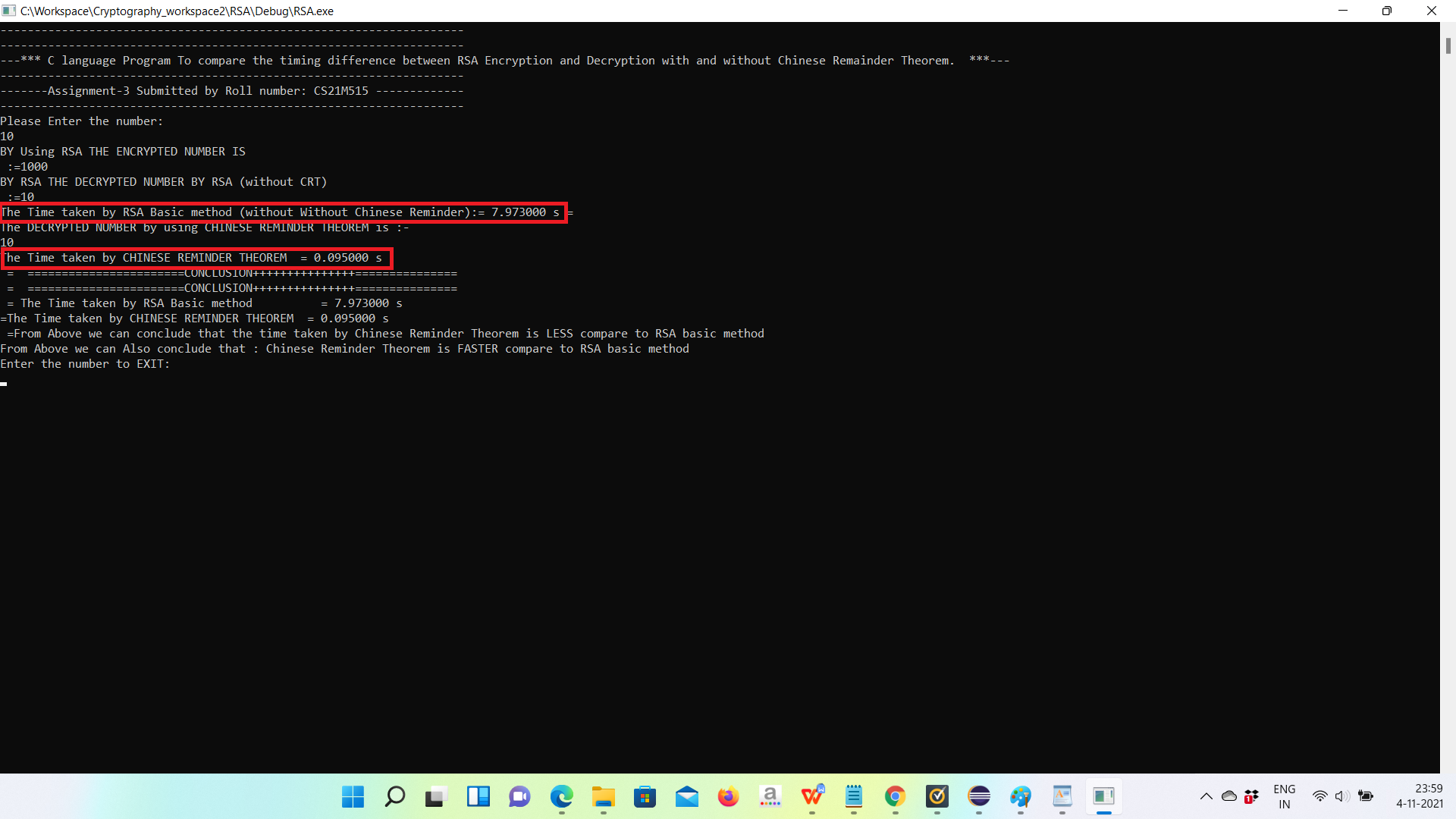
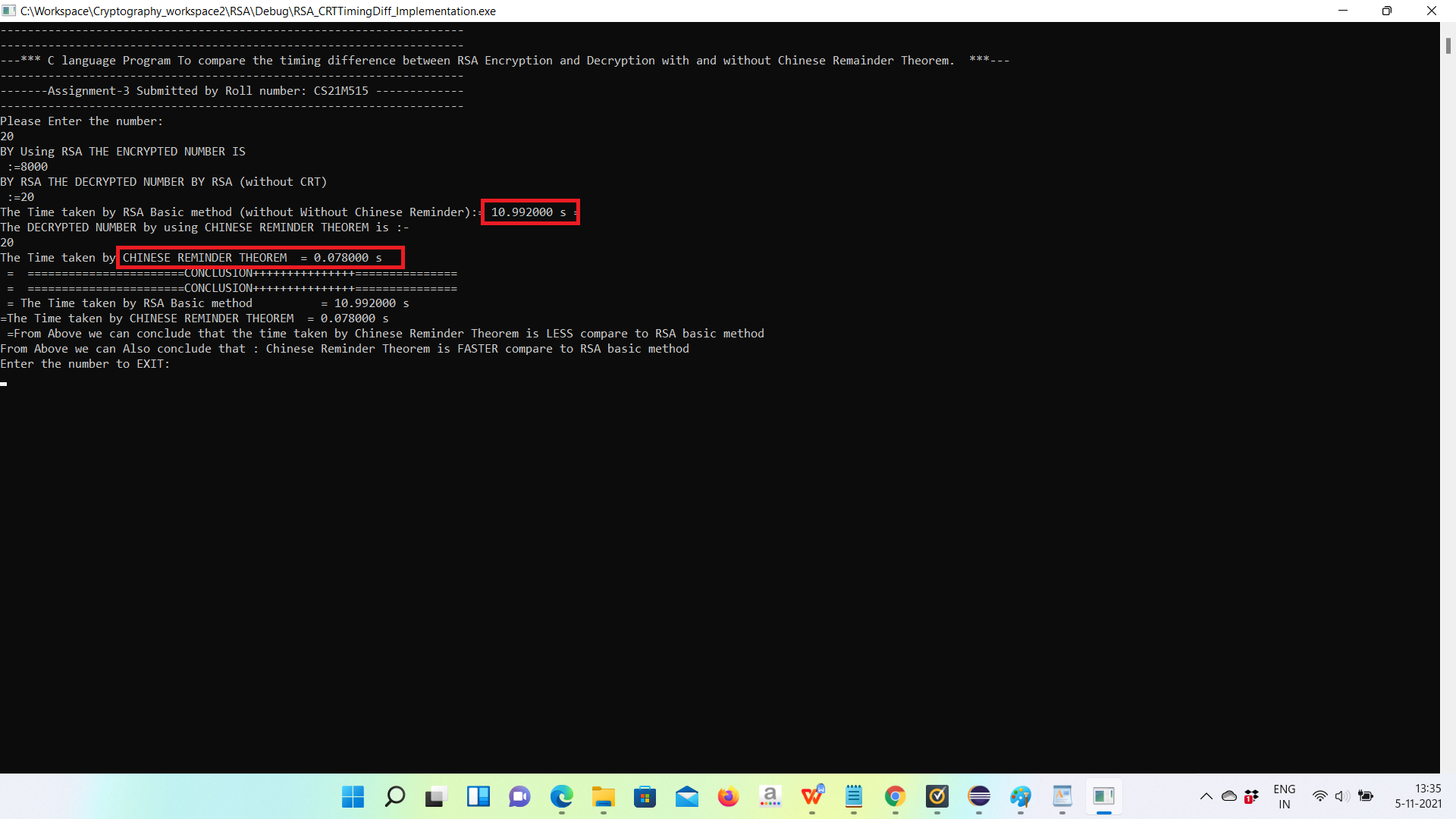
**Compare the timing difference between RSA