**Applied Crypto**

**Learning Enigma Machine**

This project is to investigate enigma machines by altering the values of its various components and write your findings. With those findings, students may develop some approaches that could help the folks at Bletchley Park where Alan Turing and others designed an electromechanical machine called the "Bombe" to quickly test rotor settings to break the daily key.

Problem 1. Describe the main components of a typical enigma machine.

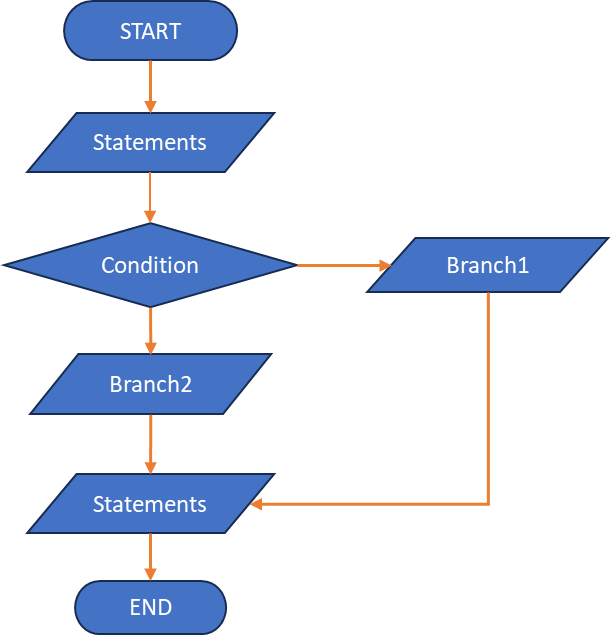
Problem 2. What is the size of the key space?

Refer to the manual at <https://py-enigma.readthedocs.io/_/downloads/en/latest/pdf/> Students can construct an enigma machine. I list my test code here for your reference.

from enigma.rotors.rotor import Rotor  
from enigma.plugboard import Plugboard  
from enigma.machine import EnigmaMachine  
  
rL = Rotor('my rotor1', 'EKMFLGDQVZNTOWYHXUSPAIBRCJ', ring\_setting=0, stepping='Q')  
rM = Rotor('my rotor2', 'BDFHJLCPRTXVZNYEIWGAKMUSQO', ring\_setting=5, stepping='V')  
rR = Rotor('my rotor3', 'ESOVPZJAYQUIRHXLNFTGKDCMWB', ring\_setting=10, stepping='J')  
  
reflector = Rotor('my reflector', 'YRUHQSLDPXNGOKMIEBFZCWVJAT')  
  
pb = Plugboard.from\_key\_sheet('AK BZ CG DL FU HJ MX NR OY PW')  
  
machine = EnigmaMachine([rL, rM, rR], reflector, pb)  
  
machine.set\_display('UPS') # set rotor positions or use its default  
position = machine.get\_display() # read rotor position  
print(position)  
  
# Encrypt A letter  
#print(machine.key\_press('C'))  
# Encrypt a text  
print(machine.process\_text('Enigma machine is powerful for Q'))

Problem 3. Explain the flow of the code and map the settings to the components mentioned in Problem 1.

One approach is to use workflow block diagram. It visualizes working logic (algorithm) of a code. A typical sample workflow is shown below. The purpose is to walk through the code like a professional software engineer, understand how the code works and do code development such as fixing bugs and adding new features, which is much-needed skills for tech students.



Problem 4. Learning by testing. Test the code with at least 7 various keys (change of wiring, ring\_setting, stepping, reflector, with or without plugboard, initial display position, etc.

Problem 5. Pick one of the ciphertexts from problem 4 and decrypt it. Make sure you keep the same parameters (or keys). Do we need to write another code for that?

Problem 6. Time for fun. Same setting as given in the sample code, but folks at Bletchley Park want to know the initial position (display). They had a ciphertext “WVUVJCSQBFLWSGTHDREWOSXYIAYEUBHHXY” from the known plaintext “ATTACK AT 5PM AT ATLANTIC Z ISLAND”. Code and find the init display.

Problem 7 (optional) Same enigma machine given by the sample code. We had the ciphertext “YNLIUNHBNVERXKRBUHZEYMJVEZNRPNWOSV” from the known plaintext “ATTACK AT 5PM AT ATLANTIC Z ISLAND”. Recover as many of the stecker settings as it possible from the known plaintext.

**Reference**

**Interesting Reading**: the more realistic decryption process “Example communication procedure” at <https://py-enigma.readthedocs.io/en/latest/guide.html> in which it gives a protocol of setting up initial display as communication vehicle is through radio signal, copied it here for fun.

