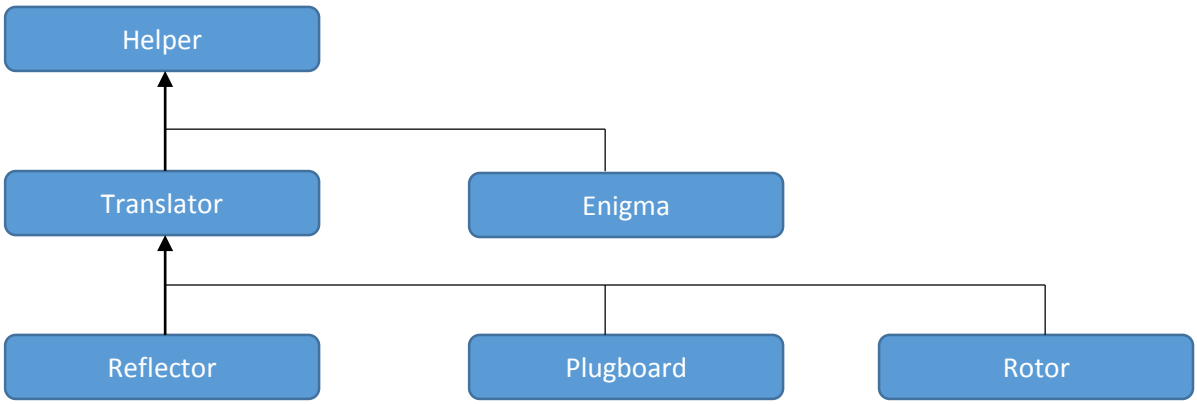
Boris Dahtiar - 307784900

Assignment 1: Enigma

The design I used is the suggested design, with a little tweaking of my own.

It was easier for me to design the Rotor functions in the Rotor class, and the forward/backward translation in the Translator class.

Design Overview



1. **Helper** – Letter-Index conversations.
2. **Translator** – Forward and reverse permutation computing.
3. **Reflector** – A Translator with only a forward computing permutation.
4. **Plugboard** – Translator with a forward computation only, can receive a string of pairs to build a corresponding permutation to be computed from.
5. **Rotor** – Single letter translation, while using the Translator computation at a specific direction, while taking into account Rotor offset and setting. Also provides notch checking and Rotor advancing functions.
6. **Enigma** – The complete machine configuration and ciphering process, and Rotor/Pairs selections. Notch checks and Double stepping are taken into account here.

Task 5 – Decryption process

The message is transmitted as - $G \parallel K \parallel [2 \text{ random letters}]R \parallel M$

G – Ground setting

K – Message key

R – Identification group

M – Encrypted message

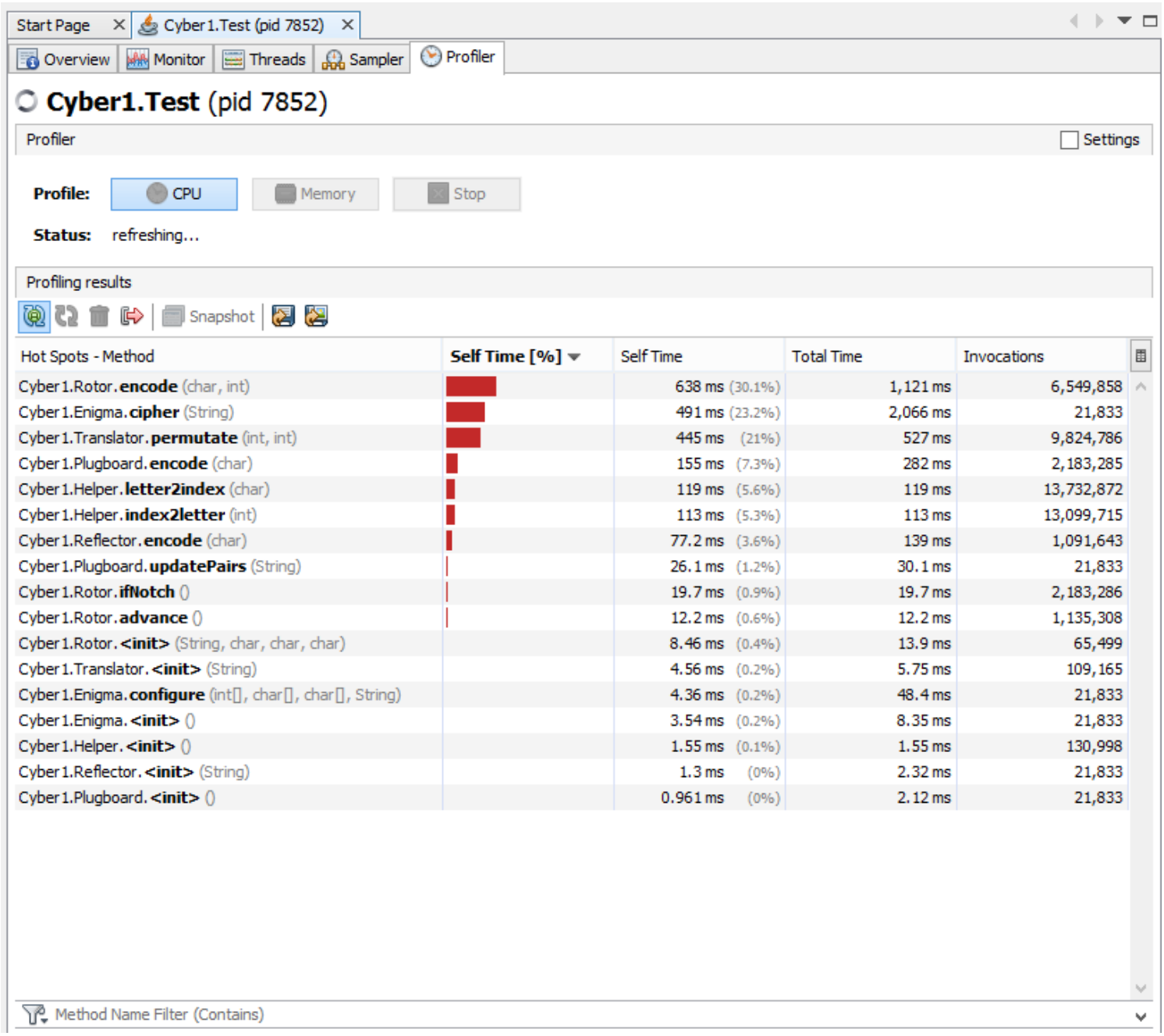
Decryption process:

