COMP311-1: Logic Circuit Design

Fall 2019, Prof. Taigon Song

Project 3. Due: Dec. 19, 9:59am [Total: 210 + 40 points]  
(submission)

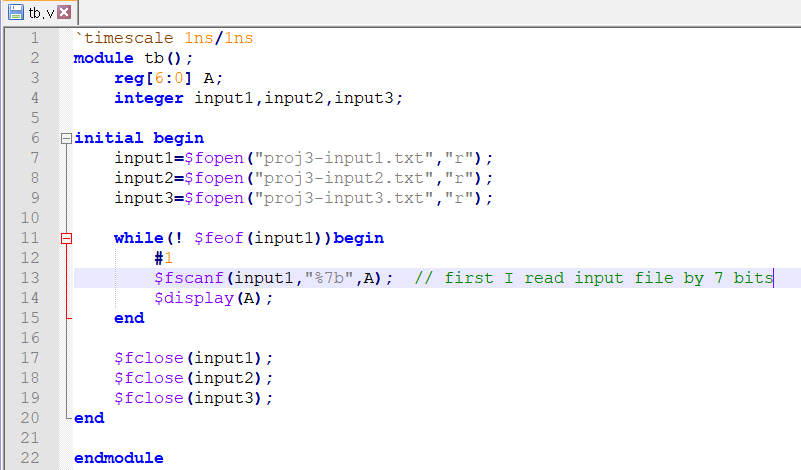
[2017114559]

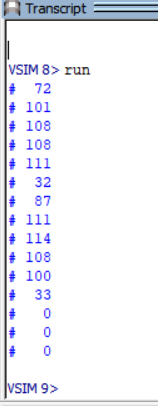
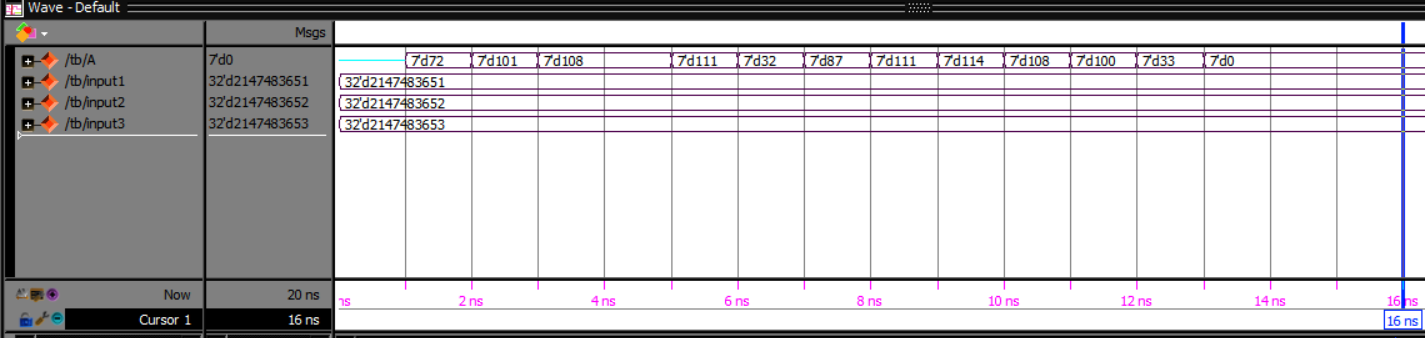
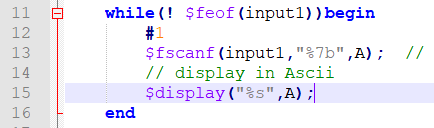
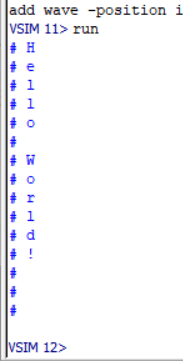
박선우 Park Sun Woo

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Checksheet item | Answer | Points |
| 1. | ascii (part 1) | 72 101 108 108 111 32 … | 10 |
| 2. | tgBASE (part 1) | 19 42 49 49 52 00 … | 10 |
| 3. | oneBig (part 1) | 1942 4949 5200 … | 10 |
| 4. | encrypt (part 1) | 9962 909 10222 … | 10 |
| 5. | DoneBig (part 2) | 1426 2427 503 … | 10 |
| 6. | DtgBase (part 2) | 14 26 24 27 5 3 3 0 … | 10 |
| 7. | Dascii (part 2) | 67 79 77 80 51 49 49 32 … | 10 |
| 8. | decrypted message (part 2) | COMP311 is fun!! | 10 |
| 9. | [Modelsim] ascii (part 1) | Y | 5 |
| 10. | [Modelsim] tgBase (part 1) | Y | 5 |
| 11. | [Modelsim] oneBig (part 1) | Y | 5 |
| 12. | [Modelsim] encrypt (part 1) | Y | 5 |
| 13. | [Modelsim] DoneBig (part 2) | Y | 5 |
| 14. | [Modelsim] DtgBase (part 2) | Y | 5 |
| 15. | [Modelsim] Dascii (part 2) | Y | 5 |
| 16. | [Modelsim] output file (part 2) | Y | 5 |
| 17. | p, q (part 3) | 97 109 | 10 |
| 18. | d (part 3) | 233 | 10 |
| 19. | decrypted message (part 3) |  | 10 |
|  | Well done on your Final Project! Have a safe 2020winter break! | |  |
| 21. | [Modelsim] p, q (part 3) | Y | 20 |
| 22. | [Modelsim] d (part 3) | Y | 20 |
| 23. | [Modelsim] message print | Y | 20 |
| 24 | [Bonus] | 40 | 40 |

