1 Enigma

Question 1: Send the non-secret information required to decrypt the message (which includes the encrypted text and your birthday) to one of your colleagues by email (make sure that you add Mick and Uraz to CC). Once you receive the corresponding message from your fellow colleague, configure your Enigma machine accordingly and decrypt the message.

I send to him this cipher in addition to the plain text from his cipher:

1- My birthday is October 04th.

```
 1st trigram: 'XYZ'
 2nd trigram: 'ABC'
 Cipher:      'EIGZB YUEXZ WUDZR RMKJW'
```

2- The Plain Text of your birthday gift is: *give me a ticket to mars*

He Sent me his cipher in addition to the plain text of my cipher:

1- My birthday is April 18th.

```
 1st trigram: 'ABC'
 2nd trigram: 'DEF'
 Cipher:      'QPEBN OLPTG KCIEX AAJWJ MB'
 The 3rd trigram (secret) are the first 3 characters of the cipher, so 'QPE'
is the one.
```

2- Your plain text message is “RAZEREARPHONESPLEASE” (razer earphones please).

About the Procedures:

1- Setup the Enigma simulator:

a- Fields:

```
 Tag: Day of the month
 Walzenlage: Choice and order of wheels
 Ringstellung: The setting of the alphabet rings
 Steckerverbindungen: The plug connections on the plugboard
 Kenngruppen: Letter groups to identify the day of the month to the receiver
at the beginning of a message
 In my case:
 My Birthday is October, 04
 | 04 | III  I  V |  15 07 10  | AE BW CP DQ FT HV JN KU LM RZ | IWG CNP DFC
TKM |
```

b- Setting the Rotators:

```
 Wheel III on the left, wheel I in middle, and wheel V on the right.
```

c- Select the alphabet for each wheel:

```
III = 15 (O), I = 07 (G), V = 10 (J)
```

d- Connect the plugs in the plug board:

```
A -> E, B -> W, C -> P, D -> Q, F -> T, H -> V, J -> N, K -> U, L -> M, R
-> Z
```

2- Encrypt a message:

e- Choose 2 random trigrams 1- XYZ, 2- ABC.

f- Put the first trigram as start point for the rotator (X=24, Y=25, Z=26).

g- Use the enigma keyboard and type the second trigram and write down the illuminate letters each time we press a key in order to produce the "encrypted message key" .

h- Change the rotator to the second rotator (A=01, B=02, C=03).

i- write down your message letter by letter "RAZEREARPHONESPLEASE".

j- Open the clipboard to get the encrypted message and copy it "EIGZB YUEXZ WUDZR RMKJW".

2- Send the message:

As described above and in the email.

3- Decrypt the message:

k - Repeat the "Setup the Enigma simulator" Process but with different date April, 18th.

```
  | 18 | II   III  I    |  04 15 02  | AK DH EV FM GL IW NY OP SX TU | NNA
VQB EMR IGT |
```

l- Verify the date by checking if 3 letters from Kenngruppen exist plus 2 random letters. We do not decrypt this part, we start at the 6th letter.

m- Type the encrypted message.

n- Display the plain text from the clipboard.

Sources: 1- https://www.enigmaworldcodegroup.com/how-to-create-an-enigma-message. 2- http://www.ellsbury.com/enigma3.htm 3- https://www.enigmaworldcodegroup.com/create-an-enigma-message 4- https://www.enigmaworldcodegroup.com/encrypting-a-message

---

2 Viola

1- Viola Machine:

a- 1 static reflector and 10 rotors each with 30 characters.

b- 5 unique reflectors to select from.

c- 50 unique(under all rotations) rotors to select from.

d- Standard plugboard for all 30 characters.

e- Unknown plugboard cables are used, so assume any number.

```
I- Any of the 50 rotors could be placed in 10 positions, there were 50! /
(50-10)! = 3.727604302×10^16 possible ways of selecting and ordering the
rotors.

II- Since each of the rings could be placed in any of 30 positions on the
ring setting. So there were  30 ^ 10 = 5.9049×10^14 possible ways of
rotationally put the rings around the rotors.

III-If we assume that Viola works exactly like Enigma so  ring setting on
the left rotor was irrelevant because its turnover notch did not affect
other rotors, there were 30 ^ 9 = 1.9683×10^13 positions for the real
contribution of the ring setting.

IV- The number of ways of choosing m pairs out of n object is:
(n!/((n-2m)!m!2^m))

so if 1 pair: (30! /((30 - 2 × 1)! × 1! × 2^1)=435)
      5 pair: (30!/((30 - 2 × 5)! × 5! × 2^5)=28392539175)
     11 pair: (30!/((30 - 2 × 11)! × 11!× 2^11)=8.04736836×10^16)
and so on.
```

If we want to calculate the total number of ways of choosing 15 pairs, I used this Python script to calculate it:

```
#!/usr/bin/env python
import math

t = 0
for m in range(1,16):
    t += math.factorial(30) / (math.factorial(30-2*m) * math.factorial(m) *
math.pow(2,m))

print ("The total number is",t)
```

NOTICE THAT I GOT A RED ANSWER ON THIS QUESTION BECAUSE I FORGOT TO ADD THE: 1 Reflector wheel contains 5 unique reflectors which is the number of possibilities is 5, so I added it to the calculation.

```
total number is = 6.069172699090484 × 10^17 so now we add it to the
calculation:
```

```
5 * 3.727604302×10^16 * 5.9049×10^14 * 1.9683×10^13 * 6.069172699090484 ×
10^17 = 1.3147∗10^63
```

SO NOW WE GET THE CORRECT ANSWER :D

2- Enigma

a- 1 static reflector and 3 rotors each with 26 characters. b- 3 unique reflectors to select from. c- 5 unique(under all rotations) rotors to select from. d- Standard plugboard for all 26 characters. e- The operator uses 10 plugboard cables.

I- Any of the five rotors could be placed in left position, any of remaining four in middle, and any of remaining 3 in the right position, there were 5 * 4 * 3 = 60 possible ways of selecting and ordering the rotors.

II- Since each of the rings could be placed in any of 26 positions on the ring setting. So there were 26 * 26 * 26 = 17,576 possible ways of rotationally put the rings around the rotors.

III- The ring setting on the left rotor was irrelevant because its turnover notch did not affect other rotors, there were 26 * 26 = 676 positions for the real contribution of the ring setting.

IV- They though that the greatest contribution of the enigma was the ten leads there were (10 pairs) 26! / (6! 10! 2^10) = 150,738,274,937,250 ways of plugging up the steckerboard, But they were wrong that huge number wouldn't guarantee the security of the Enigma.

The total number of states of the Enigma is: 60 * 17576 * 676 * 1.507382749373 * 10^14 = 1.074586873273 * 10^23

Sources:

a- https://crypto.stackexchange.com/questions/33628/how-many-possible-enigma-machine-settings b- http://www.ellsbury.com/enigma4.htm c- https://www.codesandciphers.org.uk/enigma/enigma3.htm d- The code book: (Section: How Many Keys?)