ISM Assignment 1

You have breached the adversary database and got its password hashvalue. The hash value is given in the attached file (check the table for your name)

You know that your adversary is using one of the most 10 million used passwords available here https://weakpass.com/wordlist/1935 (ignis-10M.txt)

You also know that they are using a technique that will make your rainbow tables useless because they add “ismsap” as a prefix to all user passwords and after that they hash them 2 times using MD5 (1st run) and SHA 256 (2nd run). The output from the MD5 step is hashed again with SHA 256.

Write a simple Java application that will brute force the adversary password. The Java solution should contain a single .java file. **The package name must contain your name**. The Java solution must print the corresponding password at the console.

Benchmark the solution by printing the number of milliseconds require to do this. To measure the performance, you can use the next sequence

```
long tstart = System.currentTimeMillis();
//do the brute force
 long tfinal = System.currentTimeMillis();
System.out.println("Duration is : " + (tfinal-tstart));
```

When you upload the solution fill up the response box with

- **The password**
- **The duration in miliseconds**

All the solutions will be cross-checked with MOSS from Stanford. Solutions with a similarity of more than 50% will be canceled.