/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

***Comments:***

.The execution is available from jdk version 14

To run program easy - double click on run.bat - (the command wrote in run.txt)

After creating the keystores - the files were copied to the projects.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\

***Encryption***:

The encryption program reads data from plaintext.txt , signs the Data a-symmetrically using ."sha256withrsa" algorithm and saves the signature in conf.txt file

It encrypts the data with symmetric key using AES algorithm , CTR mode without padding, and saves an encrypted version of key in conf.txt using RSA algorithm. (gets the public key from decrypts certificate witch was imported to keystore.)

As well conf.txt will include the IV of the symmetric key .The output of this program will be encrypted.txt with represents the plaintext encrypted. We chose working with the CTR mode instead of CBC because some issues we had with the signature verification - the CTR mode solved this issue.

***Decryption***:

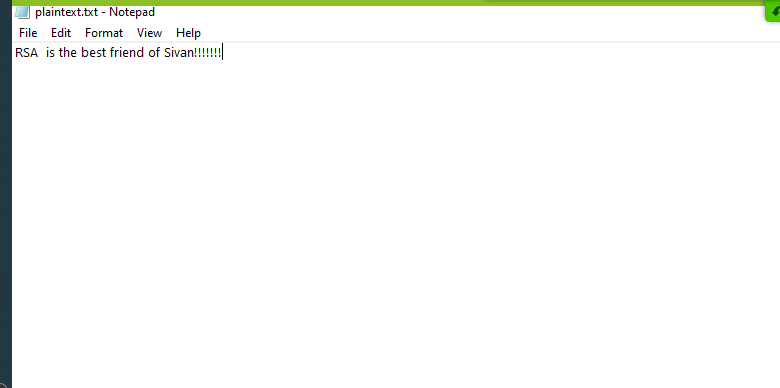
.The decryption program reads as input the encrypted.txt and conf.txt

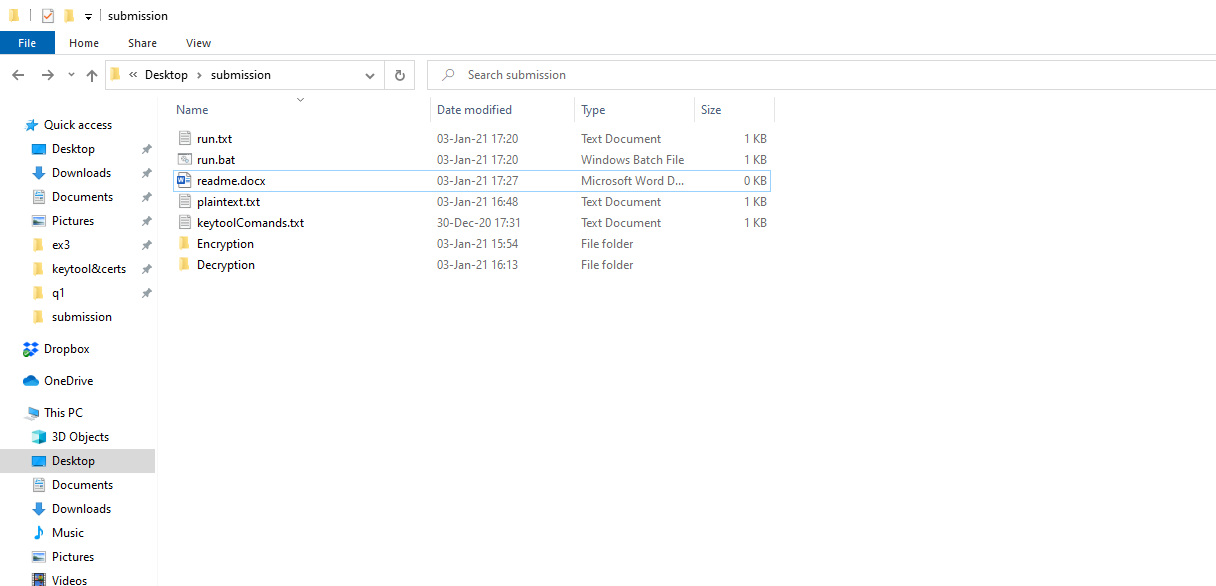
From conf.txt it decodes the signature bytes , IV bytes and encrypted symmetric key bytes ,thus he can decrypt the symmetric key using Decryptor RSA private key and the data itself. (using same algorithms and modes as above).