**(PART 1)**

**1. ascii (first I did not make array, and use $feof, but I change it later)**



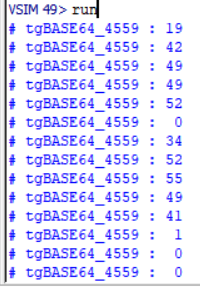
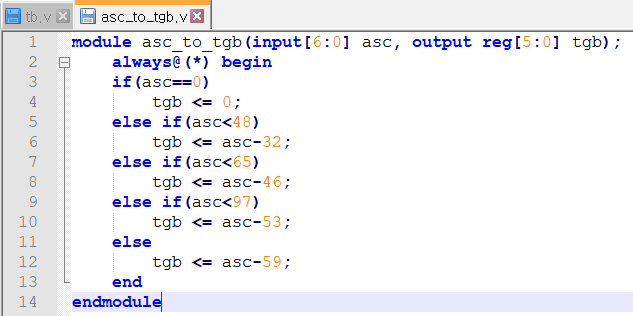
 

I open the input1.txt and read it by 7 bits binary and display it

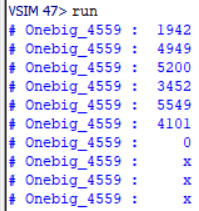
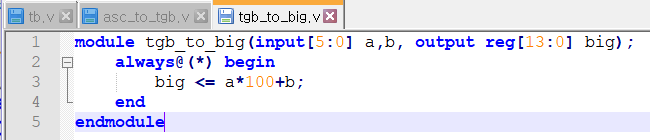
**2. tgBASE64 (PART 1)**

And I convert it by hand with conversion table

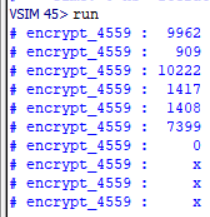
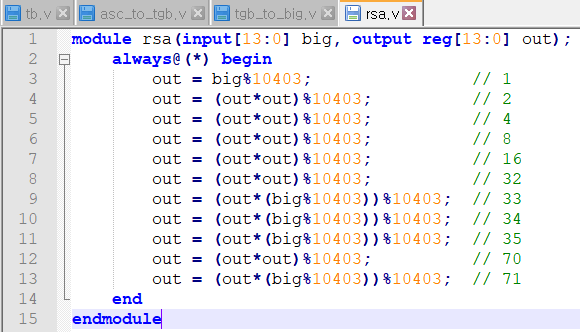
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Decimal | 72 | 101 | 108 | 108 | 111 | 32 | 87 | 111 | 114 | 108 | 100 | 33 | 0 | 0 | 0 |
| Ascii | H | e | l | l | o |  | W | o | r | l | d | ! |  |  |  |
| tgBASE64 | 19 | 42 | 49 | 49 | 52 | 00 | 34 | 52 | 55 | 49 | 41 | 01 |  |  |  |



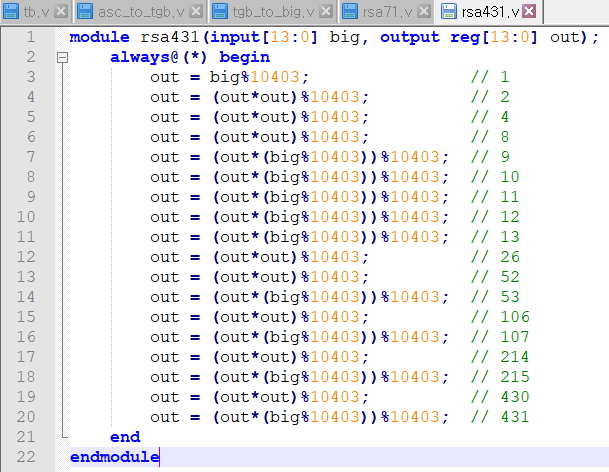
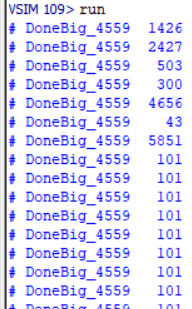
**3. oneBig (PART 1)**



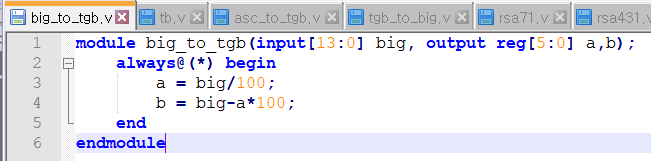
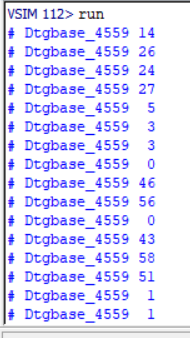
**4. encrypt (PART 1)**



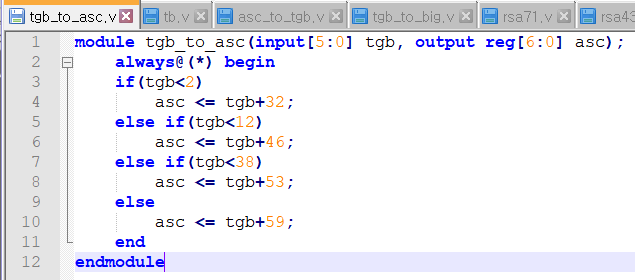
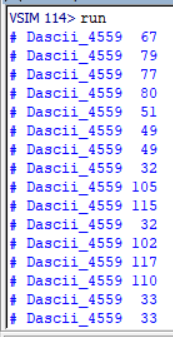
**5. DoneBig (PART 2)**