Encryption and Decryption with and without Chinese Remainder Theorem.**

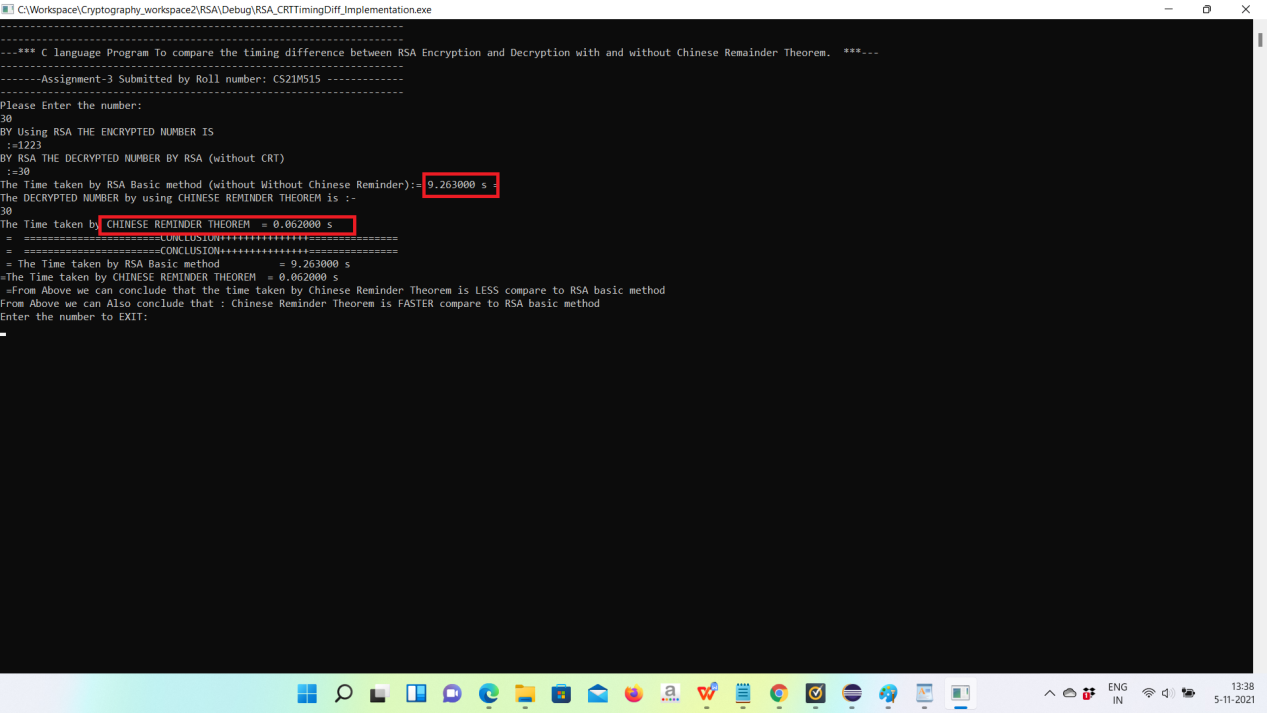
