Procedural report (project phase II)

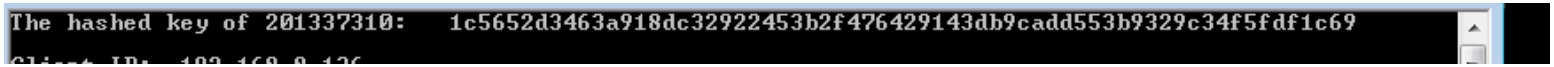
Name: Abdulwahab Hassan Alzahrani
ID: 201337310

Abstract

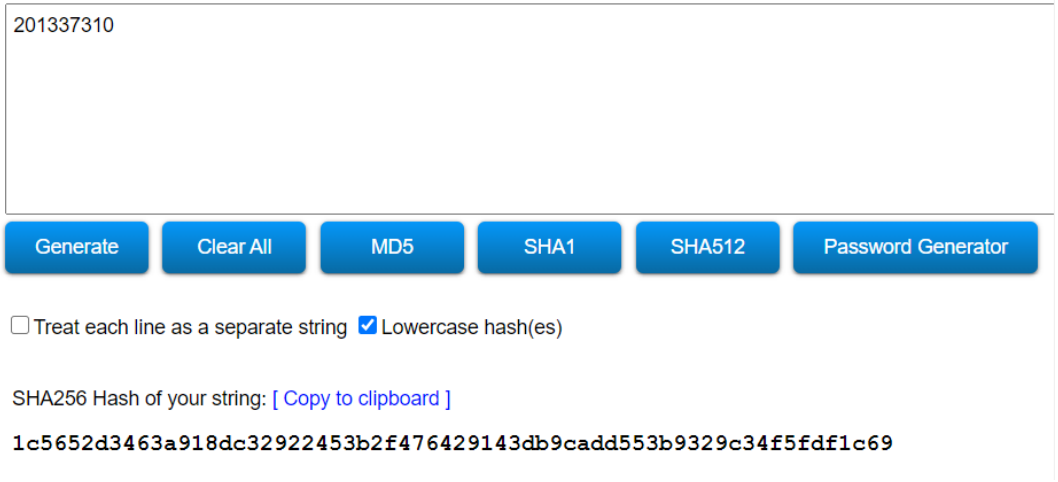
This report shows the procedural process of the encryption and the decryption of the exchanged messages between two sides (Client and Server) using AES_256_CBC.

The hashed key:

- The key is the 256-bit hash of 201337310 using Hash library in Python.
- Also, it was verified using sha256 online tool.