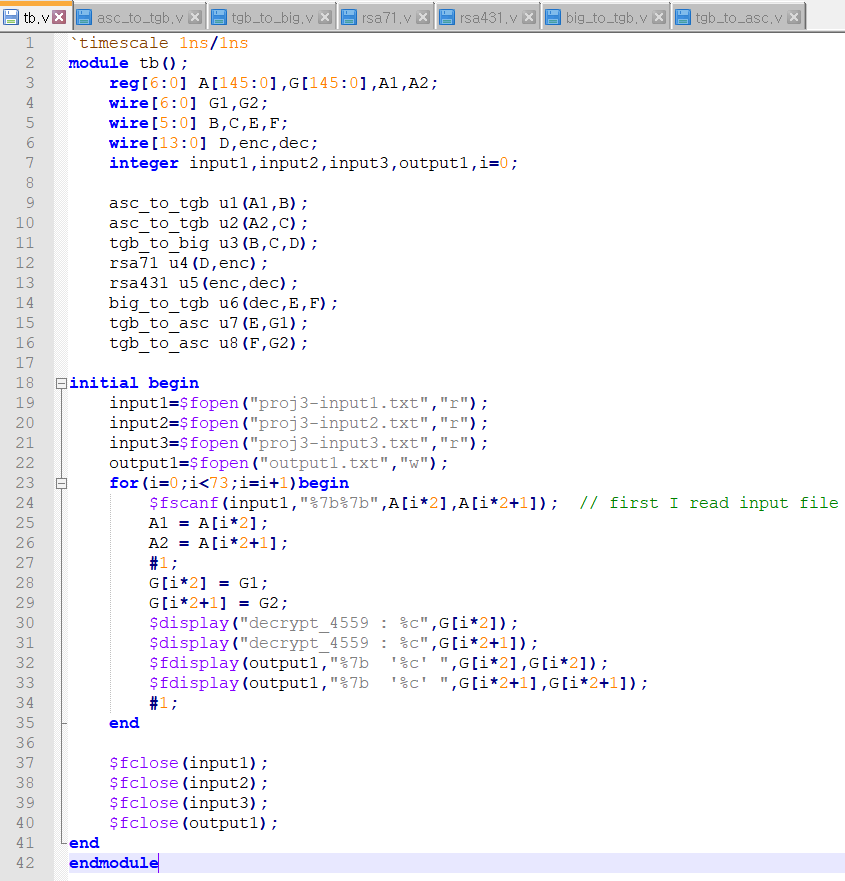
**6. Dtgbase (PART 2)**

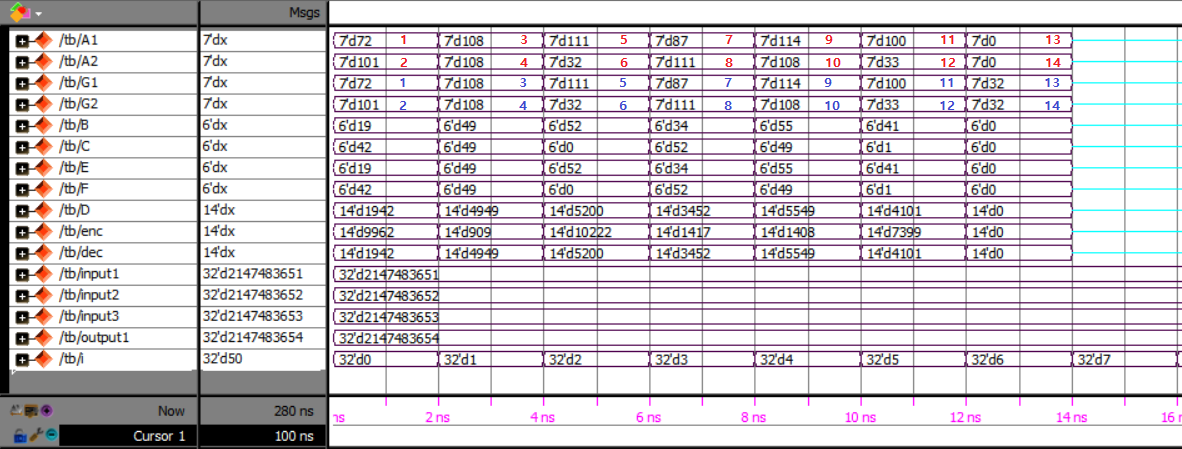
**7. Dascii (PART 2)**

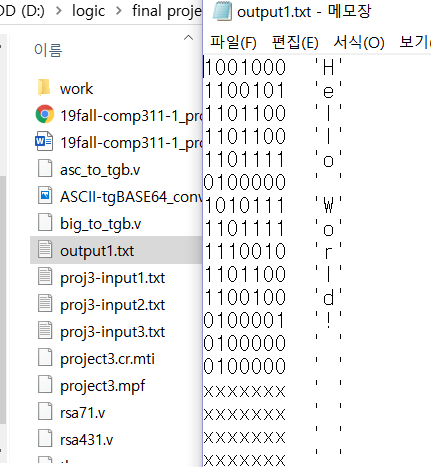
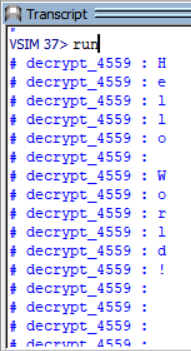
**8. file output result (PART 1)**



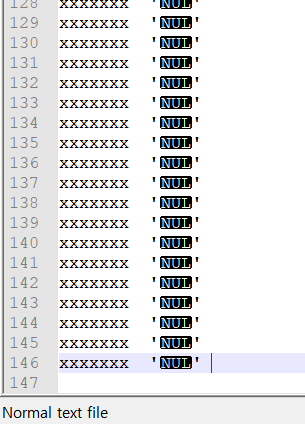
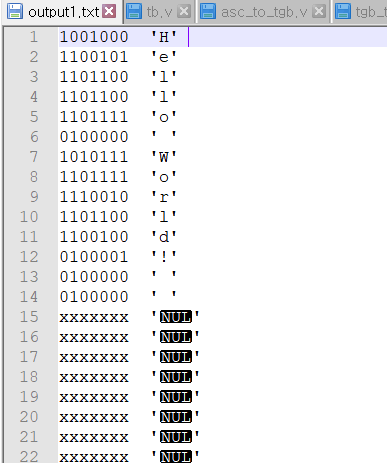
**Waveform result**

