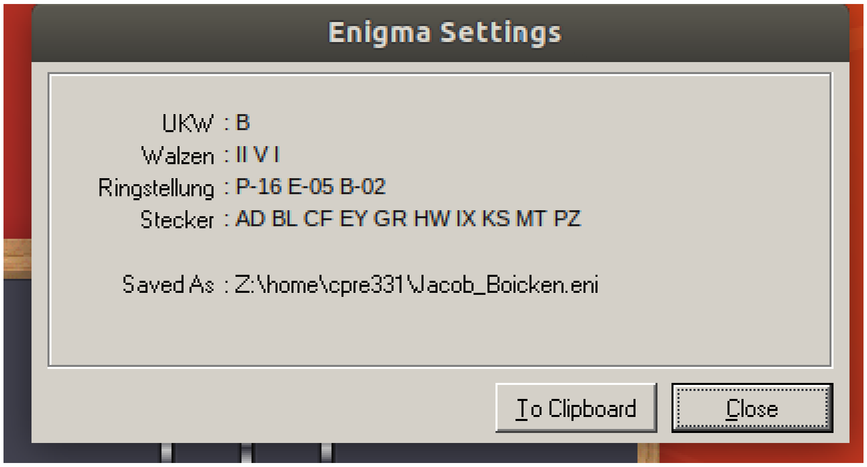
1) Part 1:

a. **Screenshot of the key view from the menu. Be sure the filename is your name.**
(10 points)



Enigma Settings

UKW : B
Walzen : II V I
Ringstellung : P-16 E-05 B-02
Stecker : AD BL CF EY GR HW IX KS MT PZ

Saved As : Z:\home\cpre331\Jacob_Boicken.eni

b. **The ciphertext that would be transmitted. Remember to include the header.**
(20 points)
1055 1tle 1tle 85 NOP OTF

FXPAW UMAQE NUNCB LASBV XASEX ASUWC MGYQH VTJSC TAOLE QRRRK NSYZN YPURI WCKAO UNZXL ZNJUN APBCA OCDXR RNUGF

2) Part 2:

a. **The decrypted message. (You do not have to add in the punctuation, but your grading TA would probably appreciate punctuation)**
(20 points)

SHES A MANIAC MANIAC ON THE FLOOR AND SHES DANCING LIKE SHES NEVER DANCED BEFORE

b. **What is the rotor order?**
(5 points)
III IV II

c. **What is the 3-letter Kenngruppen used for the message and the 2 random characters?**
(5 points)
EPL XD

d. **What is the encrypted message key?**
(5 points)
GOP

e. **What are the original random trigrams selected by the sender?**
(5 points)
EKI and XSU

f. **What time was the message sent? Please use the 12-hour format (include am or pm)**
(5 points)
6:40 am

g. **How many characters are in the message?**
(5 points)
66

3) Questions relating to Part 1 & 2:

a. **Some Enigmas used up to 5 rotors. What does an additional rotor add to the machine?**
(10 points)

The machine would perform an additional layer of substitution that an entered character would go through. This multiples the possible key combination by 26 for the rotor initial positions, and increases the rotor count the possibilities of rotor combination.

(Which I think is like n! If there are the same number of rotors and slots. And n^m if more rotors than slots. n = # of rotors, m = # of slots)

b. **It has been argued that the plugboard adds more security to the Enigmas than the additional rotors. However, the plugboard also provided a flaw that was used in the early cryptanalysis of the device. What was the design error and why was that a fatal flaw?**
(10 points)

I looked up information, but not quite sure:

The plugboard's relation for each character was one to one. So A could map to F, but then F had to map back with A as well. This means when testing a possible solution, you could find an inconsistency, i.e. multiple mapped to one character, then you could prove that solution doesn't work. This would limit the number of tests needed to be completely done. Thus significantly reducing the time to break the ciphertext.