Gaven Finch
Lab 9

Report:

1. I bypassed the CD key by putting a 1 into register $eax right before the function returned.
2. When an incorrect CD key is entered, a 0 is loaded into $eax and then a jump instruction moves to the clean up phase of the function. I changed that jump instruction into two nop instructions. Why? Because right after that jump is the section of code that's executed when the correct CD key is entered.
3. In the print_fortunes function there is a call to random. After this call returns, I modified the contents of $eax so I could incrementally view every fortune in order. They eventually started to wrap around from a mod operation or similar.

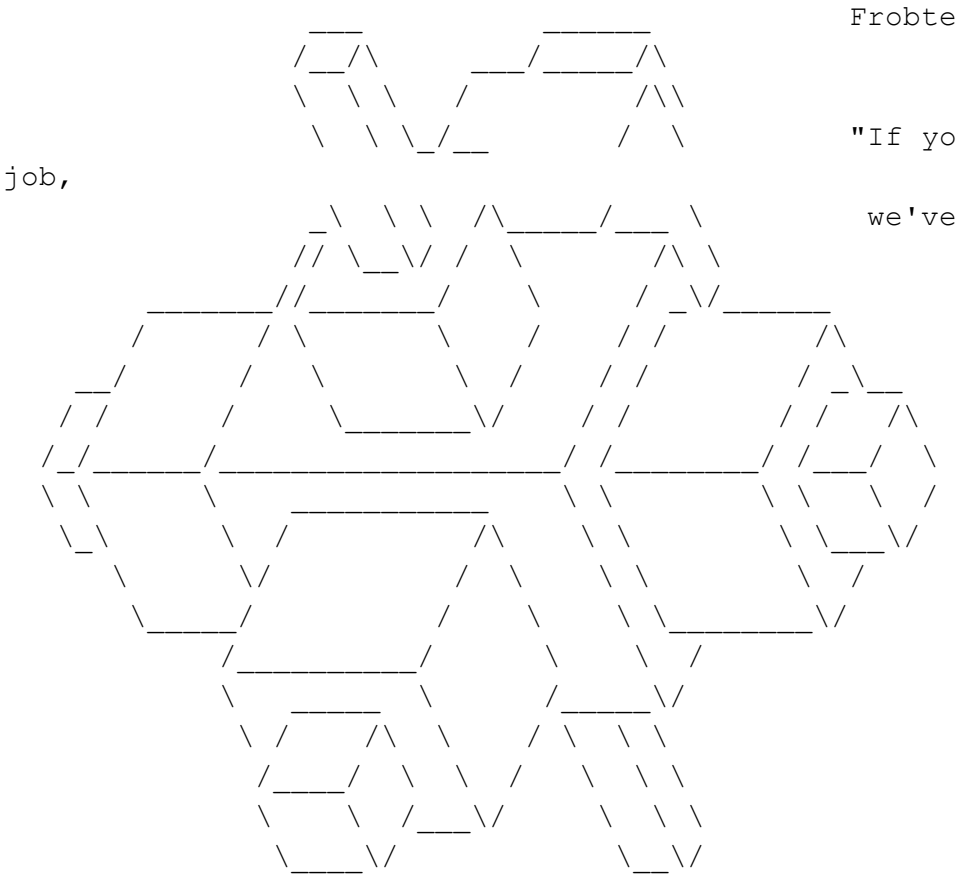
The fortunes:

A Thaum is the basic unit of magical strength. It has been universally
established as the amount of magic needed to create one small white pigeon
or three normal sized billiard balls.
-- Terry Pratchett, "The Light Fantastic"

"A wizard cannot do everything; a fact most magicians are reticent to admit,
let alone discuss with prospective clients. Still, the fact remains that
there are certain objects, and people, that are, for one reason or another,
completely immune to any direct magical spell. It is for this group of
beings that the magician learns the subtleties of using indirect spells.
It also does no harm, in dealing with these matters, to carry a large club
near your person at all times."
-- The Teachings of Ebenezum, Volume VIII

"Do not meddle in the affairs of wizards, for you are crunchy and good
with ketchup."

Rincewind had generally been considered by his tutors to be a natural wizard
in the same way that fish are natural mountaineers. He probably would have
been thrown out of Unseen University anyway--he couldn't remember spells and
smoking made him feel ill.
                -- Terry Pratchett, "The Light Fantastic"



Win98 error 001: Unexpected condition: booted without crashing.

