Cryptography Assignment 3: Passwords

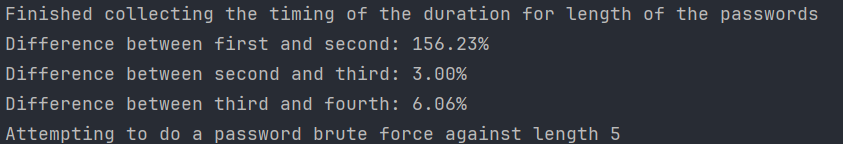
By Nishaal Naseer

[S2100555@students.villacollege.edu.mv](mailto:S2100555@students.villacollege.edu.mv)

SetA:

The program attempts to do a side channel(time) attack on the password. A set password of increasing length is checked n number of times. The timings are saved.

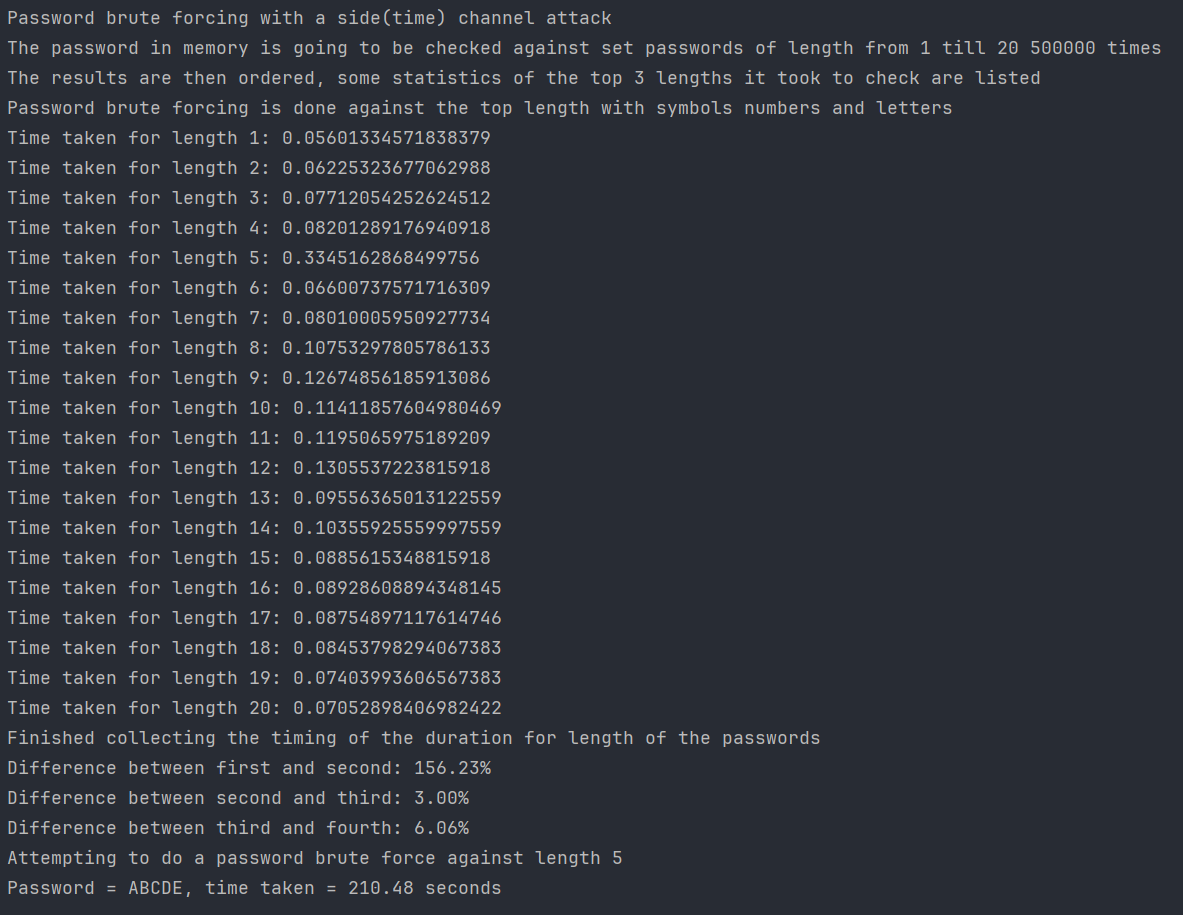
When finished they are sorted and some statistics of the first 4 are printed for the user to see, so the user can I have an idea of the attacks reasoning.



During the above part it was noted that a string of length 5 took noticeably more time than other lengths, hence its length 5 and only 5 would be brute forced.

All possible strings of n length can are achieved by saving the indexes of the characters inside a list, and at each iteration a 1 is added to the right most digit and 1 is carried over to the left if need be. Essentially, I have treated this list both as a list and as a number. Like Integers and Floats this is also susceptible to an overflow, so the length n should not be less that what it should be. The iterations are set by m \*\* n where m is the number of characters in a string, in this case its 95.

Complete output:



SetB:

A password is set in plain text in memory, values are set by iterating from 1 till 1 billion, encoding them and decoding, and checking if the value is valid. An output is printed for each 10,000 to keep the user updated on progress.

