**EECS 444 HOMEWORK 3 LAB – PART (1)**

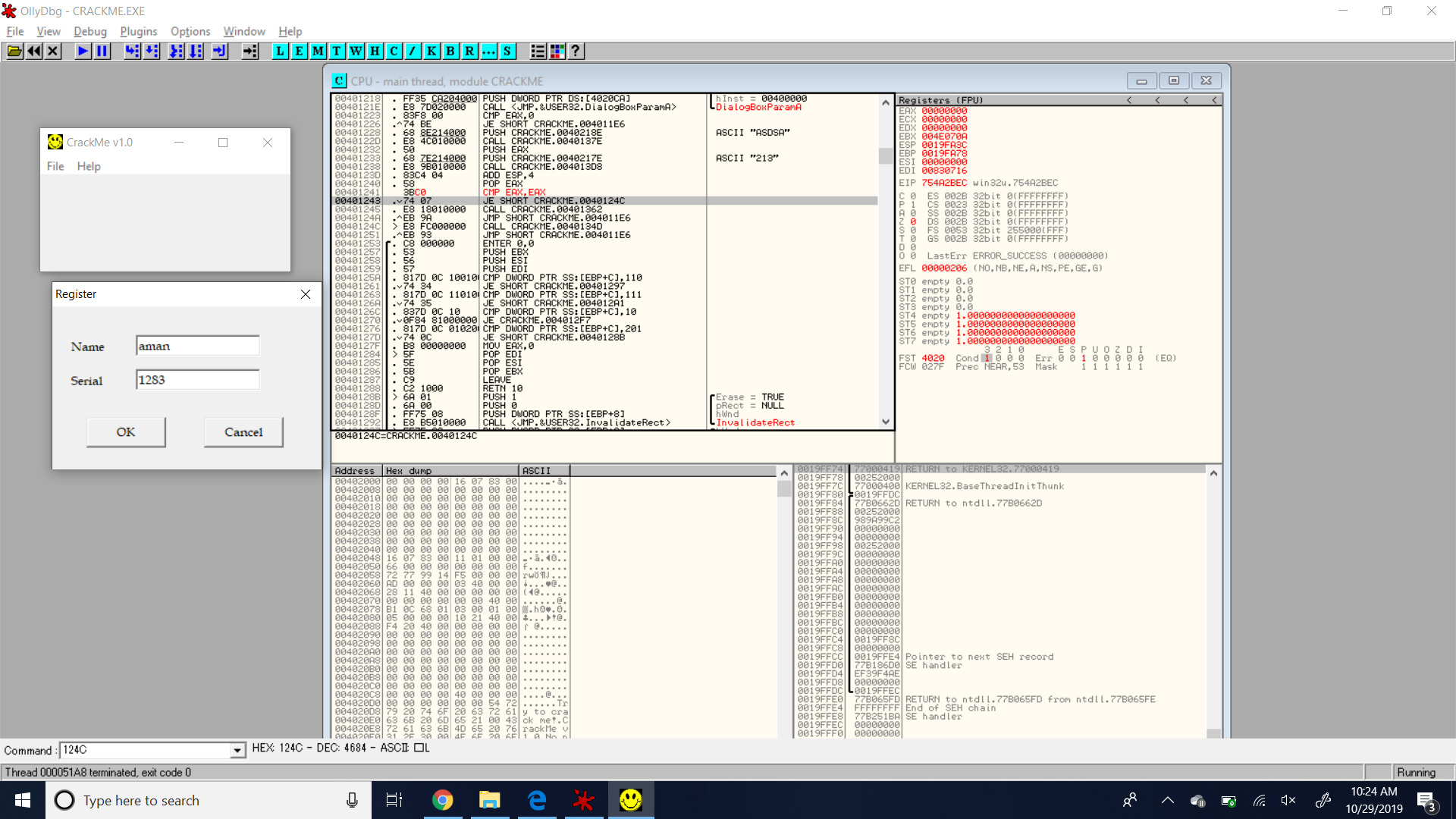
**AMAN ANAND**

**STUDENT ID:3473516**

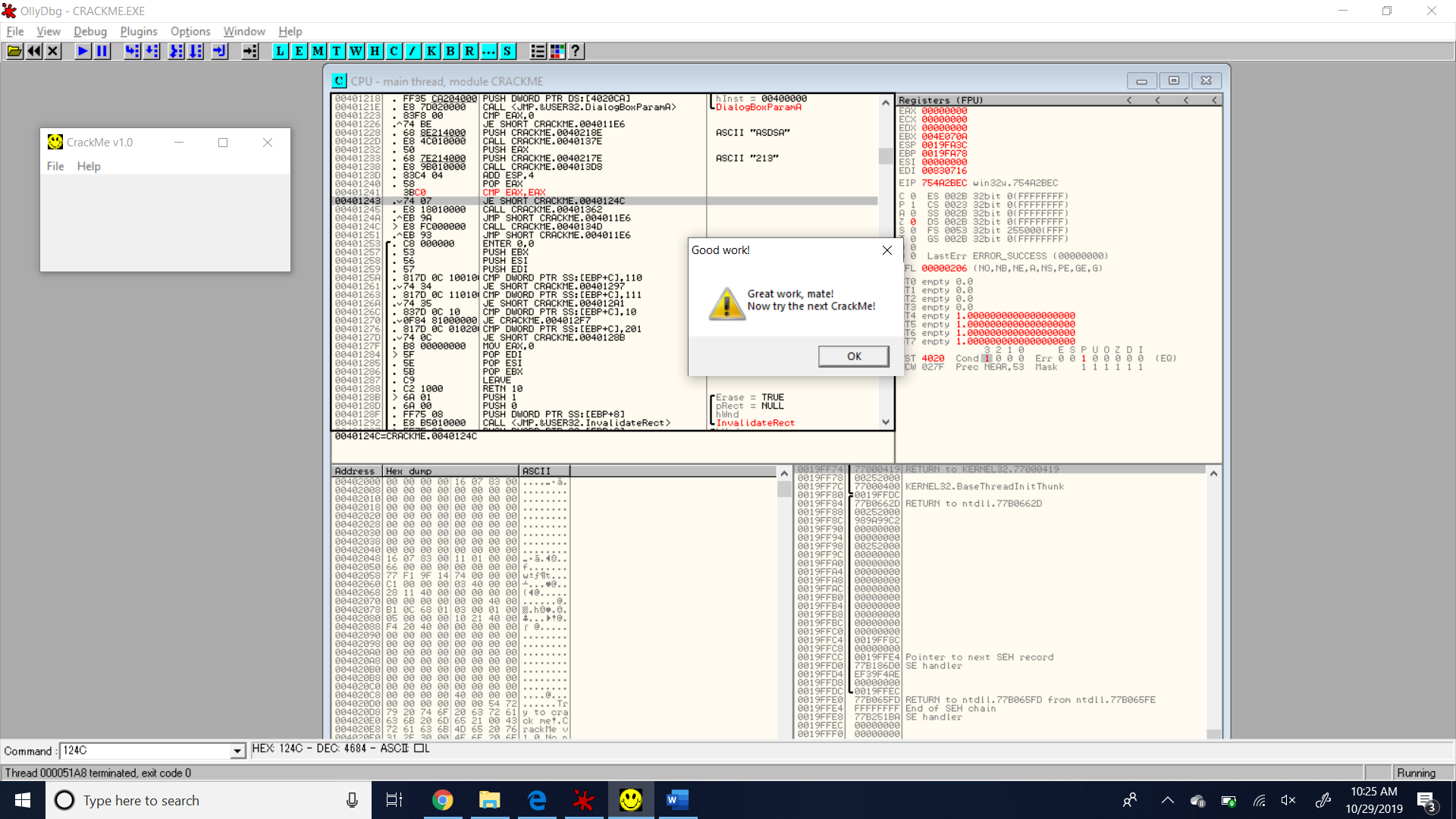
**Question 1:**

The first part of the homework is to successfully get into CRACKME.exe with the help of OllyDbg by changing something in the machine level code.

After using OllyDbg, the code is observed and it is noted at a point where a comparison is made between EAX and EBX and based on which the final result popup is displayed, by changing this EBX to EAX, we can compare eax with itself i.e. cmp EAX, EAX will always give us an equal result and will always crack the file regardless of what input and code we enter for it. This is demonstrated in the screenshots below,



AFTER MAKING THAT CHANGE, FOR NAME AND SERIAL :

