ISM Challenge 1 – November 1st, 2020

You have breached the adversary database and got their hash values. The hash is given a hexa string on Sakai. Check the assignment.

You know that your adversary is using one of the most 10 million used passwords available in the file that you received with the challenge

You also know that they are using a technique that will make your rainbow tables useless because they add the “*ismprefix*” salt with PBKDF2WithHmacSHA1 algorithm with 200 iterations. The generated hash value has the same size as the given one.

Write a simple Java application that will brute force the adversary password. **The Java solution should contain a single .java file.**

Benchmark the solution by printing the amount of milliseconds require to do this. In order to measure the performance you can use

```java
long tstart = System.currentTimeMillis();

//do the brute force

long tfinal = System.currentTimeMillis();
System.out.println("Duration is : " + (tfinal-tstart));
```

All the solutions will be cross-checked with MOSS from Stanford. Solutions with a similarity of more than 50% will be canceled. Only compiler-free solutions will be taken into account.