Lab 2 (Due Feb 9th)

The MD5 algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. Suppose you were able to access a password file containing the following six entries, i.e., each entry is the MD5 hash value of a password.

```
6f047ccaa1ed3e8e05cde1c7ebc7d958
275a5602cd91a468a0e10c226a03a39c
b4ba93170358df216e8648734ac2d539
dc1c6ca00763a1821c5af993e0b6f60a
8cd9f1b962128bd3d3ede2f5f101f4fc
554532464e066aba23aee72b95f18ba2
```

Could you design a Java program to conduct a *dictionary attack* on these passwords? What are these passwords? How long does your program take to find these passwords? A sample output of your program may look like:

The password for hash value 6f047ccaa1ed3e8e05cde1c7ebc7d958 is 181003, it takes the program 0.012 sec to recover this password
The password for hash value 275a5602cd91a468a0e10c226a03a39c is xxxxxx, it takes the program 0.02 sec to recover this password
The password for hash value b4ba93170358df216e8648734ac2d539 is xxxxxx, it takes the program 0.2 sec to recover this password
The password for hash value dc1c6ca00763a1821c5af993e0b6f60a is xxxxxx, it takes the program 1.2 sec to recover this password
The password for hash value 8cd9f1b962128bd3d3ede2f5f101f4fc is xxxxxx, it takes the program 2 sec to recover this password
The password for hash value 554532464e066aba23aee72b95f18ba2 is xxxxxx, it takes the program 12 sec to recover this password

You may want to try different password dictionaries available on the Internet. While you are submitting your solution, please upload on D2L the Java program and the password dictionary you used.