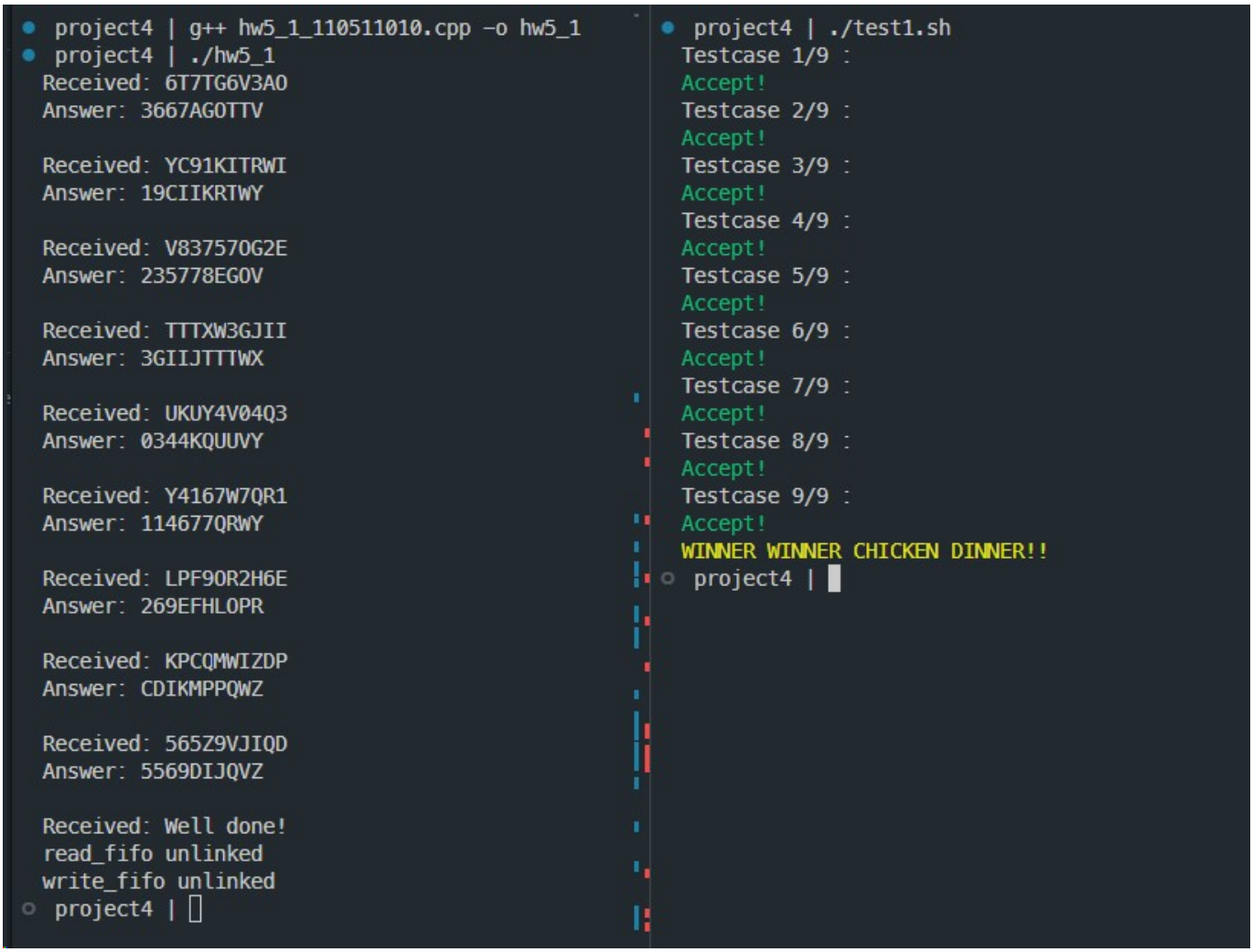
Report

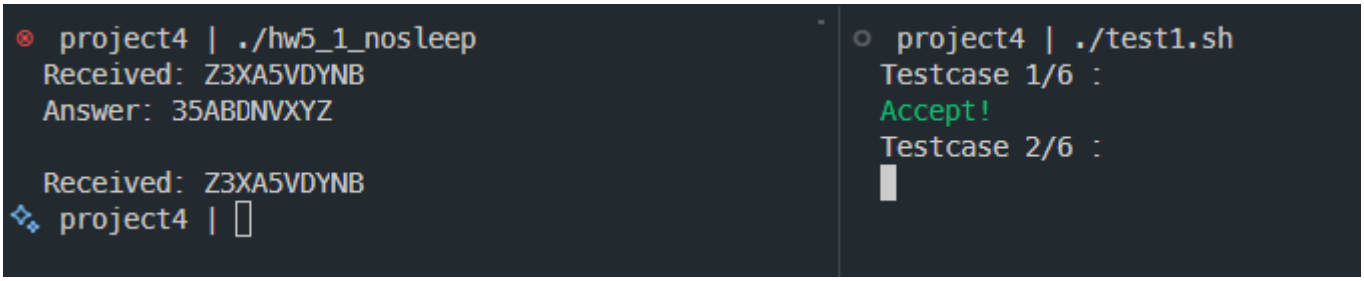
110511010 楊育陞

Part 1

a. test result:



b. What might happen if your program didn't call sleep(1) ? Why? => The program will read the same value from the FIFO, because the program will read the FIFO before the shell finish reading the FIFO and write to it, which is usually slower than the program. And the shell will keep waiting to read.

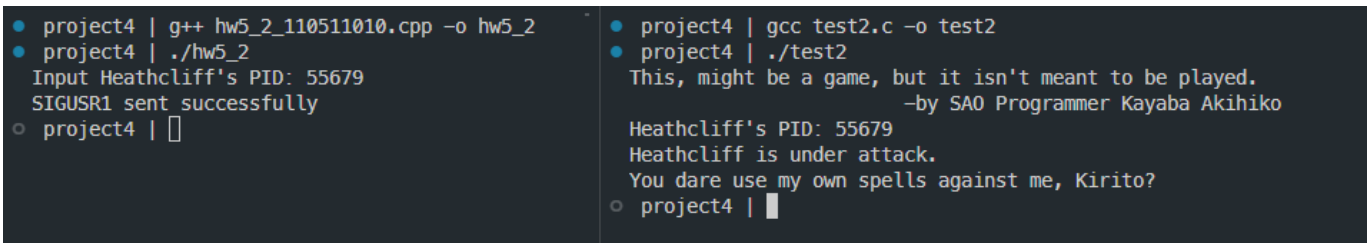


c. What happens when a process writes to a FIFO, but there is no process reading from it? => According to linux manual, the process will be blocked until another process opens the FIFO for reading.

> Once you have created a FIFO special file in this way, any process can open it for reading or writing, in the same way as an ordinary file. However, it has to be open at both ends simultaneously before you can proceed to do any input or output operations on it. Opening a FIFO for reading normally blocks until some other process opens the same FIFO for writing, and vice versa. See fifo(7) for nonblocking handling of FIFO special files.

Part 2

a. test result:



b. How did you defeat Heathcliff ? => Write down the pid of Heathcliff repeatedly for size of 0xC8763 to shared memory, and send SIGUSR1 to Heathcliff.

c. What might happen if you reverse steps 6 and 7, meaning, sending SIGUSR1 before writing the data? => Heathcliff will start to read the shared memory before the data is finished writing, which may cause Heathcliff to read the wrong data and fail to defeat Heathcliff.