ISM Challenge 2

Your company require a safe way to communicate by encrypted emails. You need to develop a PGP like system in which you will use X.509 certificates to authenticate between parties and to exchange AES random generated keys used to encrypt the emails.

Considering that messages/emails are text files the system must allow users to

- Digitally sign the encrypted messages
- Use destination public certificate to send them the password used to encrypt the message

Using the given files, implement a Java application that will

1. Decrypt the "**Session.key**" file that contains a string based key for AES. The key has been encrypted using your public key from "**studentCertificate.cer**" with RSA in ECB mode with PKCS1 padding. The associated private key is in the "studentstore.ks" (the store pass is **passks** and the key password is **passism1**; the key alias is **private1)**
2. Using the AES key, decrypt the original message received from ISM. You received 3 encrypted messages but the original one is the one for which the digital signature checks (for the plaintext message). The digital signature is given in the "***signature.ds***" file (the signature is generated using MD5 with RSA). The file was encrypted with AES in CBC mode with PKCS5 padding. The IV is known and has a default value of 0x01010101…….01.
3. Reply to the original message by sending a response file "**response.enc**" which contains your name and the answer to the original question. The response should be encrypted with the same password and the same AES (CBC with the given IV). Along with the response send its digital signature, in the "***response.ds***" file. The destination should be able to check the signature of the plaintext response with your public key from "***studentCertificate.cer***".

The Java solution should contain a single .java file.

All the solutions will be cross-checked with MOSS from Stanford. Solutions with a similarity of more than 50% will be canceled.