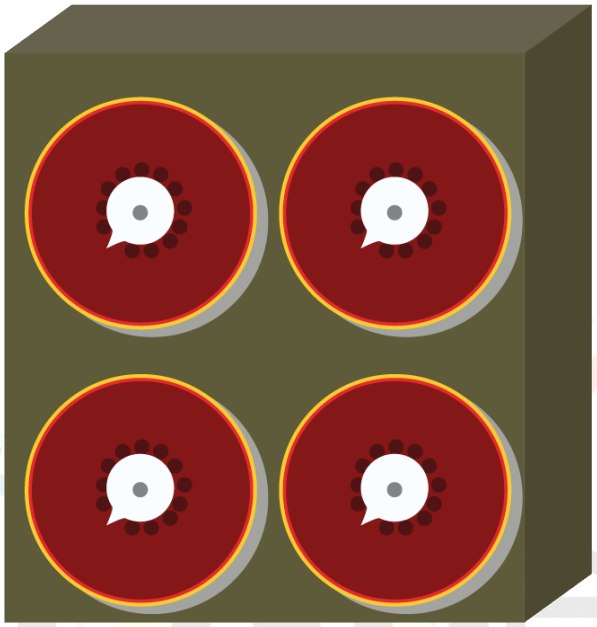
CONCORDIA ENGINEERING WEEK COMPETITIONS



CODING CHALLENGE

MARCH 8TH, 2017

ENG WEEK 2017
CODING CHALLENGE

Welcome! You are part of a select group of brilliant minds hand-picked by Alan Turing to program his new machines and finally finish this war. The enemy is smart, so we have to be smarter!

Through the sacrifice of hundreds of our soldiers and secret agents, we were able to acquire the taxonomy of the enemy's message cryptography device. As it turns out, it was an enigma machine all along, a well know device that has been used for several years already. Unfortunately, to mere humans, deciphering it is impossible, but luckily Dr. Alan Turing has guaranteed that his machines can all outsmart the enemy given the right instructions and inputs.

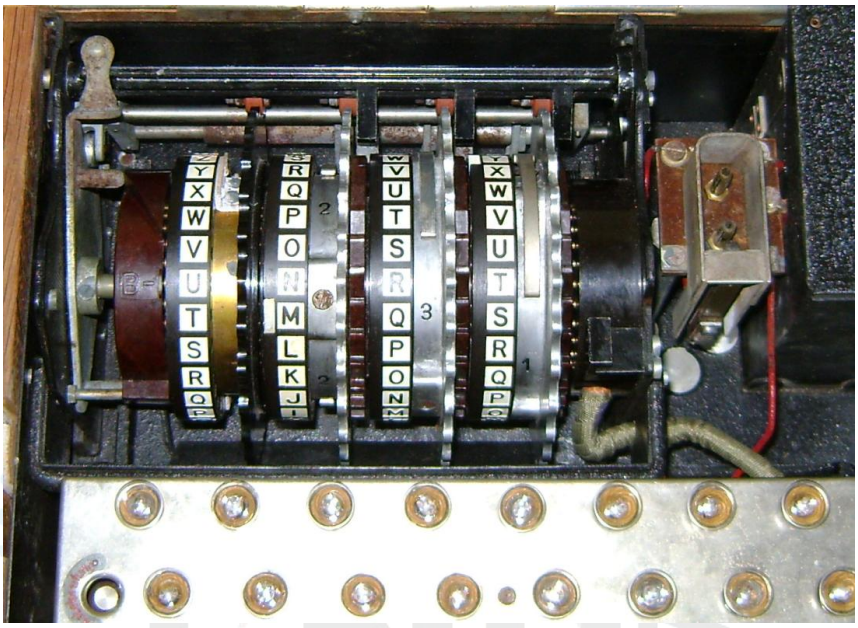
Let us start by explaining to you how enigma machines work and how you can start decrypting it:

A normal enigma machine is comprised of 3 different parts:

