JAVA Crypto API - Exercise

# Submitting

Limor Frost 302675772

Elad Spira 200732618

# The Commands that we were using to create the KeyStore files

keytool -genkeypair -alias encryptKeys -keyalg RSA -keypass encPass1 -keystore C:\Keys\EncryptKeyStore.jks -storepass encPass2 -dname "cn=Limor Frost, ou=TAU, o=TAU-CS, c=IS" -validity 360

keytool -genkeypair -alias decryptKeys -keyalg RSA -keypass decPass1 -keystore C:\Keys\DecryptKeyStore.jks -storepass decPass2 -dname "cn=Elad Spira, ou=TAU, o=TAU-CS, c=IS" -validity 360

# The following providers were used

1) SunJCE contains valuable features such as "AES", "JCEKS", "RSA".

* The first is used for encrypting the raw data in blocks.
* The second is for handling the KeyStore.
* The third is used for asymmetric encrypting of the secret key.

2) SUN contains SHA1PRNG for generating the pseudo-random Initialization Vector.

3) SunRsaSign contains SHA1withRSA algorithm that was needed to encrypt and hash the signature.