Below is the Screenshots of the program executions :-

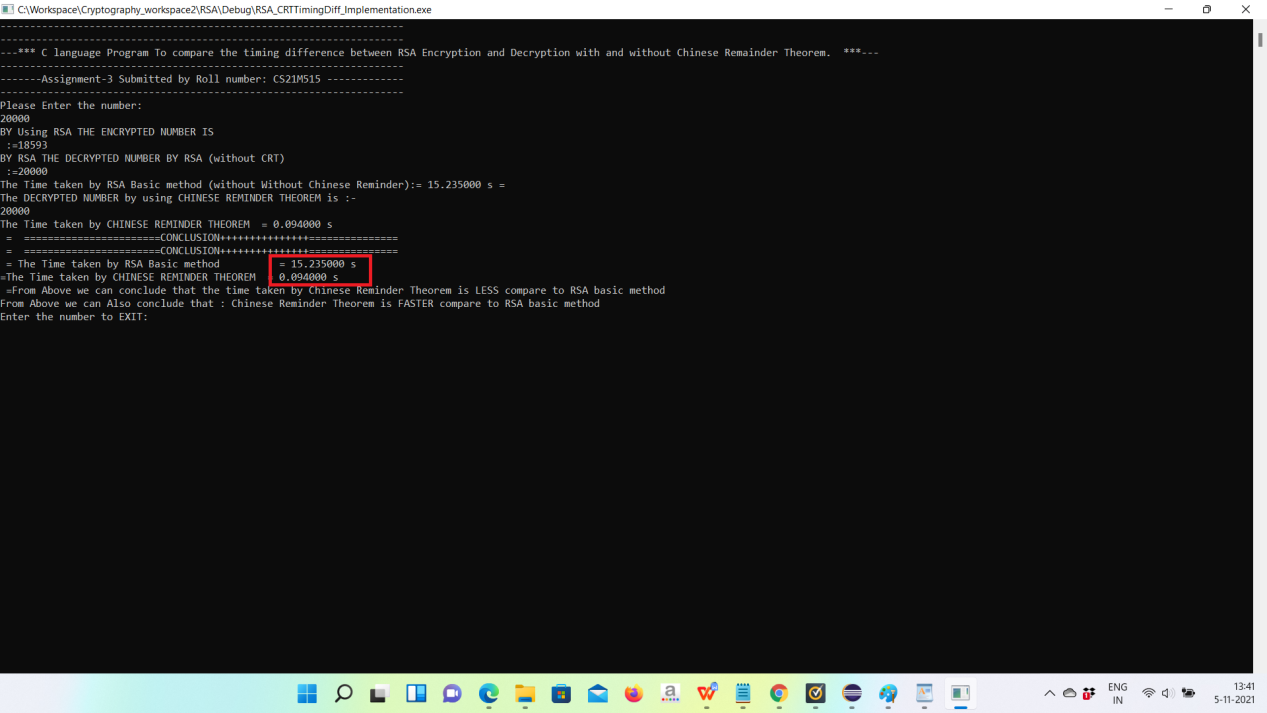
The main program file is written in C language.

