For extra credit, I wrote a program that uses the Knapsack Cipher to encrypt plaintext and decrypt the ciphertext. The program will let you save the ciphertext generated to a file. This file can be opened and decrypted by the program. A password is used to ensure only the person that knows the password can decrypt the ciphertext saved in the file (password hashes must match). Though this program works, it is buggy, has features that are not fully implemented and needs to be polished. Also, to allow the program to decrypt saved ciphertext files, it was necessary to embed the key in with the ciphertext. Since the program currently uses very little obfuscation, to hide the key, the saved ciphertext files are not very secure. Additionally, for this program I created a reduced character set (RCS). Instead of the 256 normal ASCII characters, my RCS only has 64 characters. I did this to improve performance because when it was not using the RCS, it seemed like my computer was struggling to convert large blocks of plaintext to ciphertext. Perhaps, my computer strains due to an implementation error. I am just a novice programmer, so I probably did not write the most efficient code or even implemented something completely wrong. I really would like to have my program use all the characters and not the limited set it currently uses. This would make the program more useful. The following are a series of screenshots that show features of my program. The file KnapsackGUI.py contains the main method of the program.





















