CIS405/ Asymmetric Assignment/ Sp 18/ Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Part A.

1. Fill in the missing code found in the AsymmetricAssignment project so that it will encrypt and decrypt using RSA.
   1. The AsymmetricAssignment project is found in R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric\
   2. In the Encrypt method, write the code to retrieve the Public key found in R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric\CollinsPublicOnlyKey.xml
   3. Also in the Encrypt method, write the statement to encrypt plaintext and store the result in cipherBytes (a byte array you must create).
   4. In the Decrypt method, write the code to retrieve the Private key found in R:\CIS\CFJC\CIS498 Misc\Assignments\Asymmetric\CollinsPublicPrivateKey.xml
   5. Also in the Decrypt method, write the statement to decrypt cipherBytes and store the result in newPlainText (a byte array you must create).
   6. Use fOAEP padding for both encryption and decryption.
2. Encrypt your S# and store the result in a file named LastNameCipherText.txt
3. Save your file to S:\CIS\Collins-j\CIS405\Assignments\Asymmetric\LastNameCipherText.txt
4. Verify your program is working correctly running R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric\AssignmentCheckA.exe from your C:\ drive.
5. Turn in a copy of your source code.

Part B.

Use the RSAKeyExchange class to accomplish the following.

1. Decrypt the contents of file RijndaelSecretKeyEncrypted.txt. It is located at R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric. To decrypt RijndaelSecretKeyEncrypted.txt use the RSA key named StudentPublicPrivateKey.xml. Use RSA decryption with fOAEP padding.
2. Use the decrypted contents of RijndaelSecretKeyEncrypted.txt as a secret key to decrypt the file CipherTextFile.txt located at R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric.
   1. The decrypted file should be a docx.
   2. Use RijndaelIvInfo.txt located at R:\CIS\CFJC\CIS405 Misc\Assignments\Asymmetric for the IV.
   3. Use default mode and padding.
3. Print out the last page of the decrypted contents of CipherTextFile.txt and staple to the back of this sheet.
4. Turn in a copy of your source code.