[Logan, Shreeyasha, and Suprabha]

Project #1 Report

1)

The distribution of the random numbers we got from generating numbers through using Python from negative one thousand to one thousand did appear as random as each number ranging from -1000 to 1000, when combining the 100 independent experiments no number appeared less than 424 times (-808) and more than 577 times (437). Hence all numbers appeared around 0.0424%-0.0577% of the time.

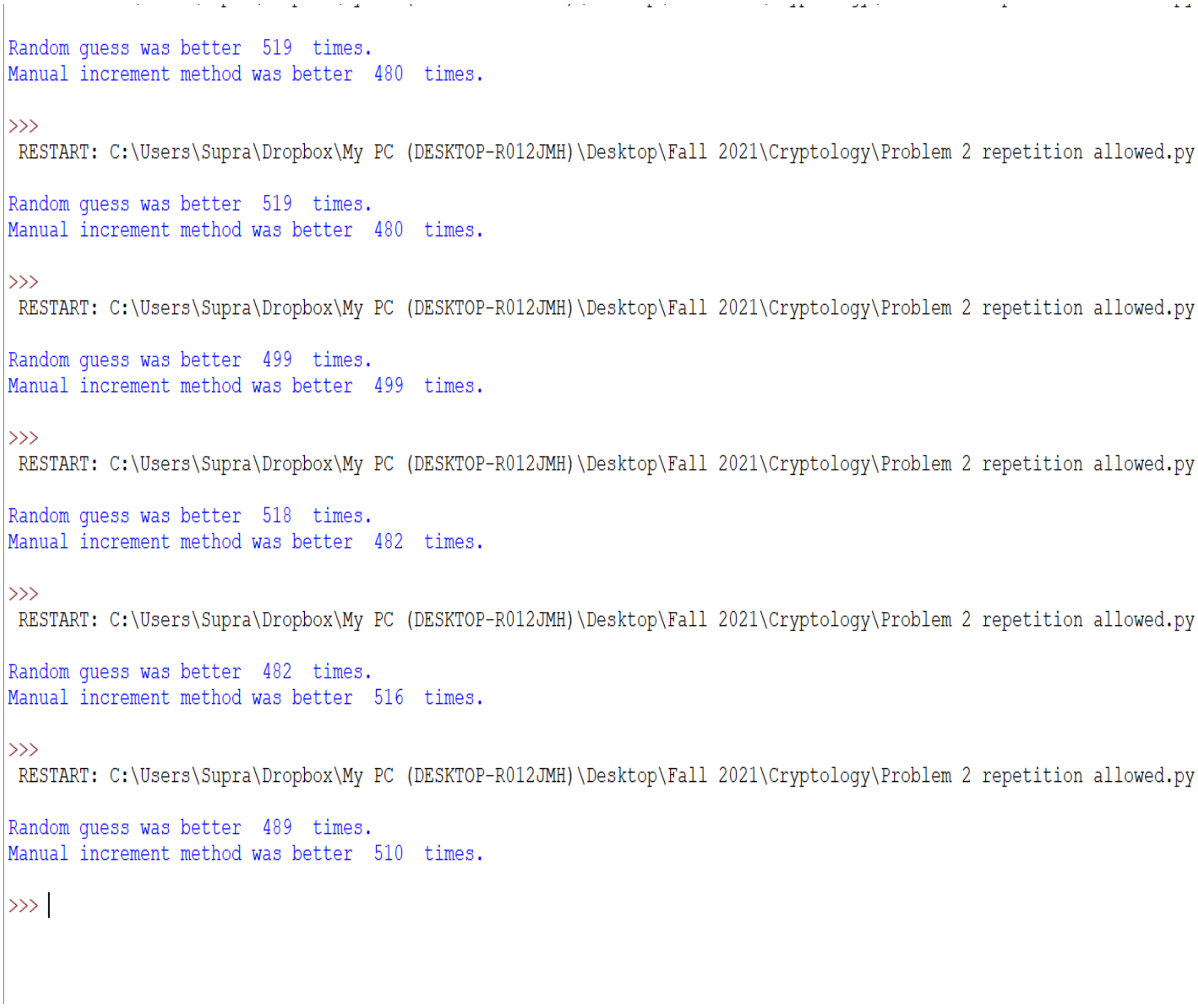
To support our statement, despite the code ran faster when running it one time through to generate 1,000,000 different numbers, when the code was executed as 100 independent trials it allowed us to increase the probability of an accurate conclusion being drawn and eliminating the extraneous results that appeared within the individual trials, as opposed to the one large trial that still left the possibility of null results within it.

Our statement from above is proven within our experience of running the code one hundred separate tries as it exposed the reality of getting extraneous results that didn’t back our overall average test result.

Despite the fact that the Python random number generator did produce a result that appeared as random, we do not believe it is an accurate assumption to conclude it to be a safe random number generator as the generator is using an algorithm to produce its random numbers. Thus, if a hacker were to know the algorithm the numbers would become projectable.

2)

After running 1000 separate trials and comparing the results of the Python random number generator trying to guess a random number and guessing that random number by counting from 1 up to that number, the conclusion as to which method was better was ambiguous. When we ran the 1000 trials different times, we found that both the methods were close to each other in steps, but sometimes random method was better, and sometimes the manual method was better as can be seen from the screenshot of the output here.



