Homework 8

August 2, 2018

1 Purpose

This homework tests your ability to implement digital signature and cryptographic hash using Java. You will use mainly the classes in `java.security` package for your implementation.

2 Instructions

2.1 Digital signature

For this problem, you will finish a partially completed program (`Sig` class) to generate public and private key pairs and to sign a plaintext message using private key and verify the signature using public key.

In particular, you implement the following constructor and methods in the `Sig` class.

1. `Sig` constructor, where you initialize the fields `keyGen`, `keyFactory`, and `signature`.
2. `initKeyPair` method, where you initialize the `keyPair` field.
3. `getPublicKey` method, where you return the public key of the key pair as a string.
4. `getSignature` method, where you return the string encoding of the digital signature of a message.
5. `verify` method, where you verify the signature of a message given a public key.

Sample output If you run the provided main method, you should expect output of the following shape. Note that the first public key (generated) and signature should be different each time you run the program.

```
public key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFK4SUuhgDSgFCFsmz3D+Fujue1DbGktEJKVNS
hmfiZ0r04PGyJ75Irh3bOHrSmKknKIcGXa8O2acO4a5G0HrKim/7gkiCVonnrwcXau4hPs4aZ2hD7NfdoMJ6bkWN
/QMPgdKVfuEMZJIxaTW5eLLfnr67Lale31VO35KawAtdAQIDAQAB

signature: dc9HHQsNAYOJSHjVd1eBFQ3TBR6/++GMbbAvYxQ1LAohbM8BatQJSWD+q6CIRfRrp02Kz2jUjunDf
Fgsp5UrlPWkc30WhZ66iJ781PhYGpmDXxDXTipkObkGeymggAUnY8oEmHuLnWTmh7bSR9A/RgrxwoVVbsJAZ6Uza
cZJdpA=

signature is verified: true

public key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChBA91S3XSUYILZyhu5ilsiDjmzOZn830xxUEP
LpeLQwr2BeLAtlCBqzihUcr5lGr9YvLN/jOta0TnEpQoa6kJYbUPnAZinh8E2Q4COfSx4Js3+TC64AD2yvlLaGOs
BrDaBN15OGq9k2FgfxzxepVEPBW6DKHCeDQqPQAO8/UDXwIDAQAB

signature: VvLONhPbhkzhmR3Z5v4WQfleSm8CR1CLwDWXjDGu4NhzN6L7n7zJBxj+z6WT8W3hb2Le69gKO2WIy
/7kNvfqOTE6hOGz68YB0idZoATB2C7m9dSjRcdL0nYxThoPrfZXVDuMVuSpDo2We/M/8a4oCAPzjCopaCsDtTac+
ZcL7/w=

signature is verified: true
```

2.2 Cryptographic hash function

For this problem, you will implement the main method of a Java file `Digest.java`, where the main method will compute and print the hash digest of the string "test message to be hashed" using SHA-256 algorithm. You should use the class `MessageDigest`.

Sample output You should generate the following output

```
The digest of "test message to be hashed" is
  uXi/fCgWC8h6cv0FKBKpemeyerRH1hAT9+HiwOu5dm4=
```

3 Requirements and Grading

Please make sure that your code does not have compilation errors and it runs correctly.

File format Java source files.

Feedback This homework will be graded within a week after submission deadline using following rubrics.

Rubrics

	Correctness	**Style**
Exceed expectation	program has correct functionalities	program is implemented efficiently and has good style
Meet expectation	program has minor errors	program has minor efficiency issues or design errors
Do not meet expectation	program does not provide main functionalities	program has major design flaws or efficiency issues

Grading 10 points total for this homework.

4 Submission

You should submit your solution as java source files by the name of `Sig.java` and `Digest` to the dropbox.