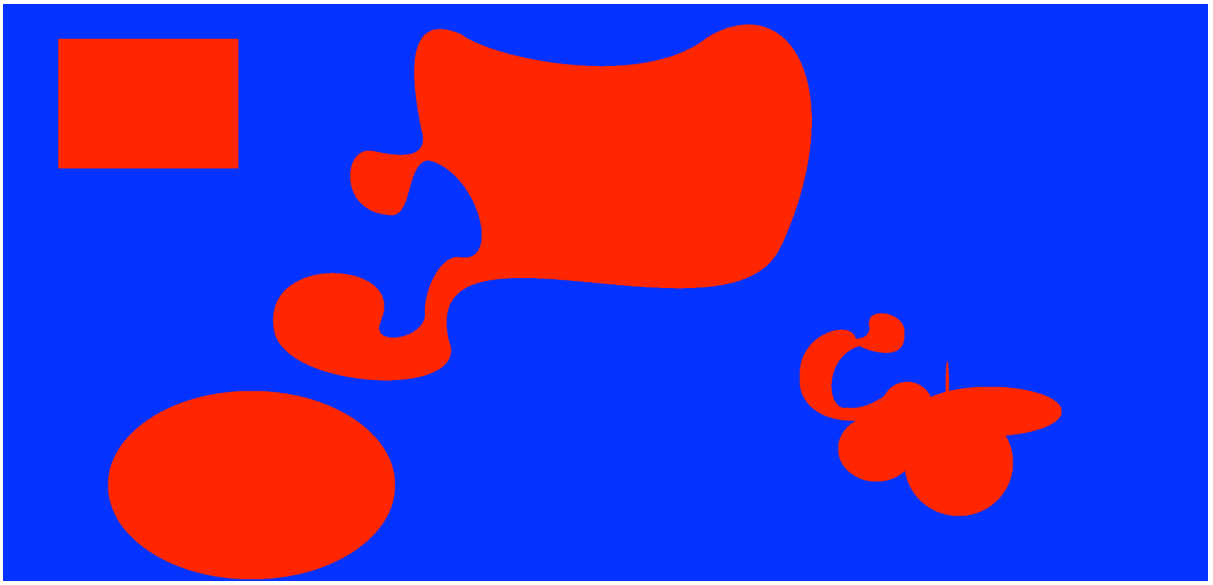
PRO Tip:

For better understanding what is birthday attack watch this video: video

Tip:

Cracking the first 40 bits usually takes a few seconds (might get to a dozen of seconds), hence I recommend for starters to find the collision only for the first 20 bits. Once it is working you can increase the number.

BONUS: PROBLEM



This morning the CIA faxed UTM the following map scan(image is also in the zip file from the email). The total captured surface is around 42 square miles (duh... this imperial metric). With red is marked the land that is mined by the guerrilla forces and at the moment they need to evaluate the logistics required to defuse the deadly mines. But they do not have enough computing resources to compute the red area from the map. Which is why they are playing their trump card, the brilliant engineers from FAF.

The stakes are very high, and lots of innocent lives can be spared. So please compute the mined area a.s.a.p., using Monte Carlo method.

Tip:

The recommended python library for image processing is **pillow** (not the one you use to sleep).