****

**Modelsim text result .txt file result**

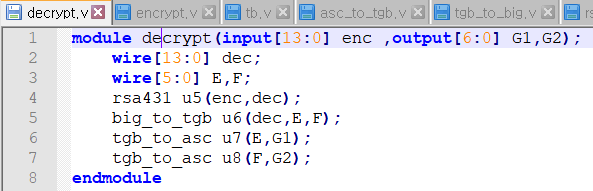
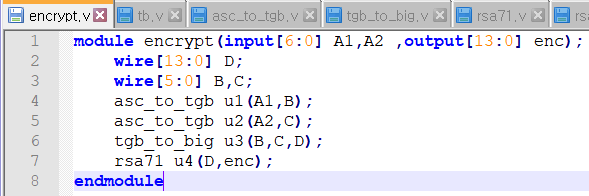
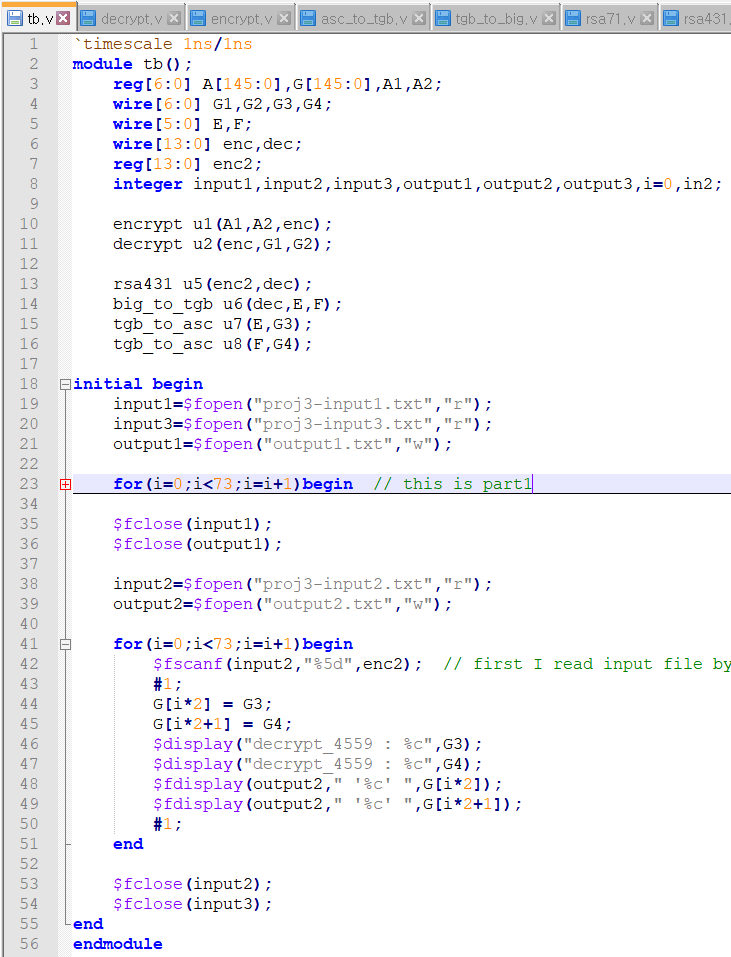


**Notepad++ result (the end line is 146)**

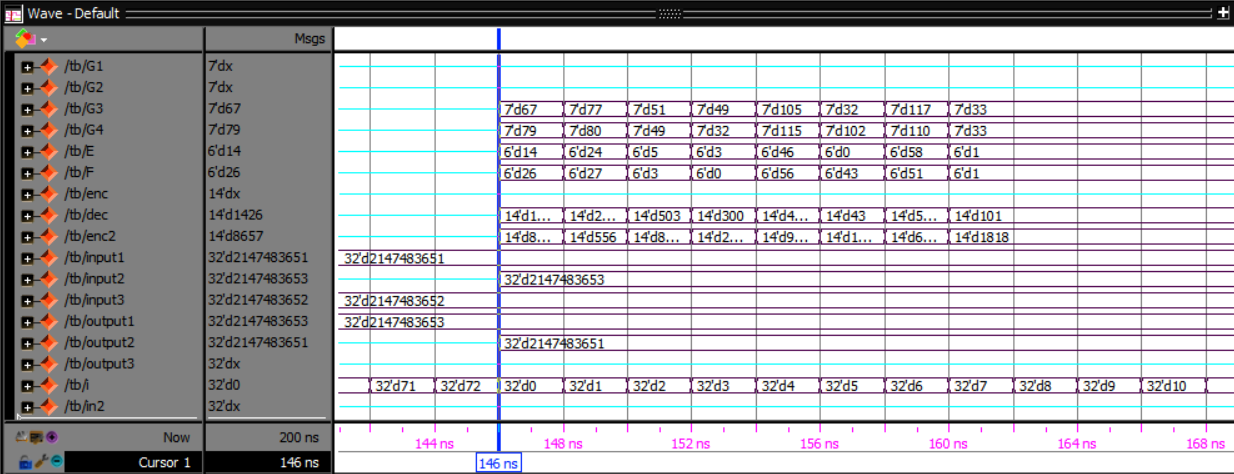


**(PART 2)**

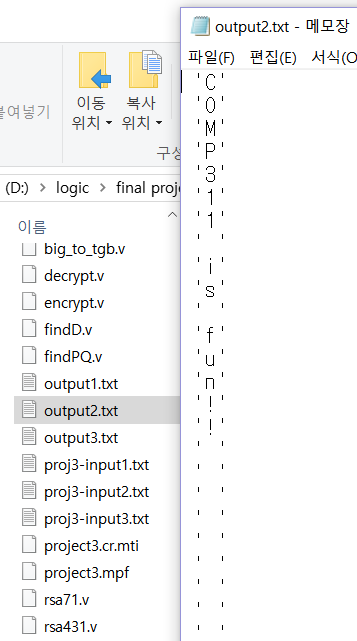
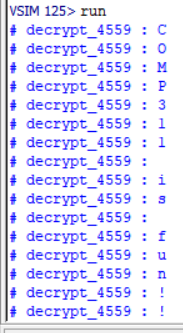
**I make two module encrypt & decrypt**