1. The emulator will read the transmitted message and will split the message by spaces to an array of strings.
2. Use the first string, which is G, to set the machine to the ground setting, and set the machine configuration to October 29th according to the sheet provided.
3. Decrypt the next string, which is K, using the current configuration – E(K,G), to receive the new group setting.
4. Set the new ground setting, E(K,G), for the machine configuration.
5. Proceed to the third string to verify the 3 last characters in that string, and compare them to the machine configuration of October 29th according to the sheet provided.
6. Decryption will begin from the 4th index to the end of the string.
7. The output of the emulator is: **GROUP SOUTH COMMA NDFRO MGENP AULUS XSIXT HARMY ISENC IRCLE DXOPE RATIO NBLAU FAILE DXCOM MENCE RELIE FOPER ATION IMMED IATEL Y**

After logical repositioning:

GROUP SOUTH COMMAND FROM GEN PAULUS X SIXTH ARMY IS ENCIRCLED X OPERATION BLAU FAILED X COMMENCE RELIEF OPERATION IMMEDIATELY

Task 6 – Profiling Summary



Hot Spots - Method	Self Time [%]	Self Time	Total Time	Invocations
Cyber1.Rotor.**encode** (char, int)		638 ms (30.1%)	1,121 ms	6,549,858
Cyber1.Enigma.**cipher** (String)		491 ms (23.2%)	2,066 ms	21,833
Cyber1.Translator.**permutate** (int, int)		445 ms (21%)	527 ms	9,824,786
Cyber1.Plugboard.**encode** (char)		155 ms (7.3%)	282 ms	2,183,285
Cyber1.Helper.**letter2index** (char)		119 ms (5.6%)	119 ms	13,732,872
Cyber1.Helper.**index2letter** (int)		113 ms (5.3%)	113 ms	13,099,715
Cyber1.Reflector.**encode** (char)		77.2 ms (3.6%)	139 ms	1,091,643
Cyber1.Plugboard.**updatePairs** (String)		26.1 ms (1.2%)	30.1 ms	21,833
Cyber1.Rotor.**ifNotch** ()		19.7 ms (0.9%)	19.7 ms	2,183,286
Cyber1.Rotor.**advance** ()		12.2 ms (0.6%)	12.2 ms	1,135,308
Cyber1.Rotor.**<init>** (String, char, char, char)		8.46 ms (0.4%)	13.9 ms	65,499
Cyber1.Translator.**<init>** (String)		4.56 ms (0.2%)	5.75 ms	109,165
Cyber1.Enigma.**configure** (int[], char[], char[], String)		4.36 ms (0.2%)	48.4 ms	21,833
Cyber1.Enigma.**<init>** ()		3.54 ms (0.2%)	8.35 ms	21,833
Cyber1.Helper.**<init>** ()		1.55 ms (0.1%)	1.55 ms	130,998
Cyber1.Reflector.**<init>** (String)		1.3 ms (0%)	2.32 ms	21,833
Cyber1.Plugboard.**<init>** ()		0.961 ms (0%)	2.12 ms	21,833