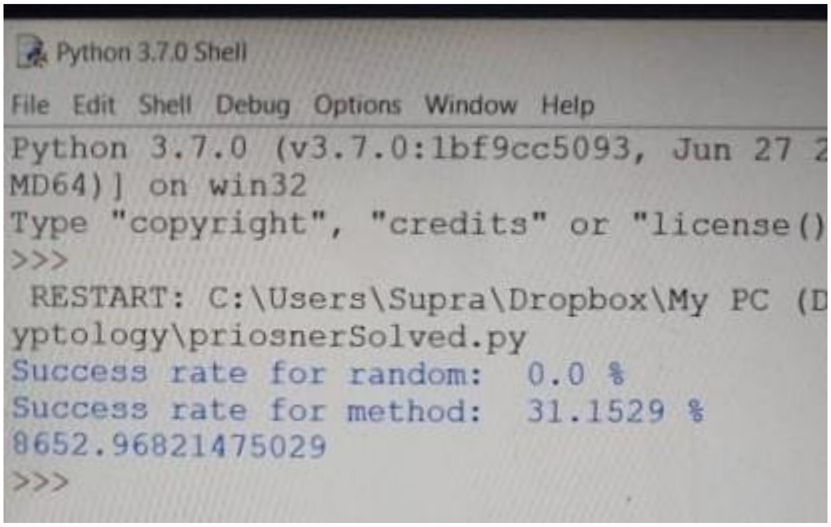
```
Random guess was better  519  times.
Manual increment method was better  480  times.

>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (DESKTOP-R012JMH)\Desktop\Fall 2021\Cryptology\Problem 2 repetition allowed.py

Random guess was better  519  times.
Manual increment method was better  480  times.

>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (DESKTOP-R012JMH)\Desktop\Fall 2021\Cryptology\Problem 2 repetition allowed.py

Random guess was better  499  times.
Manual increment method was better  499  times.

>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (DESKTOP-R012JMH)\Desktop\Fall 2021\Cryptology\Problem 2 repetition allowed.py

Random guess was better  518  times.
Manual increment method was better  482  times.

>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (DESKTOP-R012JMH)\Desktop\Fall 2021\Cryptology\Problem 2 repetition allowed.py

Random guess was better  482  times.
Manual increment method was better  516  times.

>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (DESKTOP-R012JMH)\Desktop\Fall 2021\Cryptology\Problem 2 repetition allowed.py

Random guess was better  489  times.
Manual increment method was better  510  times.

>>> |
```

When running this experiment, it was crucial to use the same number in parts B and C in each independent trial as the random number being used would be considered the “controlled variable” in the experiment and when a controlled variable is adjusted within an experiment you skew the ability to accurately conclude the cause and effect of what causes a specific result.

When we executed the program different times, the preferred method based on the lower number of steps required to guess the number alternated between the manual increment and the random method. While both method might look equivalent, the random guess method could be better than the manual increment method. For a very large range, manual increment can take a lot of steps if the number is large. Also, the random number generator of python is not truly random, i.e. both the number selected at the beginning and the random choices we made for Part C are not truly random; because of this, there could be a pattern in the algorithm that programmers can exploit to make the guess correctly in fewer steps using the random choice.

3)

After having run the code for the “100 prisoner problem” one million times for both the part A and B cases we concluded that within the trials the prisoners never made it out alive using the “part A” strategy (0.0%), while within our experiment using the “part B” strategy the prisoners were able to all find their number and make it out alive around 30 – 32% of the time.



```
Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2
MD64)] on win32
Type "copyright", "credits" or "license()
>>>
 RESTART: C:\Users\Supra\Dropbox\My PC (D
yptology\priosnerSolved.py
Success rate for random:  0.0 %
Success rate for method:  31.1529 %
8652.96821475029
>>>
```

Here in this experiment it was crucial to perform steps A and B under the same setting because without the use of the same numbers being set in each drawer for the independent experiments (part A and B) you would be affecting the “controlled variable” in the experiment and when a controlled variable is adjusted within an experiment this can skew your ability to accurately conclude the cause and effect of why a specific result was produced.

Thus, we concluded that with “part A” having a 0% success rate and “part B” having roughly a 30% success rate, we conclude it is more efficient to use the strategy described in “part B” as the prisoners actually had successful trials. From this experiment we do not believe that the results our answer is based on is a “mere coincidence” as the use of the strategy being utilized in “part B” allowed for the prisoners to follow a pattern rather than simply working with a random guess that had no true structure behind it.

4) Decrypted Text:

To be or not to be that is the question whether it is nobler in the mind to suffer the slings and arrows of outrageous fortune or to take arms against a sea of troubles and by opposing end them to die to sleep no more and by asleep to say we end the heartache and the thousand natural shocks that flesh is heir to it is a consummation devoutly to be wished to die to sleep to sleep per chance to dream ay there is the rub for in that sleep of death what dreams may come when we have shuffled off this mortal coil must give us pause there is the respect that makes calamity of so long life for who would bear the whips and scorns of time the oppressors wrong the pround mans contumely the pangs of despised love the laws delay the insolence of office and the spurns that patient merit of the unworthy takes when he himself might his quietus make with a bare bodkin who would fardels bear to grunt and sweat under a weary life but that the dread of something after death the undiscovered country from those bourn no traveler returns puzzles the will and makes us rather bear those ills we have than fly to others that we know not of thus conscience does make cowards and thus the native hue of resolution is over with the pale cast of thought and enterprises of great pitch and moment with this regard their currents turn awry and lose the name of action soft you now the fair Ophelia nymph in thy orisons be all my sins remembered.