Cryptography Homework 5c—Using RSA and AES together.

Public key encryption gives us a way to exchange keys securely, but it is very slow. Symmetric encryption is fast but has no method for secure key exchange. In practice, most systems use public key encryption to securely exchange a session key and then switch to symmetric encryption using that session key.

This exercise follows a variation of the technique that HTTPS in your web browser generally follows. It uses public key encryption (RSA in this case) to securely exchange a key (session key) that will be used in symmetric encryption. It then switches to AES symmetric encryption to transfer the data.

The lab follows the method used in the example, Encrypt data with RSA in the Pycryptodome documentation. <https://pycryptodome.readthedocs.io/en/latest/src/examples.html>

You will use the RSA public/private key pair you created in the last lab and give the public key to your partner. Your partner will create a session key, encrypt the session key with your public key, and give the encrypted session key to you. You should be able to decrypt the session key with your RSA private key. Finally, your partner uses AES and the session key to encrypt a file and send it to you. (Actually, your partner will give you the encrypted key and the AES data bundled into a single file.)

Note: If your course is entirely online, you can send the message to yourself instead of to a partner; your choice.

A picture containing indoor, object

Description automatically generated