Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 2

Subject:	Hash Function and Digital Signature
Language:	Java
Due Date:	21/11/2017 - 23:59
Advisors:	Assoc. Prof. Dr. Ahmet Burak Can, Dr. Ali Seydi Keçeli

1 Experiment

You are expected to develop a file integrity checking tool. The program will monitor the changes on a specified folder. The program must keep track of all changes, such as deleting, altering and creating the files in the monitored folder and record all these changes to a log file. The requirements are below:

- The program must be developed as a console application.
- The program should be run as follows:

  integrity start -p P -r R -l L -h H -k PriKey PubKey -i #

  * *-p* specifies the path of the folder that will be monitored by the program.
  * *-r* specifies the path of the registry file.
  * *-l* specifies the path of the log file.
  * *-h* specifies a hash function, which can be MD5 or SHA-512.
  * *-k* specifies the path of the private and public key files.
  * *-i* specifies interval time.

  After starting the program, it must create the registry file specified by *-r* parameter. The registry file stores the path of all files in the monitored

folder specified by *-p* parameter and hash values of their contents which is calculated by using the hash algorithm specified by *-h* parameter. The format of registry file is as follows:

```
path/to/file1 hash value of file1
path/to/file2 hash value of file2
path/to/file3 hash value of file3
. . .
##signature: signed hash value
```

The last line of the registry file contains a signed hash value, which is obtained by calculating the hash value of all the content of registry file except the last line and then by signing the hash value with the key specified by *-k* parameter. When creating this signature, RSA algorithm (2048 bits) should be used.

As a last operation, the program should add itself to UNIX system's periodical tasks. This task should run the program in every # minutes which is specified by *-i* parameter in the following format:

```
integrity -p P -r R -l L -h H -k PubKey
```

When this task is executed, the registry file must be verified before opening. If the verification process is failed, it must be recorded to the log file specified by *-l* parameter as follows:

```
time stamp: verification failed
```

If the verification process is successful, the changes in the folder are written to the log file as follows:

```
time stamp: path/to/file type
```

In this log line, the formats of the *time_stamp* and the *type* values are as follows:

* *time stamp:* → dd-MM-yyyy HH:mm:ss
* *type* → deleted, altered or created

- The periodic task of the program should be stopped with the following command:

```
integrity stop
```

2 Notes

1. You can ask questions about the experiment via Piazza group (piazza.com/hacettepe.edu.tr/fall2018/bbm465).

2. Late submission will not be accepted!

3.You are going to submit your experiment to online submission system:
www.submit.cs.hacettepe.edu.tr

The submission format is given below:
<Student_id>.zip
−src/
−−*.java
−report/
--report.pdf