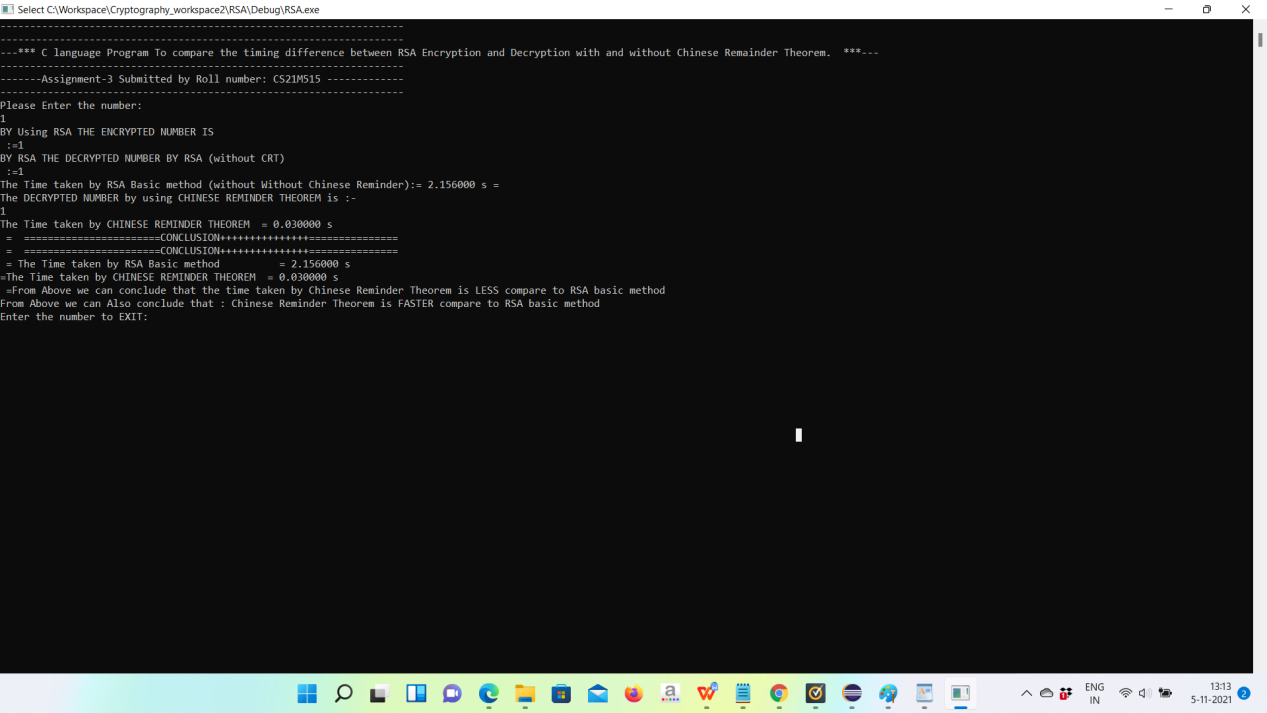
Name of C Program file for timing difference is - [RSA\_CRTTimingDiff\_Implementation.c](https://github.com/AyubShaikhVahidoddin/CryptographicsBasic-Assignment_3_RSA/blob/main/RSA_Algo_CRT_TimeComplexity/RSA_CRTTimingDiff_Implementation.c" \o "RSA_CRTTimingDiff_Implementation.c)

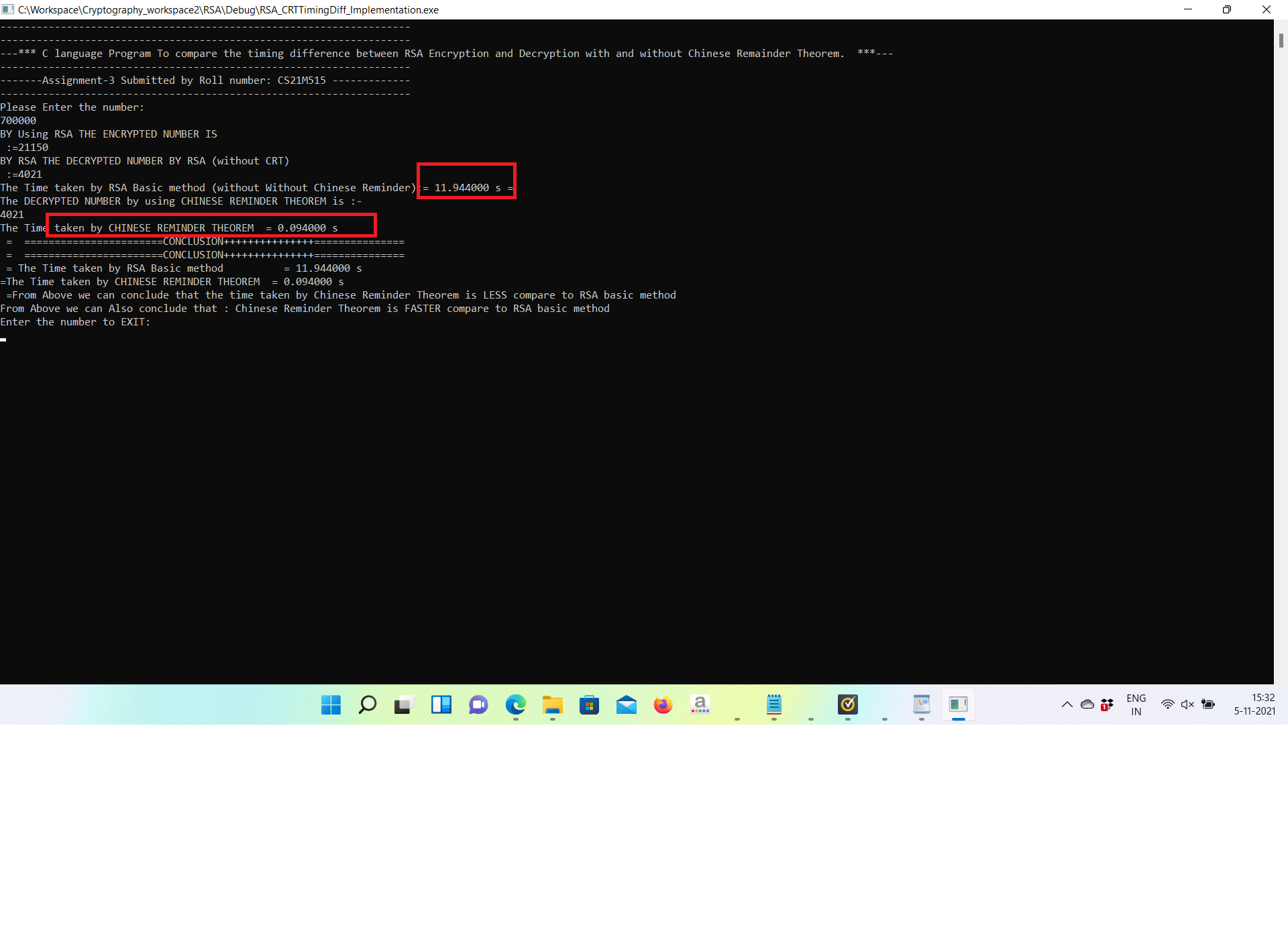












So from above screen shots we see the timing difference between RSA and CRT.

RSA Vs RSA With CRT timing Difference Table

|  |  |  |  |
| --- | --- | --- | --- |
|  | input | RSA(**Time** in **Seconds**) | RSA with Chines Reminder Theorem (**Time** in **Seconds**) |
| 1 | 10 | 7.97 Sec | 0.0957 sec |
| 2 | 20 | 10.99 Sec | 0.0780 Sec |
| 3 | 30 | 1. 26Sec | 0.06 sec |
| 4 | 20000 | 15.235 Sec | 0.094 sec |
| 5 | 100000 | 18.456 Sec | 0.121 Sec |

RSA encryption algorithm is one of the most powerful public key encryption algorithm. The problem with RSA algorithm is that RSA decryption is relatively slow in comparison to RSA encryption. Chinese Remainder Theorem (CRT), a modulo based mathemati- cal theorem, is proposed by researchers as a way to enhance the performance of decryption. CRT minimizes the mathematical computation to large extent, thus improving the speed. CRT is well known for improving RSA’s decryption speed.