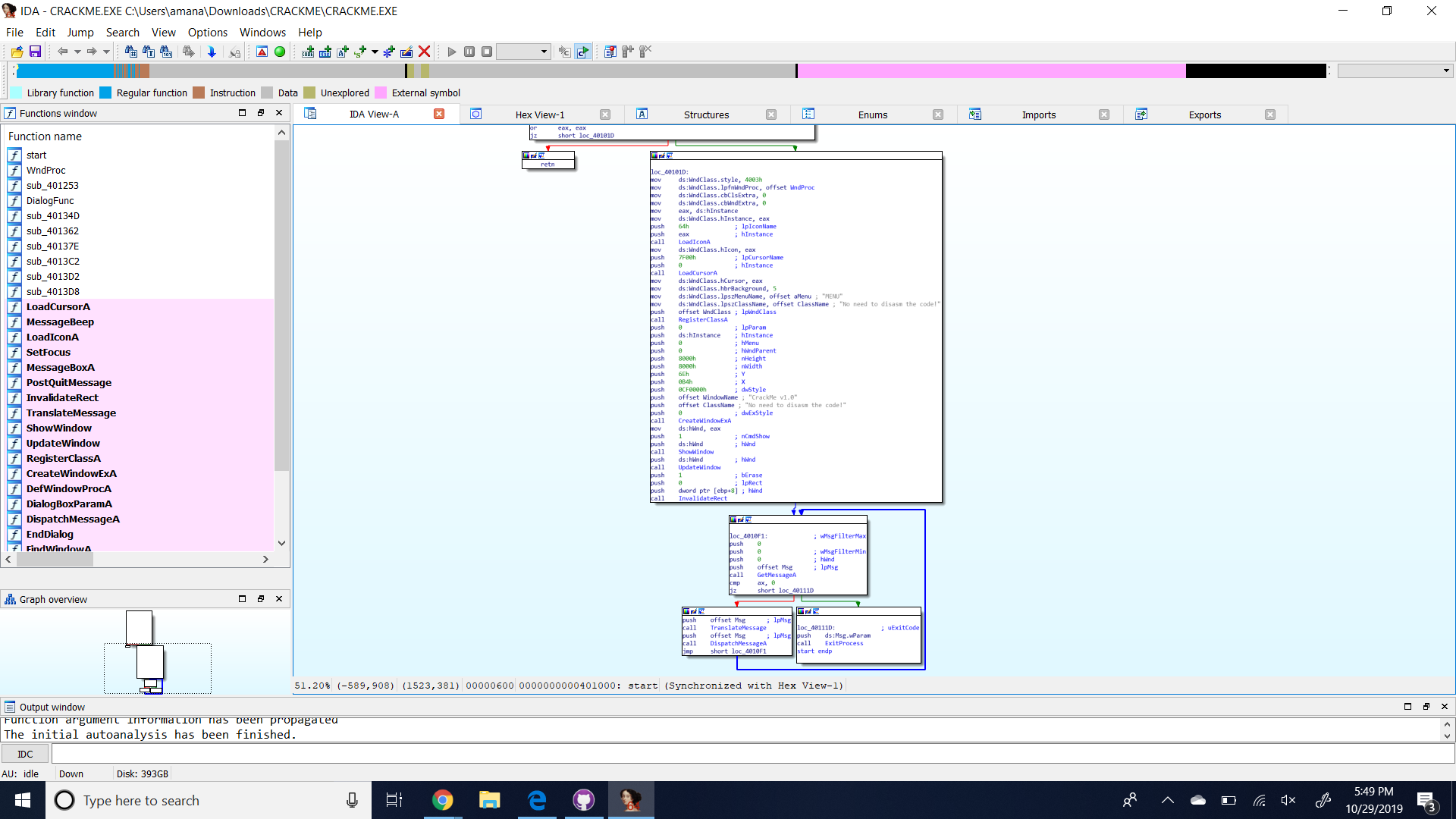


THE EXECUTABLE FILE WITH THIS MODIFICATION IS CREATED AND UPLOADED ON GITHUB, TITLED ‘CRACKED!’ WHICH DEMONSTRATES HOW IT WORKS FOR ANY INPUTS. THIS IS THE SOLUTION FOR UPLOADING THE CRACKED BINARY FILE IN AN EXE MANNER.

**Question 2:**

Now for the second question we need to understand the code with the help of OlyDbg and IDA to fully go through the functionality and hence find the correct serial sequence that corresponds to the name entered.

Analysis using IDA :



The functionality of the code is understood as the following, it performs the following steps sequentially:

1. Take the input name and convert it to the uppercase letters.
2. Find the ascii values for each uppercase letter of the input sequence.
3. Add all the ASCII values for the individual letters.
4. XOR the sum of ASCII values with 5678h.
5. Next, again XOR the previous result again with 1234h.
6. Finally convert the result into the decimal value.
7. This decimal value is the corresponding code for the input name.

For the name: aman

Steps:

1. Uppercase > AMAN
2. ASCII values for each letter > 41 4D 41 4E
3. Add all the above ascii values > 11D
4. The result after the XOR with 5678h > 5765
5. Next, XOR operation with 1234h > 4551
6. Finally, the result is converted into decimal > 17745
7. Giving input as 17745, we successfully crack into the exe file.

For the name: shifu

Steps:

1. Uppercase > SHIFU
2. ASCII values for each letter > 53 48 49 46 55
3. Add all the above ascii values > 17F
4. The result after the XOR with 5678h > 5707
5. Next, XOR operation with 1234h > 4533
6. Finally, the result is converted into decimal > 17715
7. Giving input as 17715, we successfully crack into the exe file.

For the name: yujie

Steps:

1. Uppercase > YUJIE
2. ASCII values for each letter > 59 55 4A 49 45
3. Add all the above ascii values > 186
4. The result after the XOR with 5678h > 57FE
5. Next, XOR operation with 1234h > 45CA
6. Finally, the result is converted into decimal > 17866
7. Giving input as 17866, we successfully crack into the exe file.

For the name: yiming

Steps:

1. Uppercase > YIMING
2. ASCII values for each letter > 59 49 4D 49 4E 47
3. Add all the above ascii values > 1CD
4. The result after the XOR with 5678h > 57B5
5. Next, XOR operation with 1234h > 4581
6. Finally, the result is converted into decimal > 17793
7. Giving input as 17793, we successfully crack into the exe file.

|  |  |
| --- | --- |
| NAME | SERIAL |
| aman | 17745 |
| shifu | 17715 |
| yujie | 17866 |
| yiming | 17793 |