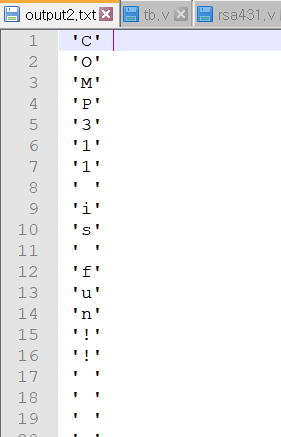
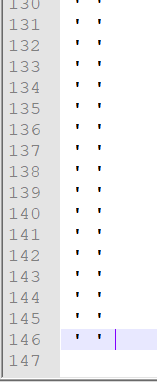
**Waveform result (PART 2)**

****

**Modelsim result .txt file result**

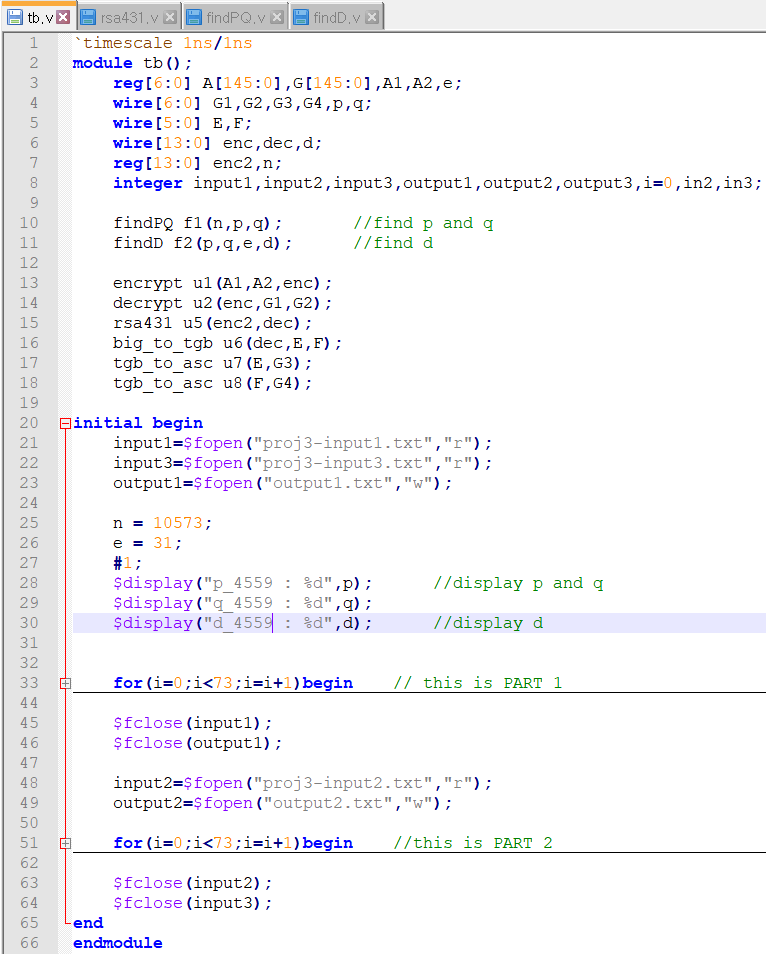


**Notepad++ result**

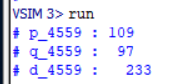
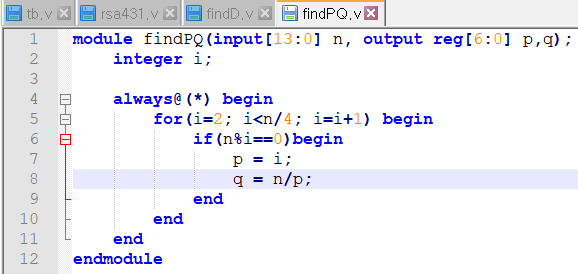
 

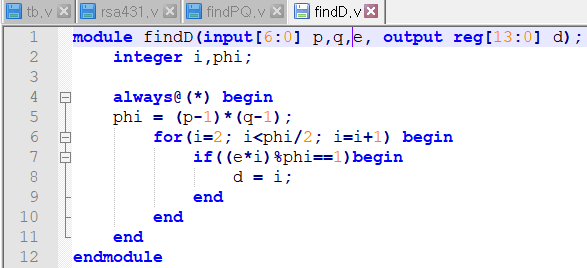
**(PART 3) Find private Key**

**Find P and Q value**

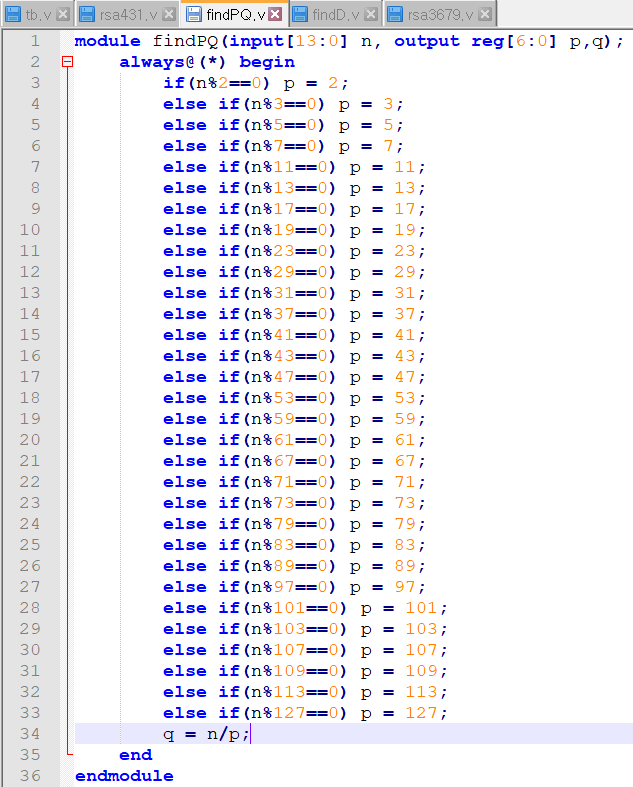
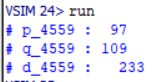