It verifies the signature using the Encrypts certificate public key with the encrypted data - on match will create as output decrypt.txt file otherwise prints error.

***Execution Example:***

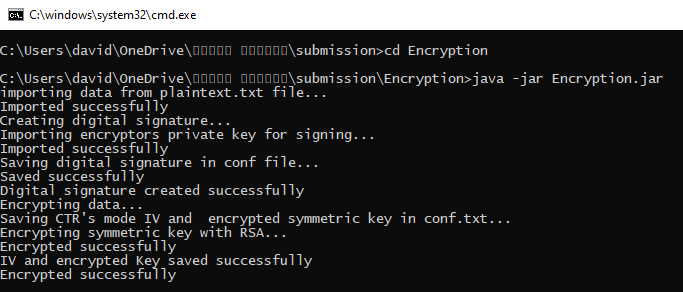
Before executing:

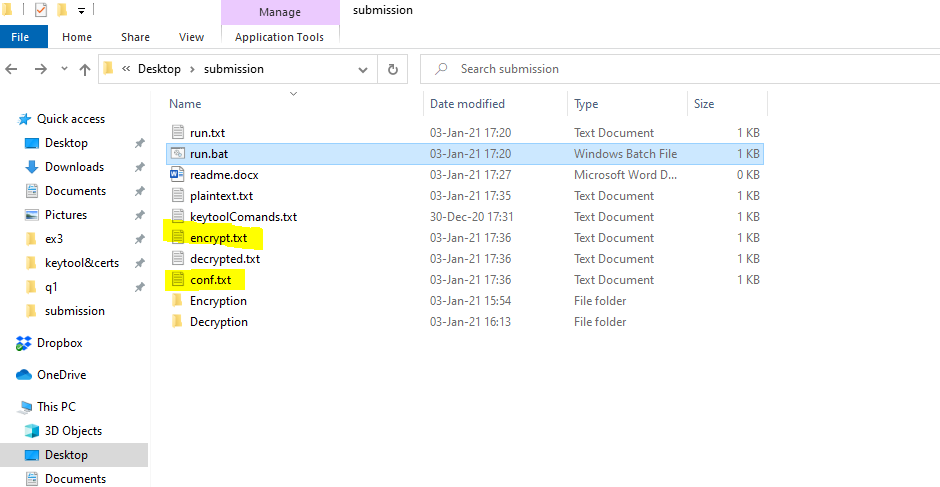




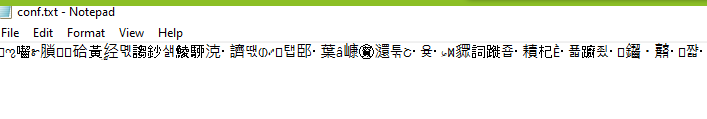
Clicking on run.bat :

Encryption part :

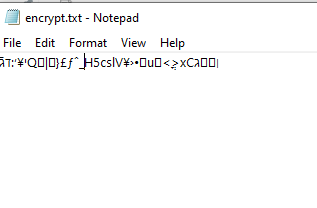




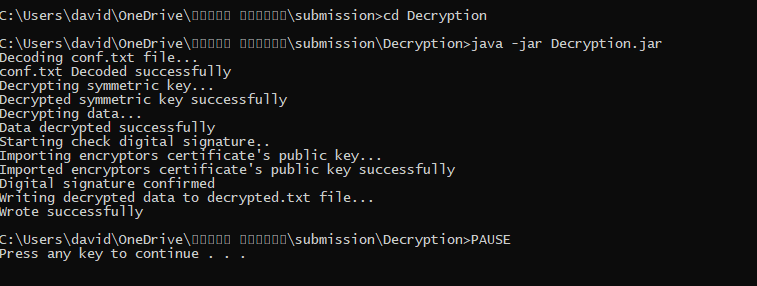
conf.txt:



encrypt.txt:



Decryption part:



decrypt.txt:

