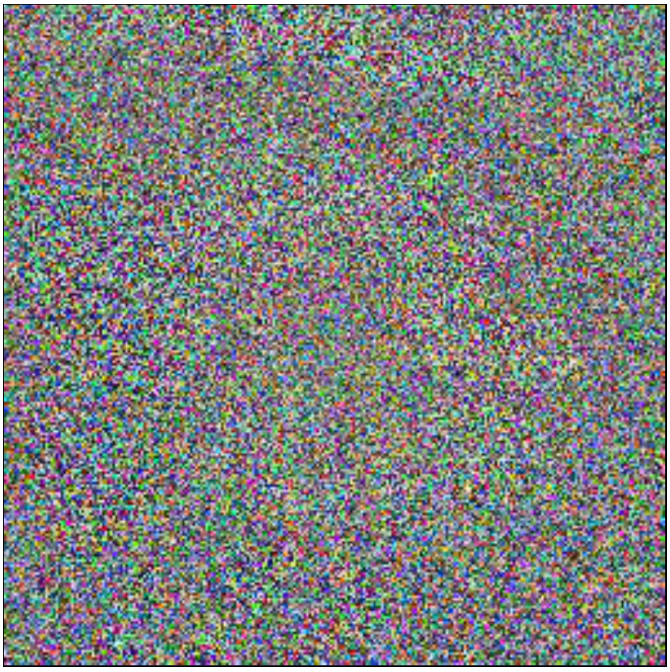
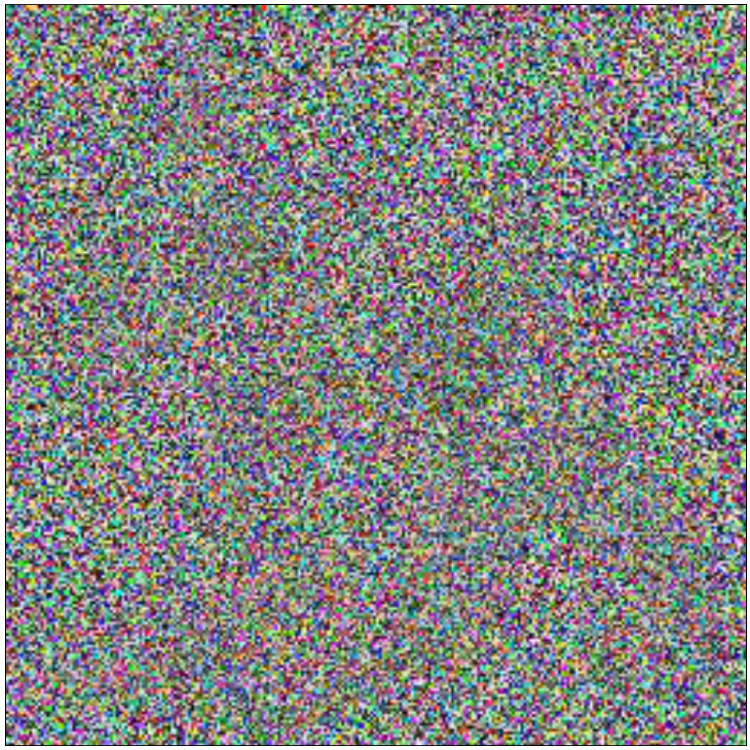
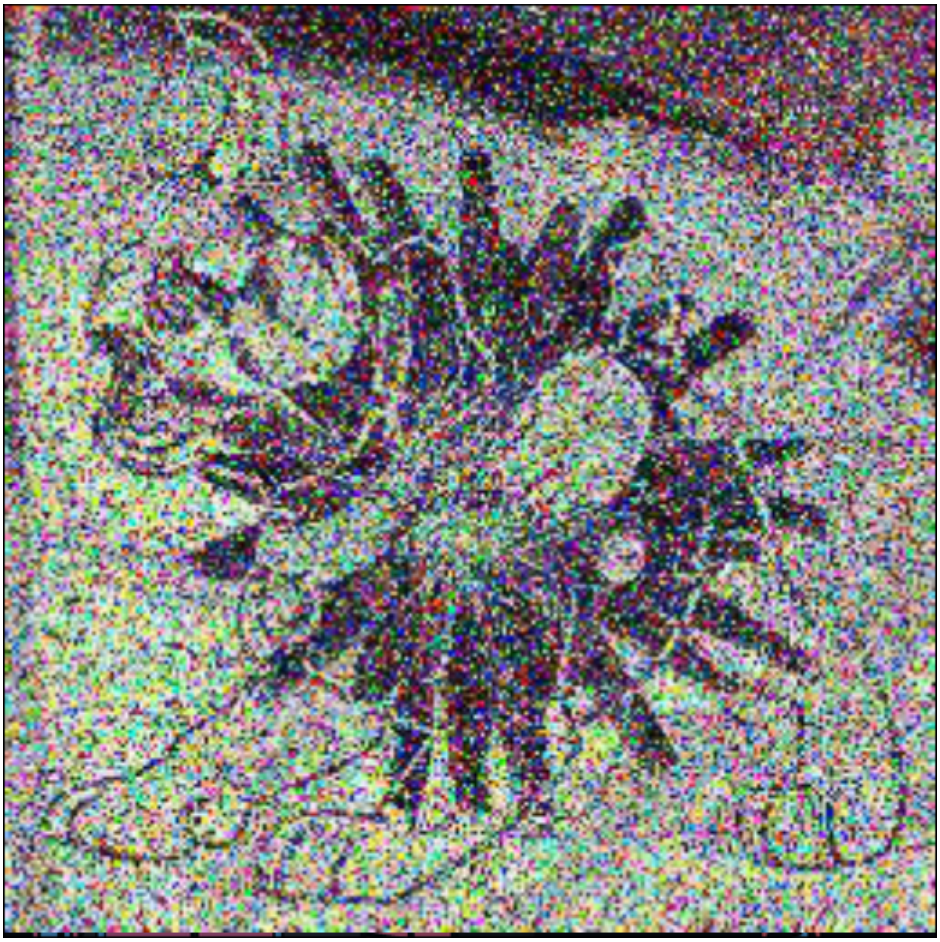
Lab04 - One-Time Pad and Rotor Ciphers

Part 01

1.) **Attach screenshots of “encryptedA.jpg”, “encryptedB.jpg”, and “output.jpg” and add them to your report.**
(5 points)

- encryptedA
  -

- encryptedB

- 
- output

- 

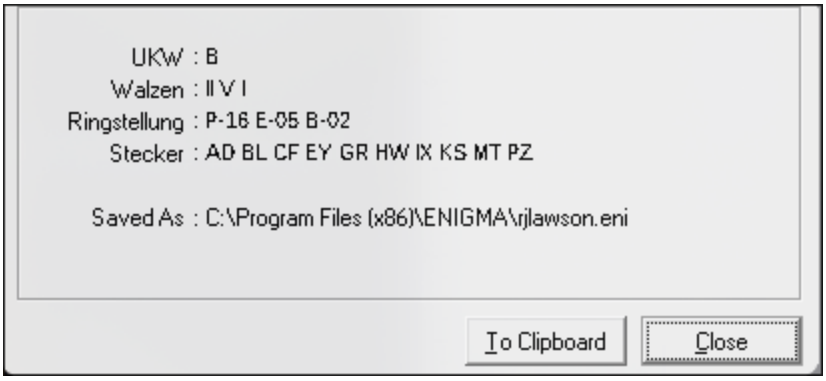
2.) What do you observe in “output.jpg”? Why does this happen?
(10 points)

- Since the ciphertext image is random it leads to perfect secrecy, but the plaintexts are different which in general doesn’t matter. The reason this happens is because when you use a one time pad on both images it is “secure” and will often give you the ability to decrypt them with each other which we just did. However, the plaintext images would be merged together causing both images to appear on one with data being lost in the process. This when Plaintext1 $\oplus$ OTP = Ciphertext1 and Plaintext2 $\oplus$ OTP = Ciphertext2 occur, you can combine both the OTP and both ciphertexts to get a “plaintext result Ciphertext1 $\oplus$ Ciphertext2 = Final Plaintext. The result stems from XORing two encrypted images and getting original images that are from two images that are encoded “1” and when formed together result in “0” leading them to a completed yet merged image.

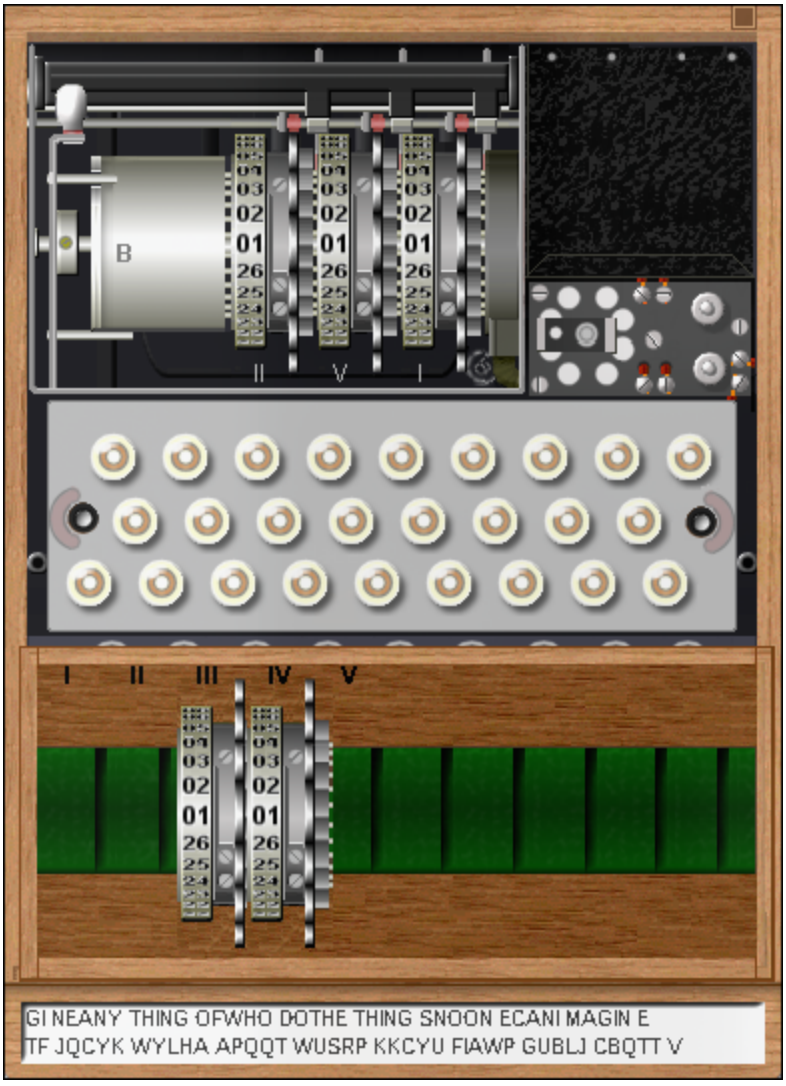
Part 02

3.) Screenshot of the key view from the menu. Be sure the filename is your name. (5 points)

-



-

- 

- 

4.) The ciphertext that would be transmitted. Remember to include the header. (20 points)

- Header
  - NOP

        - FXP
        - MT
    - Third Header
        - 

- using NOP
    - JNTLU EDTFC UPICL ICDFY TKREC SUJFA LCOZY UMNVD EKUUZ TKUYG GFSUA UMDLF OYGQX GOWSL HUWGV M
    - With extra letters
        - FXPMT JNTLU EDTFC UPICL ICDFY TKREC SUJFA LCOZY UMNVD EKUUZ TKUYG GFSUA UMDLF OYGQX GOWSL HUWGV M
- using TSR
    - LRFTR UIQPC REIPN CIXWM MGEFI JLZEH NBKBH YIONE ZKTSZ YTSNO GLSRA SYKYR KIFRJ MSFQW JKZ

      76 characters

5.) The decrypted message from December 16th 1944.
(20 points)

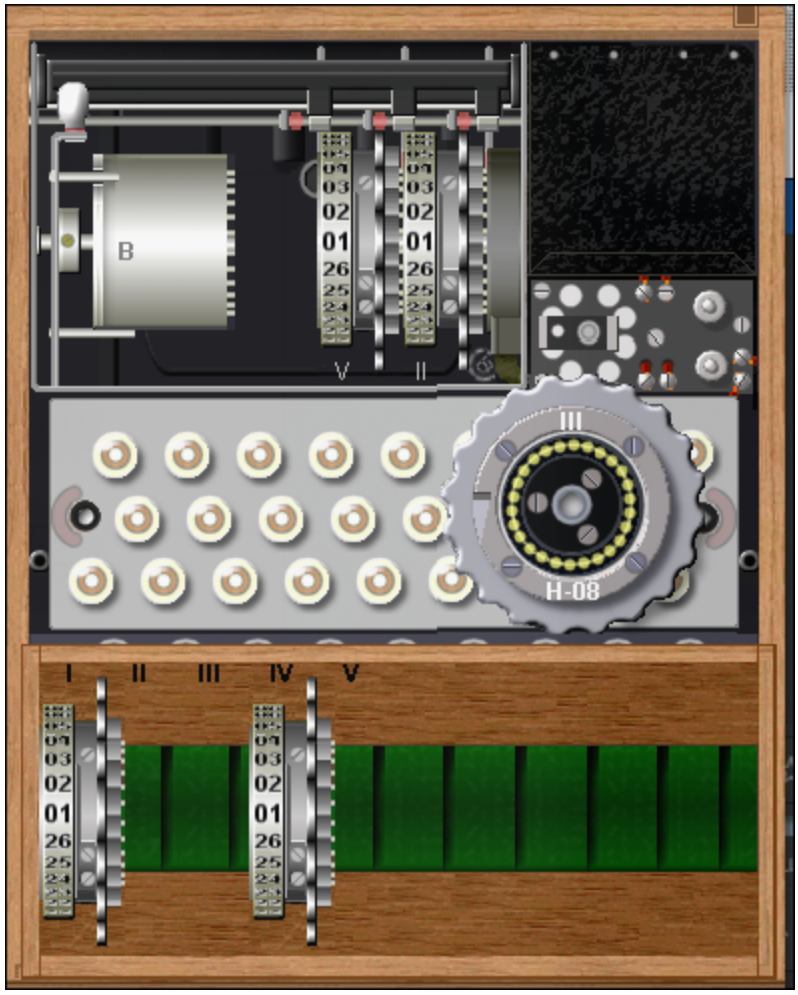
- SOMEB ODYON CETOL DMETH EWORL DISGO NNARO LLMEI AINTT HESHA RPEST TOOLI NTHES HED
- Somebody once told me the world is gonna roll me I ain't the sharpest tool in the shed

6.) What is the rotor order?
(5 points)

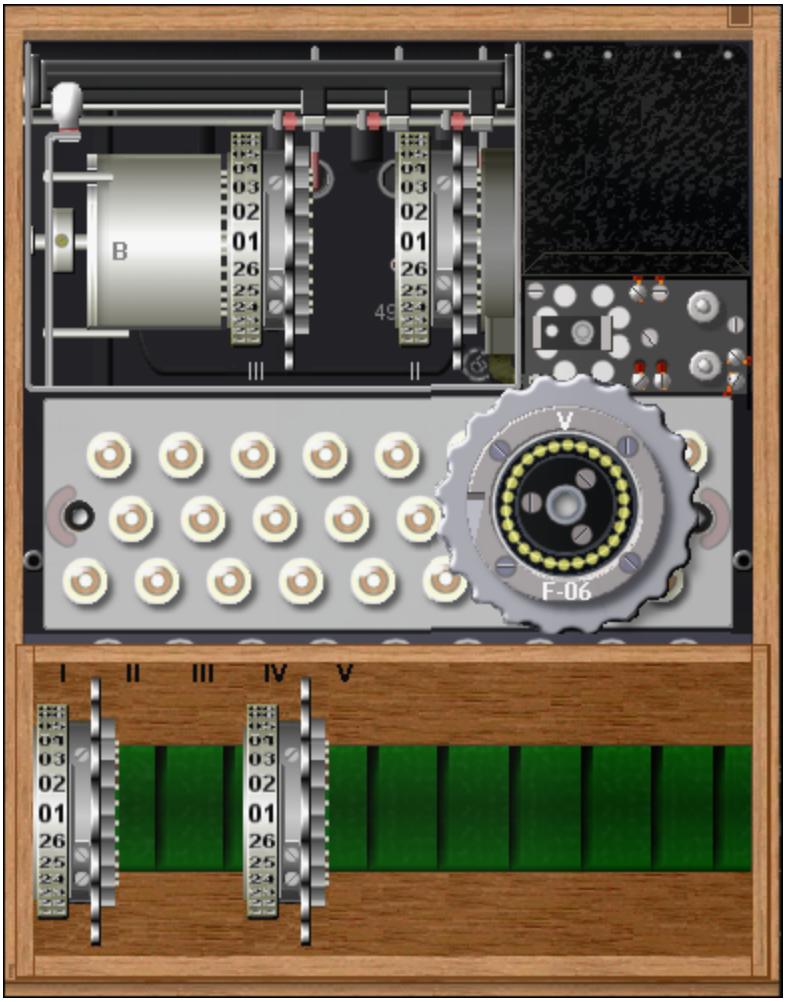
- 

- The Rotor Order is
    - III, V, II
        - 8, 6, 23

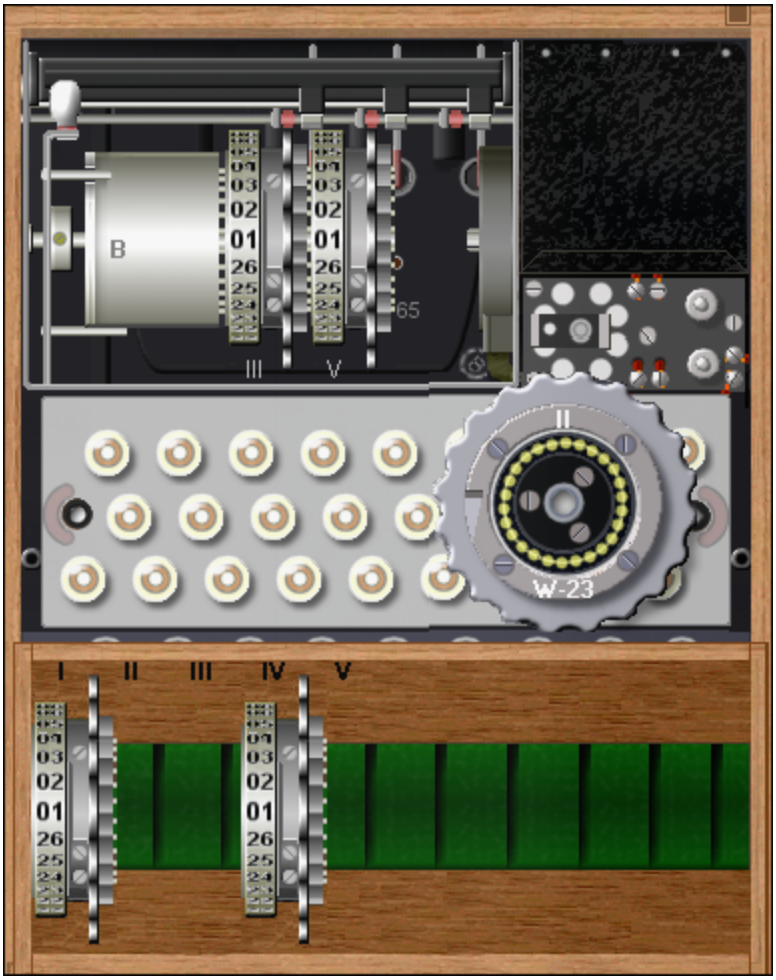
-


B
01
03
02
01
26
25
24
V
II
III
H-08
I
II
III
IV
V

-


B
01
02
03
26
25
24
III
II
V
F-06
I
II
III
IV
V

-


B
65
III
V
II
W-23
I
II
III
IV
V

-

7.) What is the 3-letter Kenngruppen used for the message and the 2 random characters?
(5 points)
- CKK
- WZ

8.) What is the encrypted message key?
(5 points)
- XKE

9.) What are the original random trigrams selected by the sender?
(5 points)
- CKK
- ASD
- ZXC

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

(10 points)

- Well an additional rotor can add up to 26 more possibilities to the table along with more options to do double notches, beta, gamma, and could add even more complexity to each encrypted message.

11.) 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)

- One fatal flaw was that when using the plugboard was the letters themselves, even when swapped they decrypted the message back to themselves. Which in turn reduced the security and even though it could add complexity to the encryption it was a weak point of the enigma.