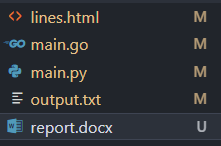
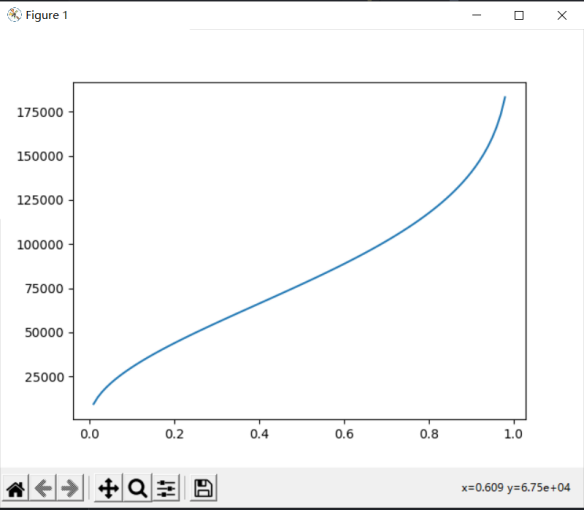
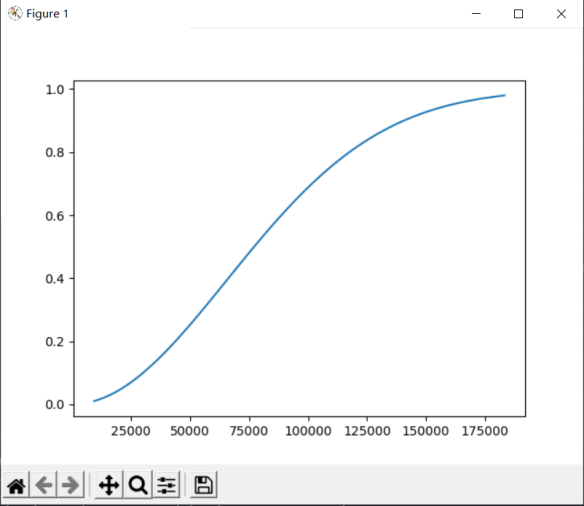
CSCI971 Modern Cryptography Assginment One: Verify the birthday paradox

All the files of this experiment are as follow. Each of them will be discussed in this document.



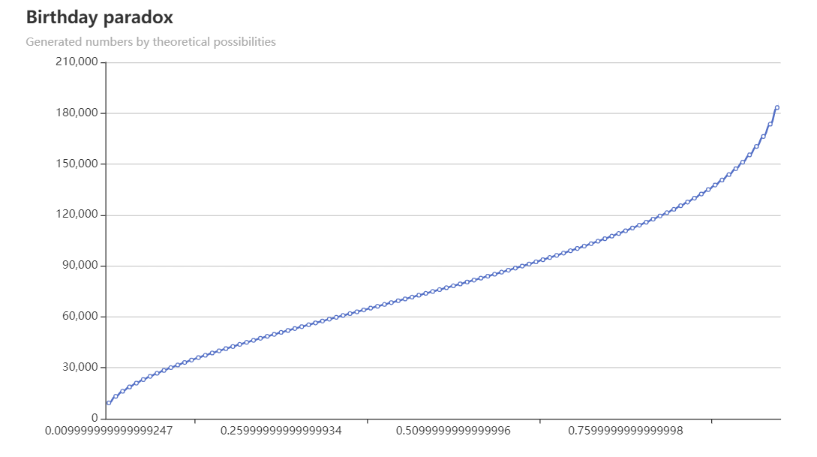
Step 1: Calculate the theoretical numbers need to be generate for given possibilities.



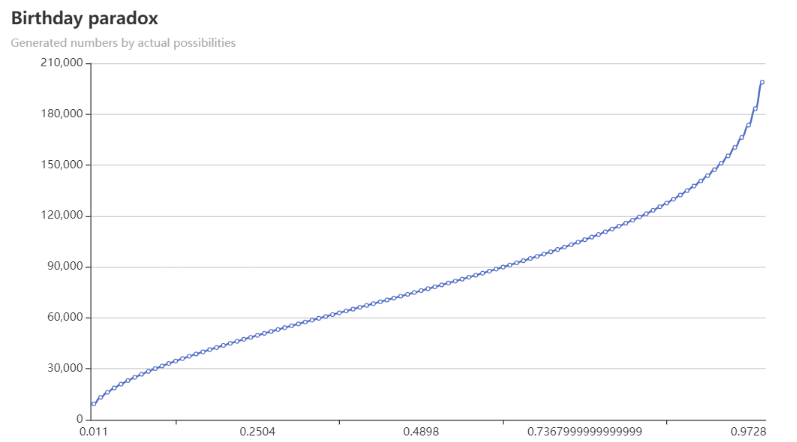
The main.py file is used to calculate and illustrate the theoretical numbers need to be generated for given successful possilibities. In the first picture, the x axis is the theoretical numbers that need to be randomly generated, and the y axis is the successful rate of collision. In the second picture, the x axis is the successful rate of collision, and the y axis is the theoretical number that need to be randomly generated.

Step 2: Verify the theoretical value.

The function birthday\_uint32\_max in the main.go file accept one parameter which indicates successful collision possibility, and then return the theoretical numbers needed for the given successful possibility. This program firstly calculate the theoretical numbers needed for given possibilites (from 1% to 99%). Then this program does some experiments to verify the actual successful possiblities when the theoretical numbers are generated. For each calculated theoretical number for a given possibilities, the actual possibilities is verified by a group of experiments were executed and repeated 5000 (5 \* 1000) times. After each small group of experiments are executed, the average hint, the average possibilities and the variance will be calculated. When the main.go file is executed by running go run main.go > output.txt, the output information of the process is redirected to the output.txt file. At the end of the main.go file, it tried to create a file named as “lines.html” to store the picture illustrating the relationship between theoretical numbers and given possibilities and the relationship between theoretical numbers and actual possibilities.



Generated numbers by theoretical possibilities



Generated numbers by actual possibilities

For more information about this experiment, please refer to files which were discussed above.