Win98 error 002: Insufficient diskspace. You need at least 300 GB free memory.

Win98 error 003: Illegal ASM instruction. If your modem worked properly, the

FBI would have been called.

Win NT error 001: Error recording error codes. All further errors not displayed.

Win98 error 004: Virus activated from DOS Prompt - but the virus requires
Windows. Your system will be rebooted for the Virus to take effect. [OK]

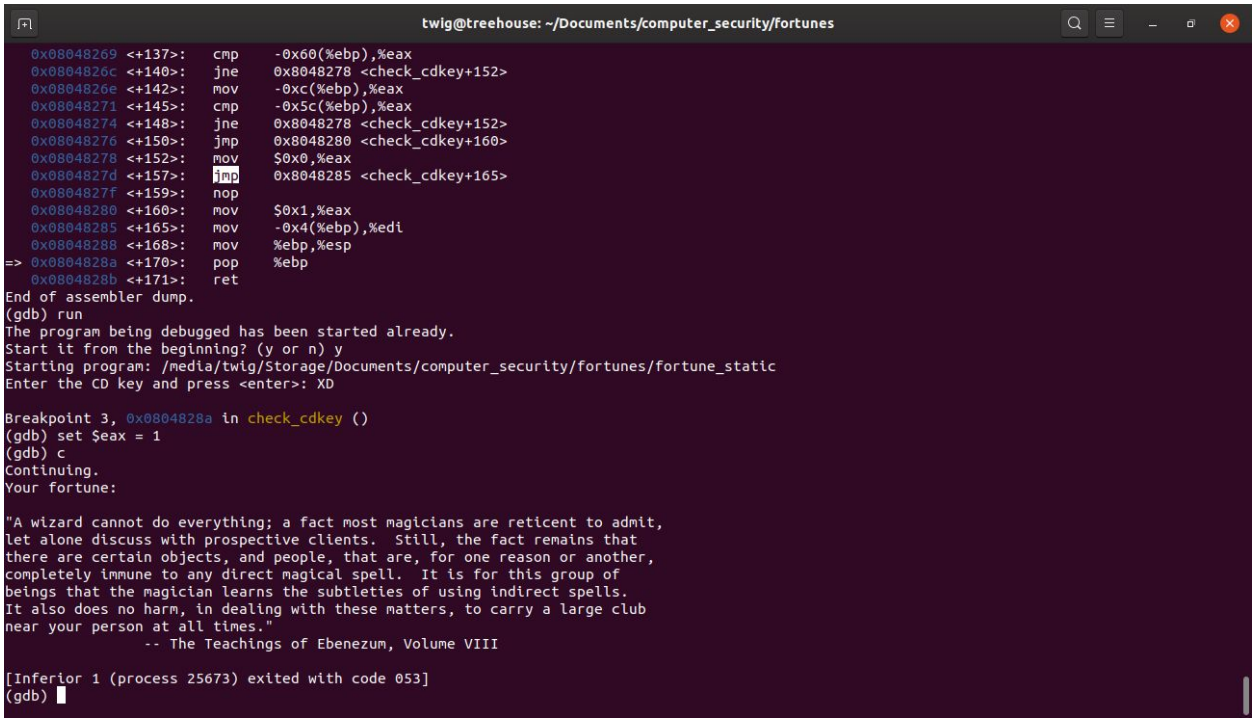
Win98 error 005: Mouse not found. Click left mouse button on ok to continue.

Win98 error 006: Keyboard not found. Press F1 to continue.

(1) Office employees will daily sweep the floors, dust the furniture, shelves, and showcases.
(2) Each day fill lamps, clean chimneys, and trim wicks. Wash the windows once a week.
(3) Each clerk will bring a bucket of water and a scuttle of coal for the day's business.
(4) Make your pens carefully. You may whittle nibs to your individual taste.
(5) This office will open at 7 a.m. and close at 8 p.m. except on the Sabbath, on which day we will remain closed. Each employee is expected to spend the Sabbath by attending church and contributing liberally to the cause of the Lord.

-- "Office Worker's Guide", New England Carriage Works, 1872

The following screenshot shows me inserting a 1 into register $aex to bypass the CD key check.



The following screenshot shows me modifying the output of the rand function to get fortunes from the file. It also shows that fortunes begin to repeat after 12, so I know I got them all.