Assembly and Machine Language

Final Project

Your task is to **crack two executables** and retrieve a quote by Mahatma Gandhi. The quote is **password protected**. You can accomplish this task using the tools and methods presented in the class plus a little bit of creativity. You will receive **80 percent** of the score by cracking the first executable named **crackme_xxxxxxx** where **xxxxxxx** is your student ID and the remaining **20 percent** by cracking the file **crackme_xxxxxxx_optimized**.

- Each student must crack his/her own files marked with their student number. The difference between the two executables **crackme_xxxxxxx** and **crackme_xxxxxxx_optimized** is that the latter is compiled with -Ofast option. Download the executables from the course website or the Telegram channel.
- You must create a cracked version of your executables using patching techniques. The cracked version must allow the user to see the quote without the need to know the correct password.
- Executables differ for each student, and so does the quote.
- You must present how you cracked the executable **in person** to the TAs. They will ask you questions to assess your grip on the project. Further details about the deadline and how to deliver the project will be posted on the Telegram channel.

Positive score:

Create a patch file using the **bsdiff** command. A patch file contains information about the difference between the two versions of a file. Using a patch file, you can update a file just by updating the parts that are changed in the recent update. The patch file can be later applied to an old file using the **bspatch** command. You can find out more about **patch file**, **bsdiff**, and **bspatch** commands here:

- https://en.wikipedia.org/wiki/Patch_(Unix)
- http://manpages.ubuntu.com/manpages/bionic/man1/bsdiff.1.html
- http://manpages.ubuntu.com/manpages/bionic/man1/bspatch.1.html