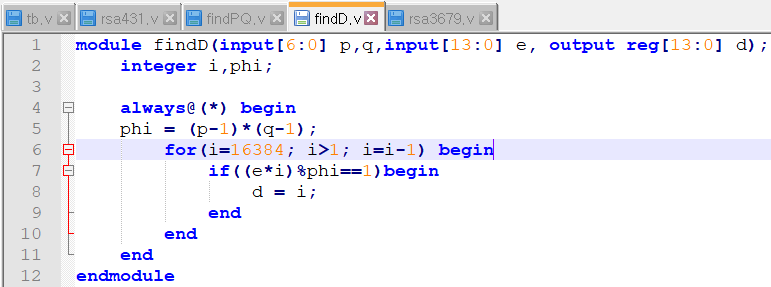
**FindPQ & FindD First ( loop version )**



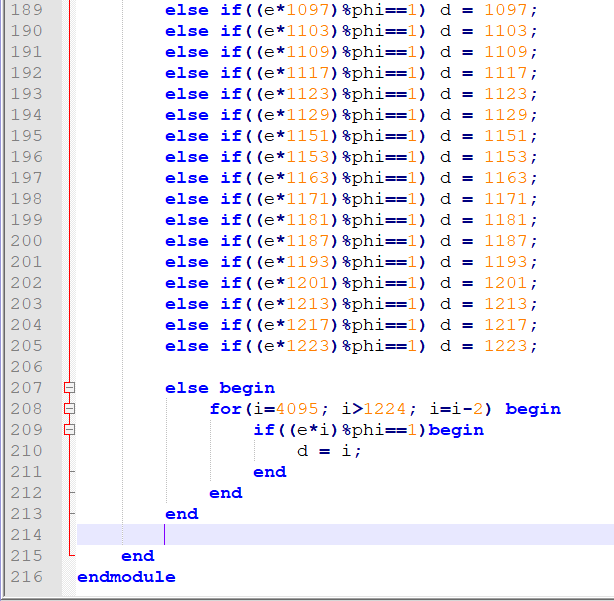
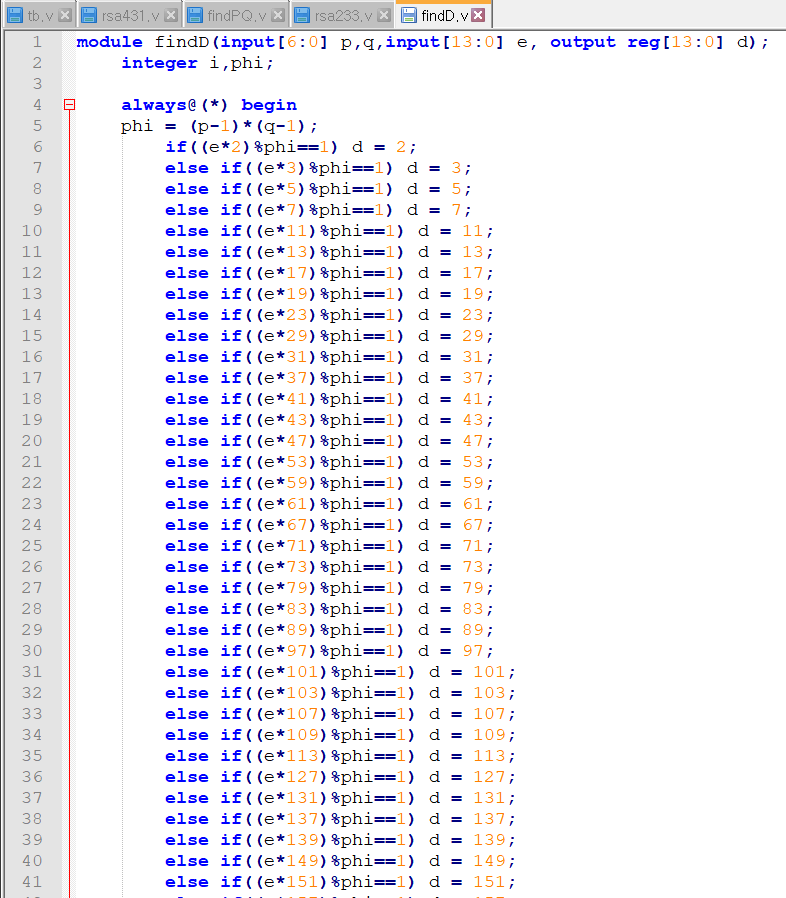
**it`s not synthesisable**

