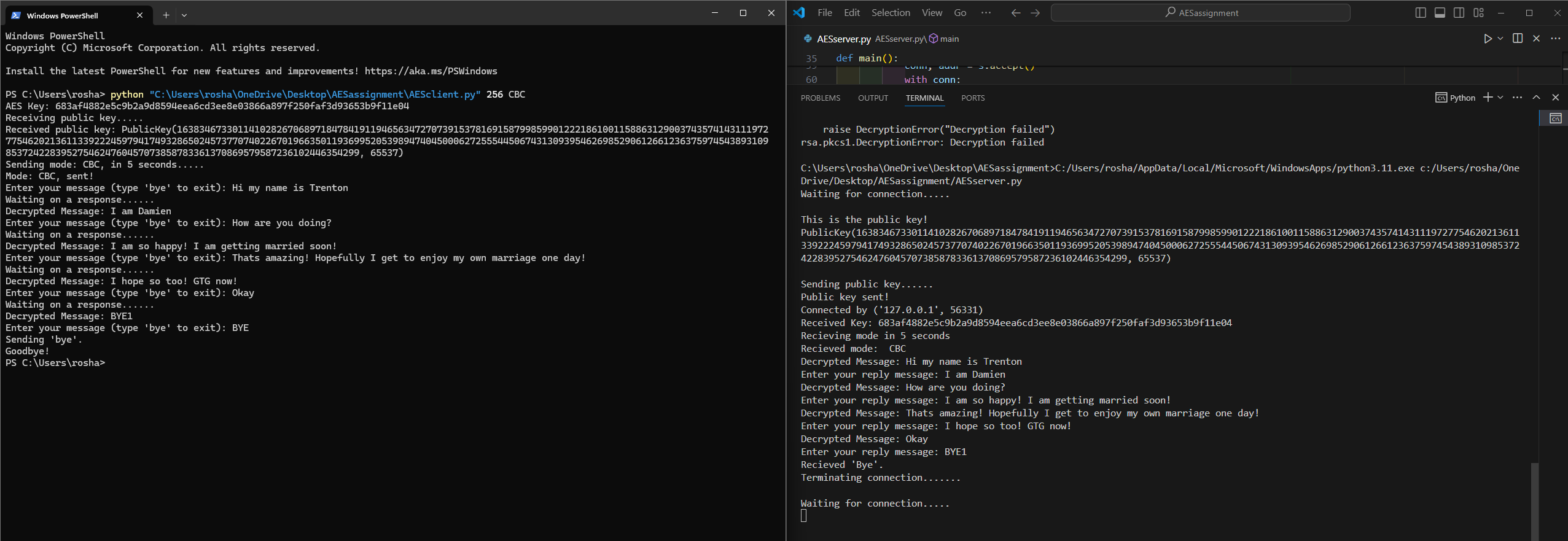
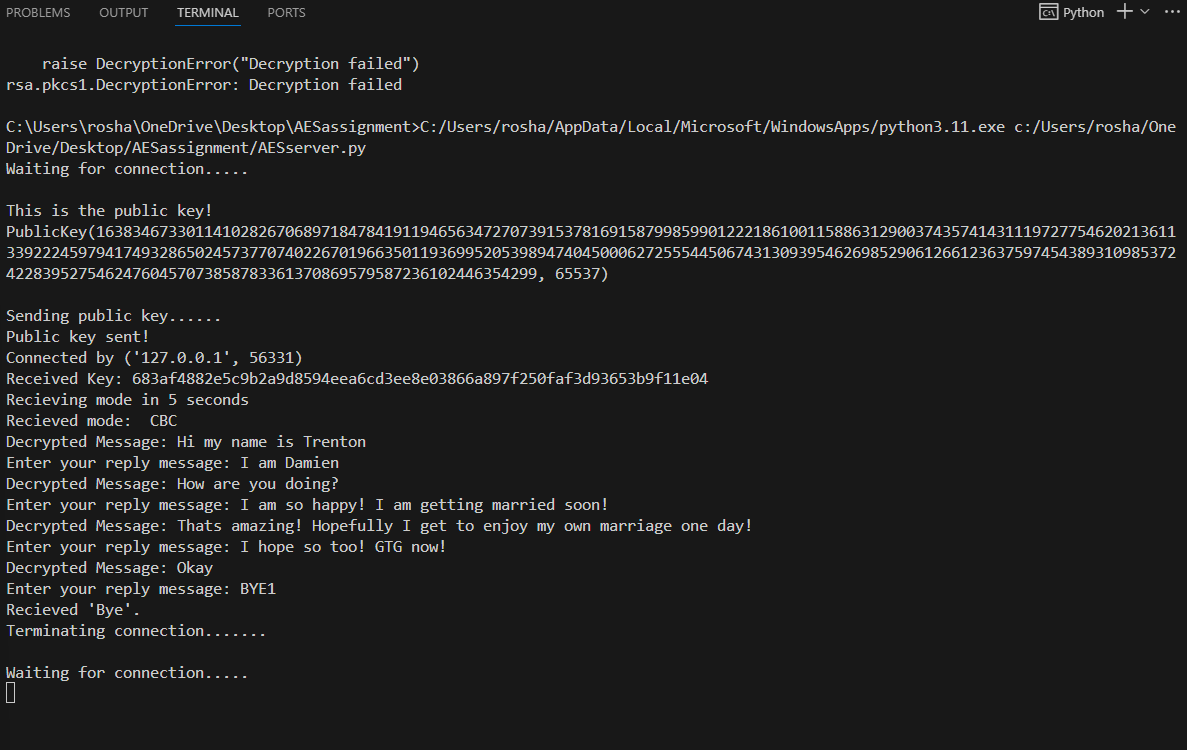
**What to submit?**

* Your well documented source code (Only .java and .py files).
  + Authors and description at the top
  + Comments within the code throughout the programs
* A Word document including
  + For each of the security properties below, explain if it is provided in this protocol:
    - Confidentiality: This program provides confidentiality in the form of encryption.
    - Message integrity: This program does not provide message integrity because digital signatures or message authentication codes are not used.
    - Source authenticity: The use of RSA encryption for key exchange ensures that the server's public key is used to encrypt the AES key, providing assurance that the key came from the intended source (the server). However, there is no explicit verification of the server's identity or authenticity beyond the key exchange mechanism. For stronger source authenticity, the server could provide a digital signature along with the public key.
    - Non-repudiation: Non-repudiation ensures that the sender of a message cannot deny having sent the message. The code does not include any mechanisms for non-repudiation, such as digital signatures with timestamps. Implementing non-repudiation would require additional steps such as signing messages with the sender's private key.
  + Screenshot of the key transport (Steps 1-7 above)

A screenshot of a computer screen

Description automatically generated

* + Screenshot of a chat of at least 3 messages between the client and server 
  + Screenshot of the end of the chat where client connection is closed, server is waiting for connections.



* + Answers to these questions:
    - If you worked with partner on this project, how did the group members contribute to the project? Did everyone fairly contributed to the work? I worked alone
    - What challenges have you faced when completing this assignment (other than arranging meeting times with the group members or other challenges about working in a group)? Learning the process and implementation of RSA and AES
    - How is the assignment helpful for you in understanding cryptographic algorithms? It helps me understand the process and components of the algorithm.
    - Any other comments/suggestions. It was difficult at the start. Maybe give us resources to give us ideas of the implementation.