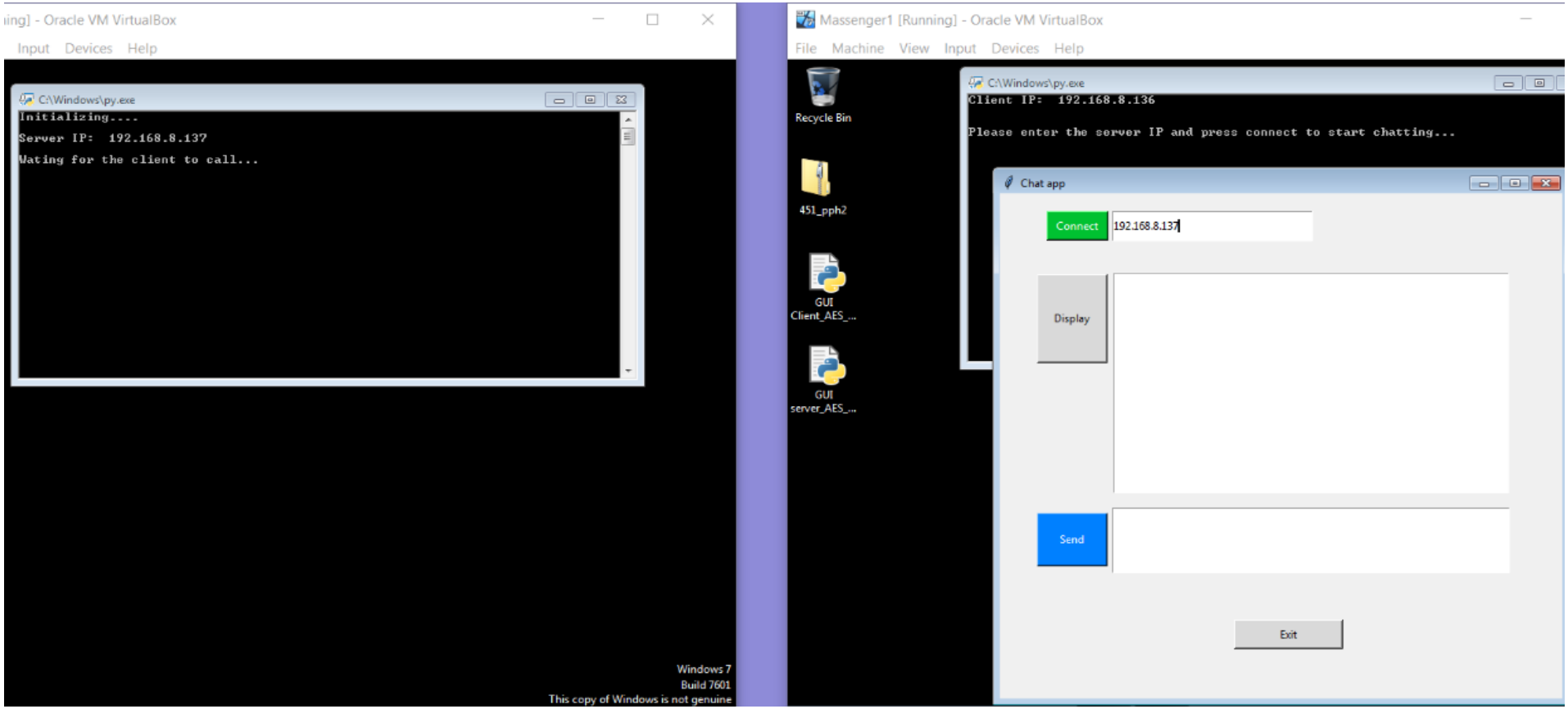


(Using python's Hash library)