**FindPQ & FindD Final ( NO loop version PQ & synthesisable D )**

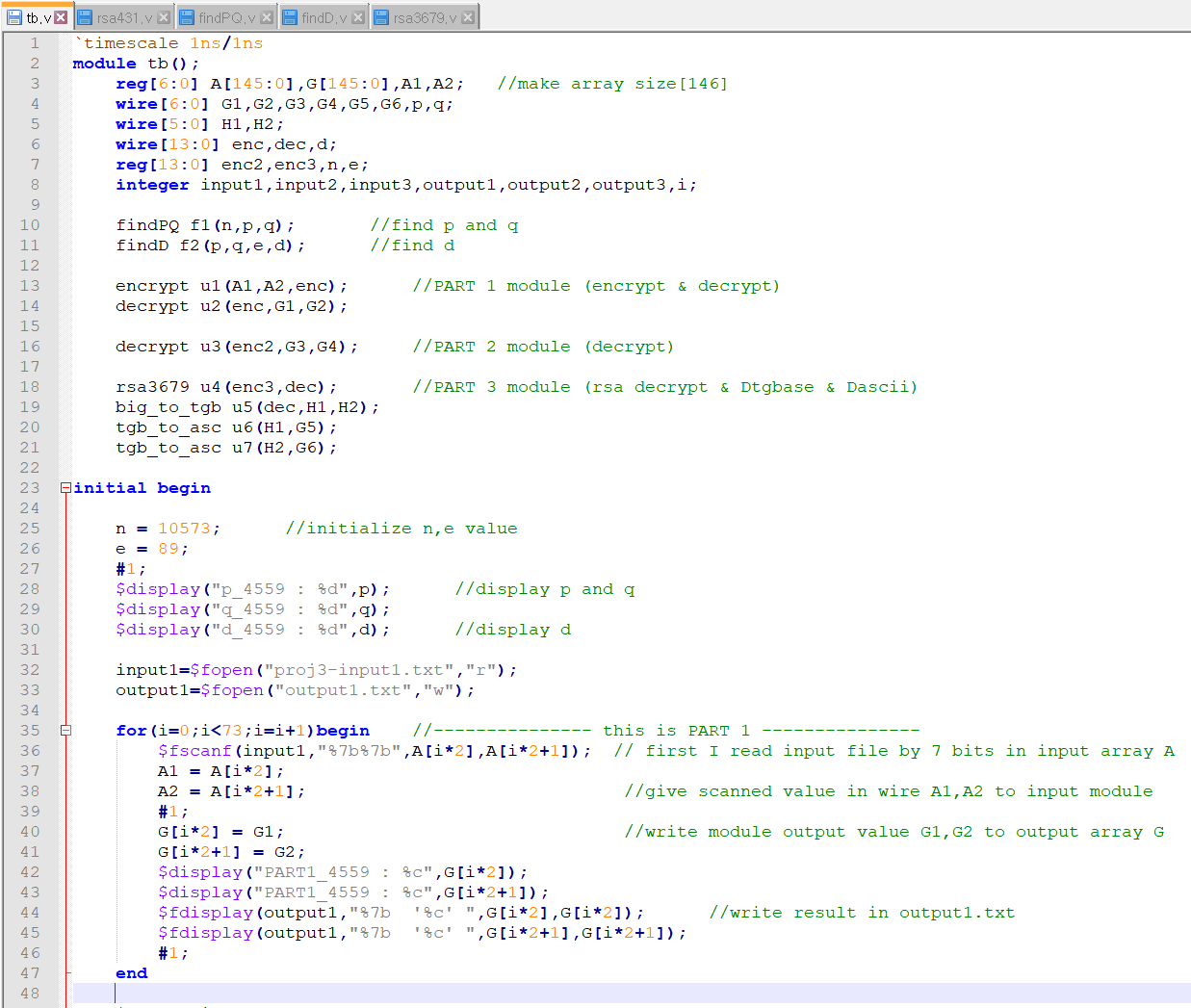
 

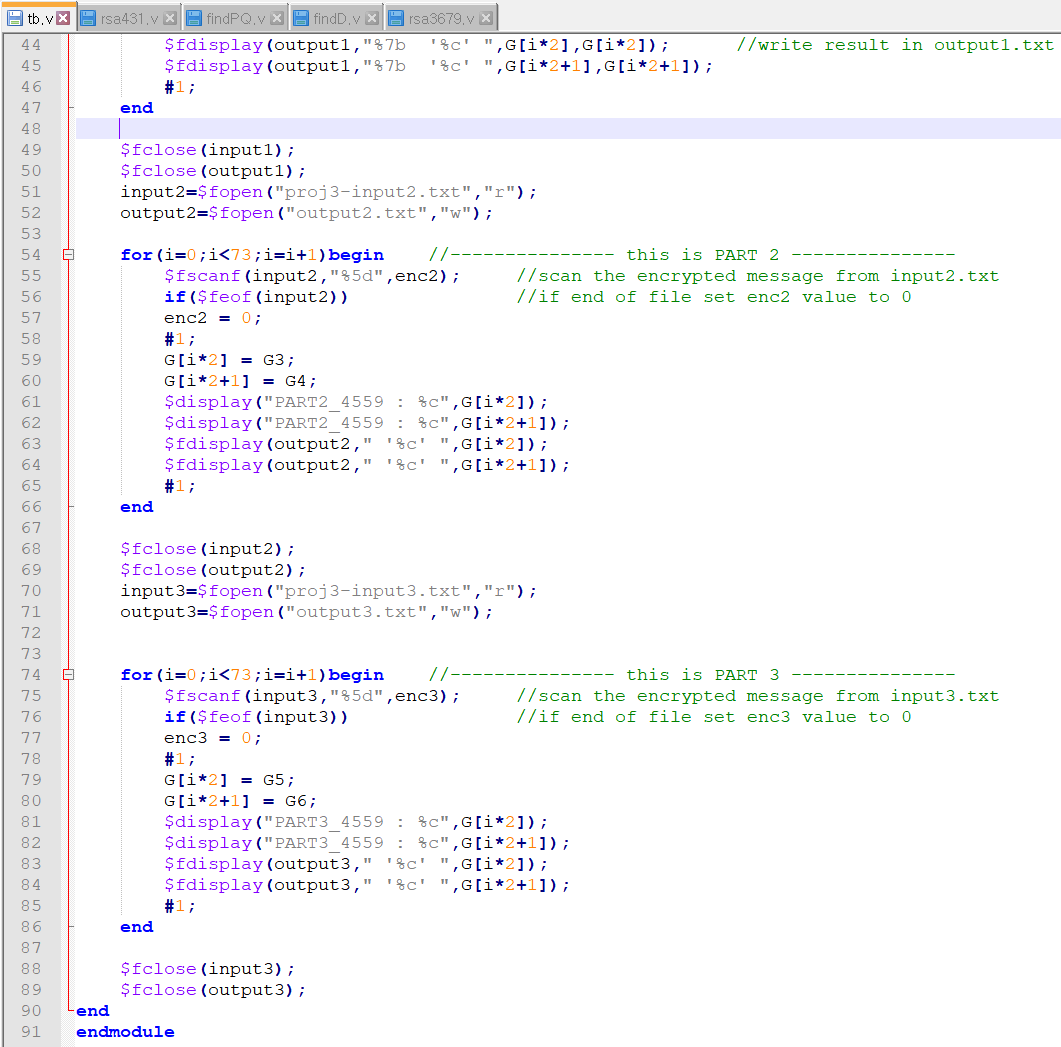


**New version of find.v (use prime number to reduce loop number)**

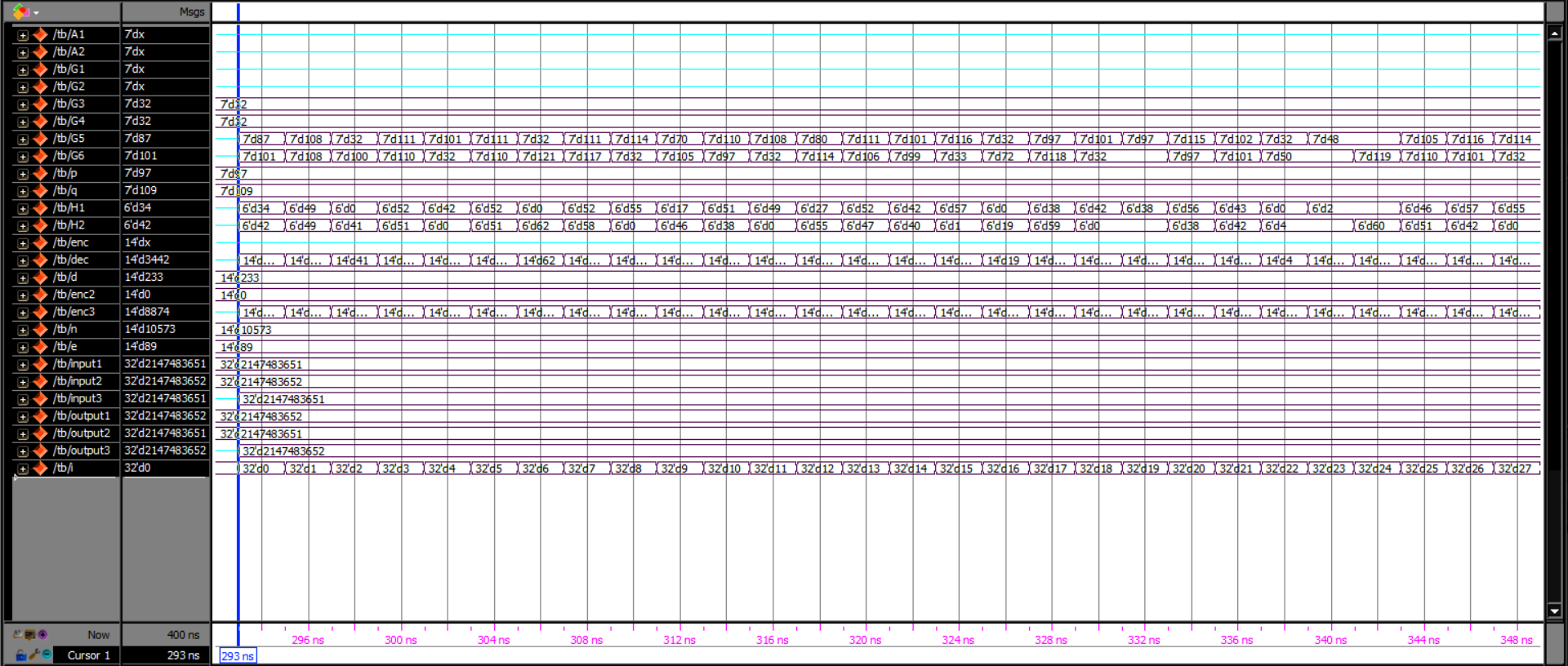