“We will now present a simplified scenario based on a procedure employed by the army (*Heer*) after 1940. This example is based upon one found in Dirk Rijmenants’ simulator manual, which is based upon a real-life example from Frode Weierud’s Cryptocellar website.

Suppose a message needs to be transmitted. The operator of the transmitting machine consults his ***key sheet*** and configures his machine according to the daily settings found inside. Let’s suppose the key sheet dictates the following initial parameters for the current day:

* Rotor usage and order is *II IV V*
* Ring settings for each rotor, in order, are: *B U L*
* Plugboard settings are: *AV BS CG DL FU HZ IN KM OW RX*
* One of the daily Kenngruppen possibilities is *UGZ*

Let us also assume the reflector employed by this army unit is ‘B’.

The operator then configures his machine:

machine = EnigmaMachine.from\_key\_sheet(

rotors='II IV V',

reflector='B',

ring\_settings='B U L',

plugboard\_settings='AV BS CG DL FU HZ IN KM OW RX')

Suppose the Enigma operator was handed a message for transmit by an officer which reads “The Russians are coming!” The operator would first randomly decide two things:

* Initial rotor positions, say WXC
* A three letter *message key*, say BLA

The operator would then turn the rotor thumb wheels to set the initial rotor position and then type the three letter message key to produce an encrypted message key:

machine.set\_display('WXC') # set initial rotor positions

enc\_key = machine.process\_text('BLA') # encrypt message key

In this example, the encrypted key turns out to be KCH. This is written down for later.

The operator then sets the rotors to the unencrypted message key BLA and then types in the officer’s message, performing various substitutions and transformations according to training and current procedures. In our simple case, he performs the following:

machine.set\_display('BLA') # use message key BLA

ciphertext = machine.process\_text('THEXRUSSIANSXAREXCOMINGX')

print(ciphertext)

This produces the ciphertext NIBLFMYMLLUFWCASCSSNVHAZ.

Next, between the Enigma operator and the radio operator, a message is formed up. This message includes the following components:

* The time of transmission
* The station identification for transmitter and intended recipient(s)
* The message length; in our case this is 24
* The initial rotor positions in unencrypted form (WXC)
* The encrypted message key value (KCH)
* The unencrypted message indicator (*Kenngruppen*)
* The encrypted message contents

In our example, the message handed over to the radio operator to be transmitted by either Morse code or perhaps even voice would look something like this:

U6Z DE C 1500 = 24 = WXC KCH =

BNUGZ NIBLF MYMLL UFWCA

SCSSN VHAZ=

The top line indicates day 31, station C transmits to station U6Z, sent at 1500 hours and contains 24 letters. The starting position is WXC and the encrypted message key is KCH.

Next we have the body of the message. The army transmitted messages in 5 letter groups. The first group contains the Kenngruppen, or indicator. Procedure required the operator pick one of the Kenngruppen possibilities from the key sheet, and then pad it out with two random letters. Here the operator chose to prepend BN to the Kenngruppen value of UGZ. He could have also appended the two letters, or perhaps appended one and prepended the other.

After the message indicator group, the encrypted text follows in 5 letter groups.

Now at receiving station U6Z, the radio operator receives the over-the-air message and types or writes it up in the form shown and hands it to the Enigma operator.

The Enigma operator first looks for the message indicator. He uses the group BNUGZ and scans his key sheet for either BNU, NUG, or UGZ. He could presumably also use the date information found in the message preamble to help his search of the key sheet. If everything checks out the operator now knows which entry in his monthly key sheet to use. Thus, as was done at the transmitting station, he configures his Enigma according to the key sheet:

machine = EnigmaMachine.from\_key\_sheet(

rotors='II IV V',

reflector='B',

ring\_settings='B U L',

plugboard\_settings='AV BS CG DL FU HZ IN KM OW RX')

The receiving operator then must decrypt the message key:

machine.set\_display('WXC')

msg\_key = machine.process\_text('KCH')

This should reveal that the message key is the original BLA. The rotors are then set to this value and the message can be decrypted, taking care to ignore the Kenngruppen:

machine.set\_display(msg\_key) # original message key is BLA

plaintext = machine.process\_text('NIBLFMYMLLUFWCASCSSNVHAZ')

print(plaintext)

The Enigma operator then decodes the message “THEXRUSSIANSXAREXCOMINGX”. He then uses his training and procedures to further process the message. Finally, the somewhat troubling message “The Russians are coming” is handed to his commanding officer.”