The cryptographic system consists of Alice and Bob, who both use AES and RSA. Assuming Alice is sending to Bob, Alice will encrypt a message with a random 16-byte AES key. This AES key will then be encrypted itself using Bob's public RSA key. Then, a signature is created using SHA-256.

These three parts are all sent in a python pickle object. The RSA encrypted AES key, the ciphertext, and the signature are combined in a dictionary, serialized, and sent to Bob.

Bob receives these messages. He can then deserialize the pickle object and access the dictionary that includes all the information Alice sent. He uses his private RSA key to decrypt the AES key, then uses the AES key to decrypt the ciphertext into the message. Finally, he creates a signature to compare using the same parameters and method as Alice, SHA-256, and compares them.

In the case that Alice is sending to Bob

Alice	**Transmitted**	**Bob**
B = Load bob_public_key	…	…
M = Message	…	…
M = Pad Message	…	…
K = Random 16 Byte AES key	…	…
C = AES Encrypt M with K	…	…
E = RSA Encrypt K with B	…	…
MAC = SHA256(K + M)	E + C	Receive E + C
Send E + C	MAC	Receive MAC
Send MAC	…	Split E from C
…	…	B = Load bob_private_key
…	…	K = RSA Decrypt E with B
…	…	M = AES Decrypt C with K
…	…	If MAC is SHA256(K + M):
…	…	Authenticated
…	…	Else:
…	…	ERROR
…		

To run the program, open the command prompt in the folder containing all related files and enter either "python Alice.py" or "python Bob.py" where Alice or Bob sends the message respectively.