Project #2 Report:

In this project, we have used certificate in sslcert.zip. If you want to test the application using this SSL certificate, the information of the certificate is as follows:

* Password: private
* Country name: MA
* State or province name: Ifrane
* City of Locality: Ifrane
* Organization Name: AUI
* Organizational Unit: AUI
* Common Name: Meryem
* Email Address: meryemmhamdi1@gmail.com

To test this application, please add the jar files included in the folder: bcprov-jdk15-1.46.jar and bcmail-jdk15-1.46.jar to the project class path.

The main menu serves as a linking point between frame that signs files and the frame that verifies the signature. If you click on sign file or verify signature, you can get back to the main menu by clicking again on go back to main menu button in both frames.

We used in signing file in PKCS7 format, p12 file (name-cert.p12), which contains the private key, certificate and other information needed to ensure the conversion and storage of both the file and its signature in PKCS7 format. A PKCS7 file (.pk7) is created in the same location as the original file to be signed.

To verify the signature of the file, we used p12 file, which contains the public key. The user must select PKCS7 file location and provide the password corresponding to the chose p12 file as well. After clicking on verify signature button, the user can see either a message saying “the signature verifies to true” in blue or a message saying “the signature verifies to false” in red. A document called document\_non\_signer.txt is generated as a result of the verification. It is found in the java project path (in the project folder in workplace).