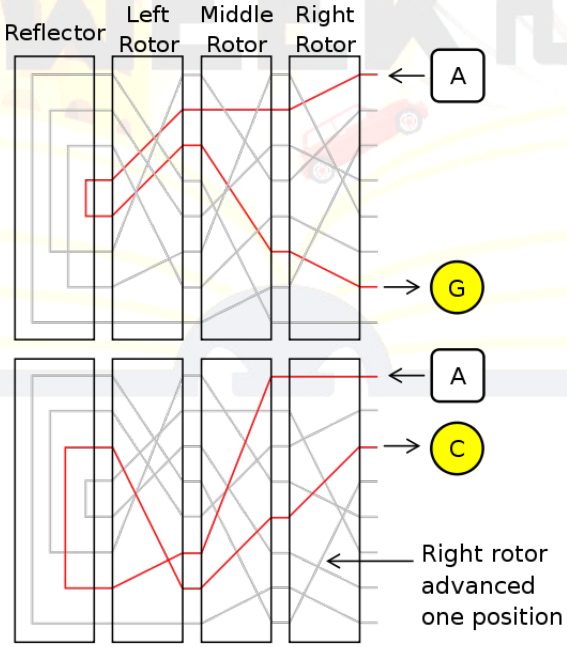
1. Input Keyboard
2. Scrambling Unit containing 4 rotation gears (Rotors)
3. Output board

As a mechanical device, the enigma passes the signal given by the keyboard through the scrambling unit where each rotor will swap the given letter and pass it on until it reaches the output board were the cyphered letter will appear. The rotors are then rotated clockwise at a programmable pace.

More on the rotors:



Every gear contains a fixed right side containing the full alphabet and a rotatable left side containing a random sequence unique for that rotor. The 3 first rotors from right to left are rotatable units and the last one (called reflector) is fixed and never rotates.



LET'S RUN THROUGH A QUICK EXAMPLE:

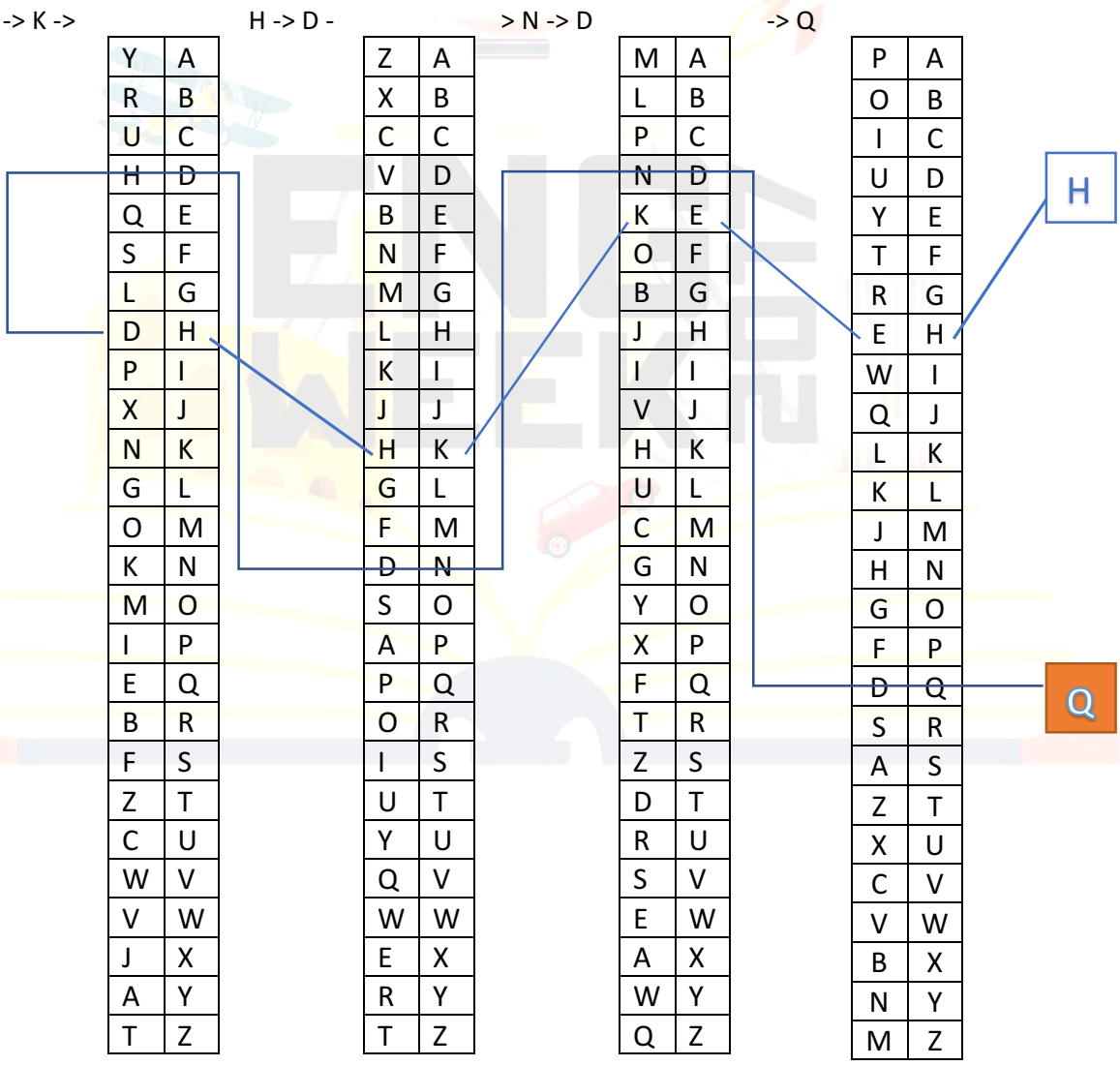
Imagine we would like to send the message “HI” to the other side with the following enigma configuration:

Rotor I: POIUYTREWQLKJHGFDSAZXCVBNM
Rotor II: MLPNKOBJIVHUCGYXFTZDRSEAWQ
Rotor III: ZXCVBNMLKJHGFDSAPOIUYQWERT
Reflector: YRUHQSLDPXNGOKMIEBFZCWVJAT
Where Rotor I rotates after every letter, Rotor II rotates after Rotor I completes a full rotation and Rotor III only rotates when Rotor II completes its full rotation.

In order to send “HI” we have:

1. To send ‘H’

H -> E -> K -> H -> D - > N -> D -> Q



Y	A
R	B
U	C
H	D
Q	E
S	F
L	G
D	H
P	I
X	J
N	K
G	L
O	M
K	N
M	O
I	P
E	Q
B	R
F	S
Z	T
C	U
W	V
V	W
J	X
A	Y
T	Z

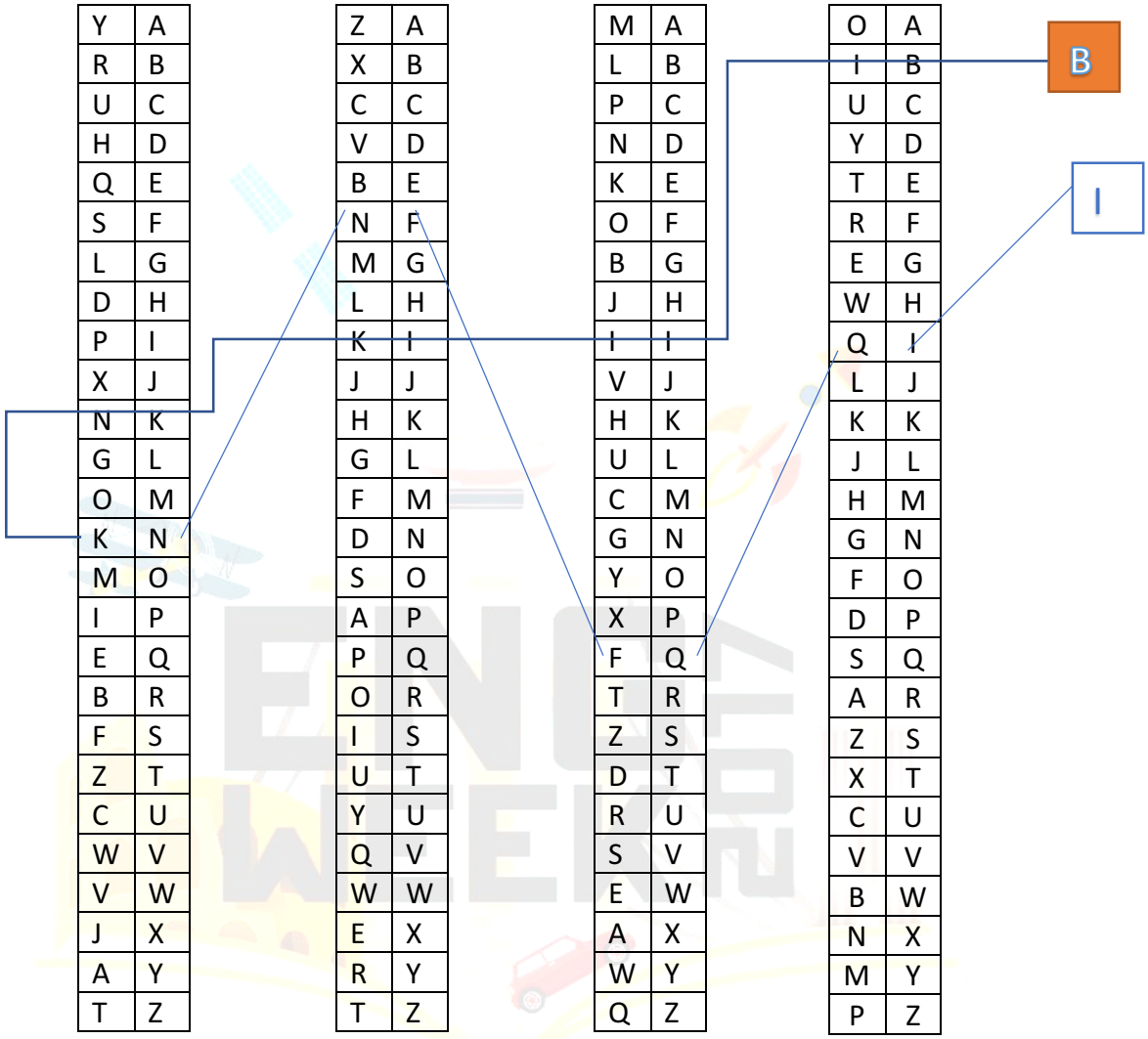
Z	A
X	B
C	C
V	D
B	E
N	F
M	G
L	H
K	I
J	J
H	K
G	L
F	M
D	N
S	O
A	P
P	Q
O	R
I	S
U	T
Y	U
Q	V
W	W
E	X
R	Y
T	Z