**Final testbench file (rsa3679 -> rsa233)**

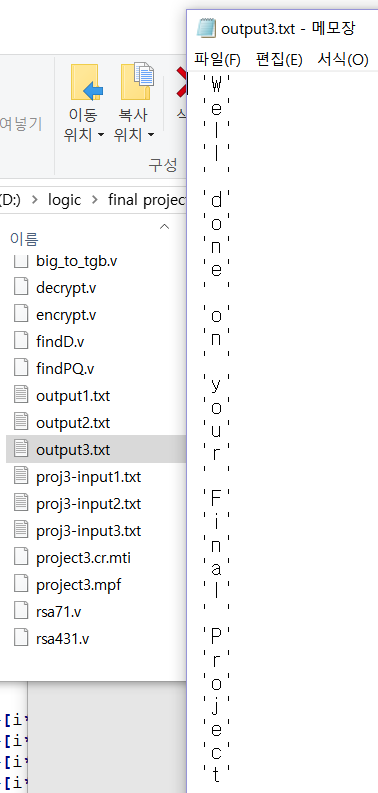
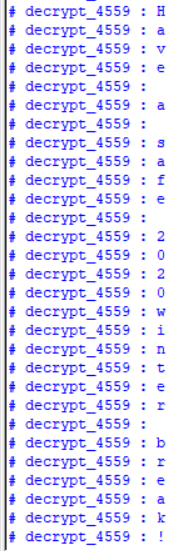
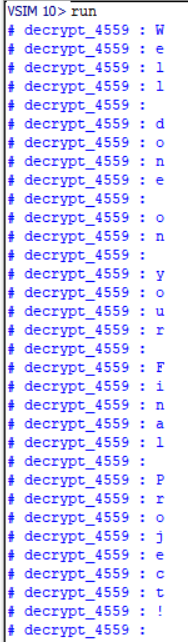




**Waveform result (PART 3)**

****

**Modelsim result .txt file result**



**Notepad++ result**

