

הבהרות

1. אין בדיקת משום שלא נדרש במסמך והנחתי שהבודק ידע להכניס ערכים נכונים.
2. התוכנה יודעת לקבל אך ורק אותיות ABC גדולות. כל קלט שאינו אות גדולה, יקריס את התוכנה.

שאלה 5 – הסבר

1. אתחול של מכונת האנגימה עם הערכים ההתחלתיים שהוגדרו לתאריך 29 לאוקטובר.

```
# enigma machine creation
enigma = Enigma(4, 24, 14, # right rotor, setting, offset
                5, 9, 15, # middle rotor, setting, offset
                2, 19, 3, # left rotor, setting, offset
                [(('Z','U'),('H','L'),('C','Q'),('W','M'),('O','A'),('P','Y'),('E','B'),('D','R'),('D','N'),('V','I')])])
```

2. הצפנה של המילה MLD וקבלה של המילה DOR

To Go Back Enter-1
Enter Message: **MLD**
Encrypted Message: DOR

3. השמה של המילה DOR כ-offset (4, 15, 18)

```
# enigma machine creation
enigma = Enigma(4, 24, 18, # right rotor, setting, offset
                5, 9, 15, # middle rotor, setting, offset
                2, 19, 4, # left rotor, setting, offset
                [(('Z','U'),('H','L'),('C','Q'),('W','M'),('O','A'),('P','Y'),('E','B'),('D','R'),('D','N'),('V','I')])])
```

4. הזנה של הטקסט המוצפן וקבלה של התוצאה הרצויה

```
Go Back Enter-1
ter Message: UMDPQ CUAQN LNVSP IARKC TTRJQ KCFPT OKRGO ZXALD RLPUH AUZSO SZFSU GWFNF DZCUG VEXUU LQYXO TCYRP SYGGZ HQMAG PZDKC KGOJM MYYDD H
rypted Message: GROUP SOUTH COMMA NDFRO MGENP AULUS XSIXT HARMY ISENC IRCLE DXOPE RATIO NBLAU FAILE DXCOM MENCE RELIE FOPER ATION IMMED IATEL Y
```

Profiling Summary

This picture was taken when I encrypted the word ENIGMA with the following configurations:

	Rotor number	Setting	Offset
Right rotor	3	1	1
Middle rotor	2	1	1
Left rotor	1	1	1

ncalls	tottime	percall	cumtime	percall	filename:lineno(function)
3	11.399	3.800	11.399	3.800	{raw_input}
267	0.000	0.000	0.000	0.000	Translator.py:14(letterToIndex)
36	0.000	0.000	0.000	0.000	Rotor.py:32(translation)
6	0.000	0.000	0.000	0.000	Enigma.py:57(encryptLetter)
72	0.000	0.000	0.000	0.000	Translator.py:23(circularShifts)
5	0.000	0.000	0.000	0.000	Rotor.py:24(reverseTranslation)
72	0.000	0.000	0.000	0.000	Translator.py:19(indexToLetter)
606	0.000	0.000	0.000	0.000	{ord}
1	0.000	0.000	0.000	0.000	Enigma.py:23(createRotors)
12	0.000	0.000	0.000	0.000	Enigma.py:52(changeDir)
5	0.000	0.000	0.000	0.000	Rotor.py:8(__init__)
36	0.000	0.000	0.000	0.000	Rotor.py:54(changeDirection)
72	0.000	0.000	0.000	0.000	{chr}
1	0.000	0.000	0.000	0.000	Enigma.py:7(__init__)
12	0.000	0.000	0.000	0.000	Plugboard.py:24(translation)
12	0.000	0.000	0.000	0.000	Rotor.py:48(isTurnover)
1	0.000	0.000	0.000	0.000	Plugboard.py:11(setConfiguration)
1	0.000	0.000	0.000	0.000	Enigma.py:38(setRotorsSettings)
6	0.000	0.000	0.000	0.000	Rotor.py:43(step)
6	0.000	0.000	0.000	0.000	Reflector.py:8(translation)
1	0.000	0.000	0.000	0.000	Plugboard.py:7(__init__)
1	0.000	0.000	0.000	0.000	Enigma.py:48(createReflector)
1	0.000	0.000	0.000	0.000	Enigma.py:43(setRotorsOffsets)
1	0.000	0.000	0.000	0.000	Enigma.py:30(selectRotors)
8	0.000	0.000	0.000	0.000	{method 'append' of 'list' objects}
1	0.000	0.000	0.000	0.000	Reflector.py:5(__init__)
1	0.000	0.000	0.000	0.000	{len}
1	0.000	0.000	0.000	0.000	{method 'disable' of '_lsprof.Profiler' objects}
3	0.000	0.000	0.000	0.000	Rotor.py:20(setOffset)
3	0.000	0.000	0.000	0.000	Rotor.py:17(setSetting)

Enigma M3 Machine – class Diagram

Author: Omri Hadad

ID: 302726088