M	A
L	B
P	C
N	D
K	E
O	F
B	G
J	H
I	I
V	J
H	K
U	L
C	M
G	N
Y	O
X	P
F	Q
T	R
Z	S
D	T
R	U
S	V
E	W
A	X
W	Y
Q	Z

P	A
O	B
I	C
U	D
Y	E
T	F
R	G
E	H
W	I
Q	J
L	K
K	L
J	M
H	N
G	O
F	P
D	Q
S	R
A	S
Z	T
X	U
C	V
V	W
B	X
N	Y
M	Z

2. To send Letter ‘I’ (Notice the clockwise rotation of rotor I):

I -> Q -> F -> N -> K -> I -> I -> B



message “HI” would be sent as “QB”.

Now, to decrypt the message, all you need is to have an enigma machine with the same configuration and the letters (‘Q’ and ‘B’) will follow the same path as you can see above.

NOW TO THE REAL CHALLENGE:

We have intercepted a message from the enemy this morning. Our secret agents have leaked us the configuration used for their machines. However, the amount of data is far too long to be deciphered by hand and now we need to use Dr. Turing's new machines.

Here is what we have:

Rotor I: MNBVCXZQWERTYUIOPLKJHGFDSA
Rotor II: AJDKSIRUXBLHWTMCQGZNPYFVOE
Rotor III: QWERTYUIOPASDFGHJKLZXCVBMN
Reflector: YRUHQSLDPXNGOKMIEBFZCWVJAT
Where Rotor I turns every letter, Rotor II turns every second letter, and Rotor III turns every third letter.
We have intel confirming that the enemy replaces all space characters with "QQ" before encrypting the messages.

Your mission is to:

1. Create a program in any language capable of reading a file given through the Command Line arguments and generating a file called enigma.txt with the encrypted or translated version of that file.
2. Submit your code in a zip file with a readme file with the team members' names as well as instructions on how to run the code.

ATTENTION: We also received information that the file contains secret messages that can possibly lead to new intel.

EXTRA POINTS: If your solution is capable of reading any given combination of an enigma machine, you will be awarded extra points. Example: config file where line 1 = Rotor I, line 2 = Rotor II, line 3 = Rotor3, line 4 = reflector and line 5 = rotation configuration. DOCUMENT YOUR ASSUMPTIONS IN THE README FILE.

P.S. As this is WAR, time is our most precious resource, a faster and optimized solution will guarantee us (and you) the victory!

TIP: You can create an extra command line flag to differentiate between translating the message (reinserting spaces) and encrypting it. Document your changes in the README file.