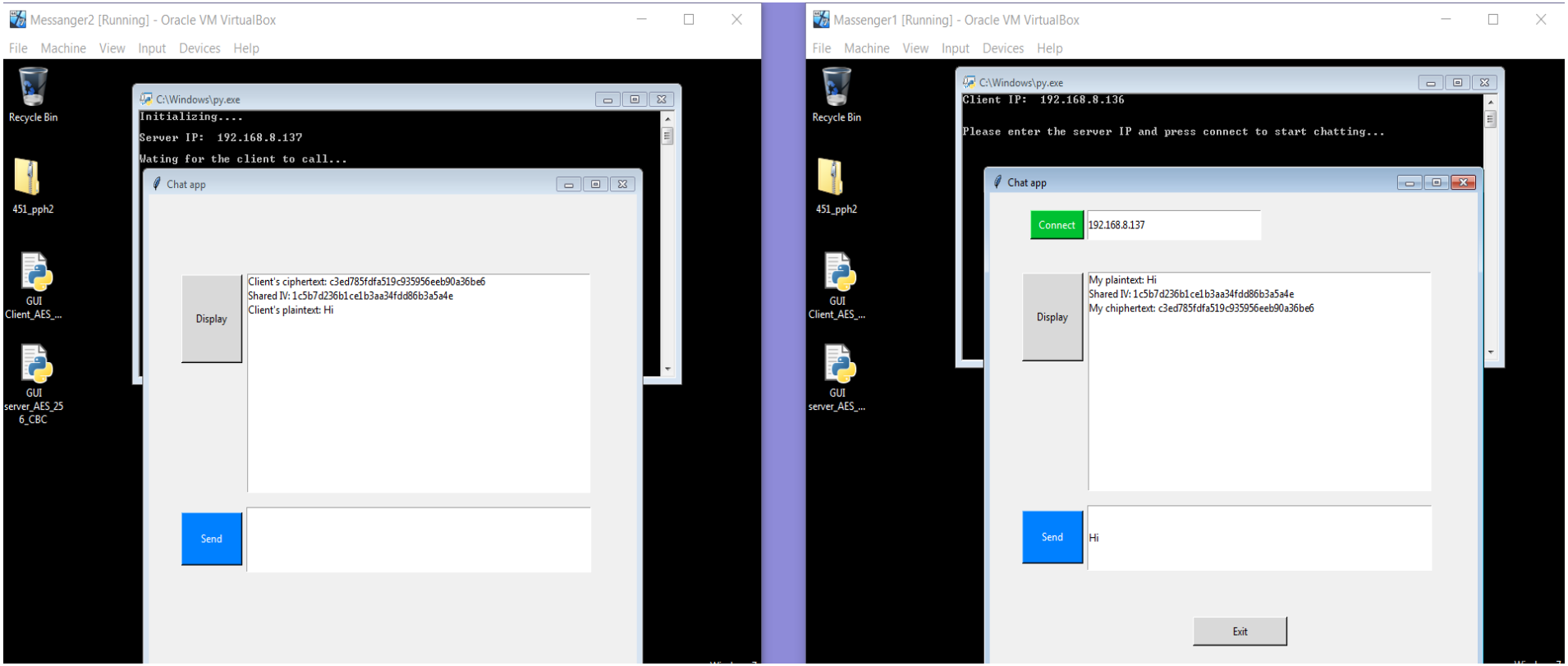


(Using the SHA256 online tool)

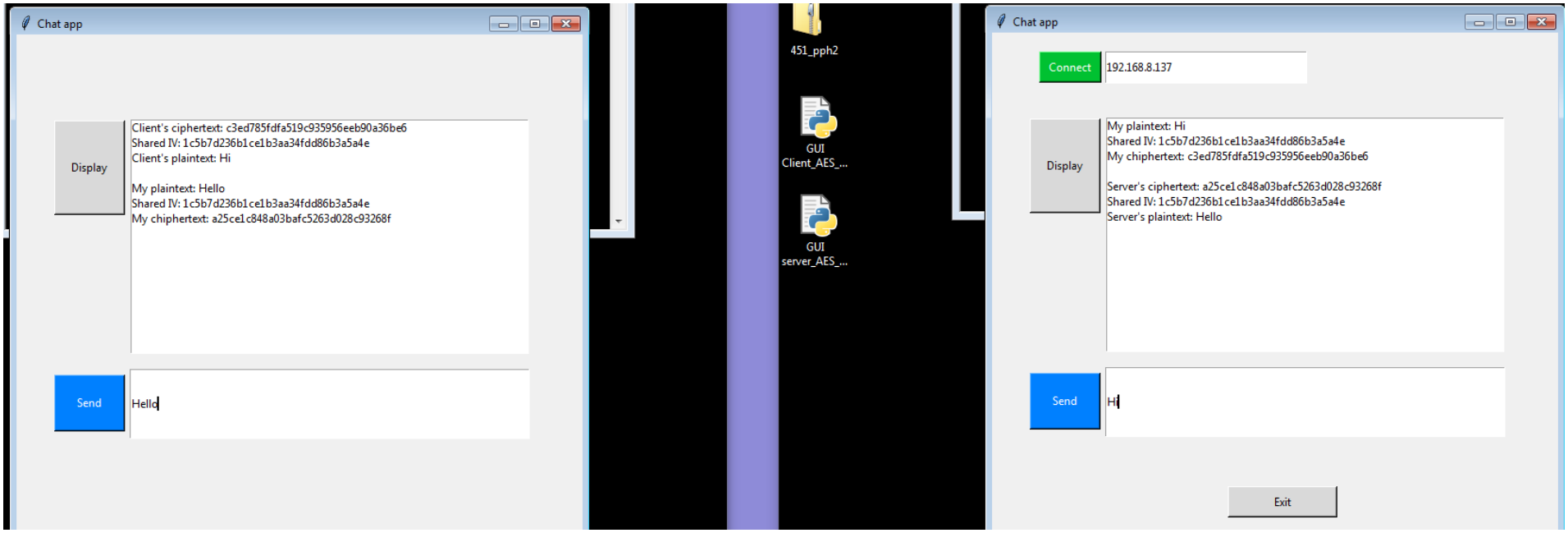
Testing: Chat session#1 (Left side: server, Right side: Client)



- Client side initiates the chat session by connecting to the server, when connect button is pressed the IV will be received by the server

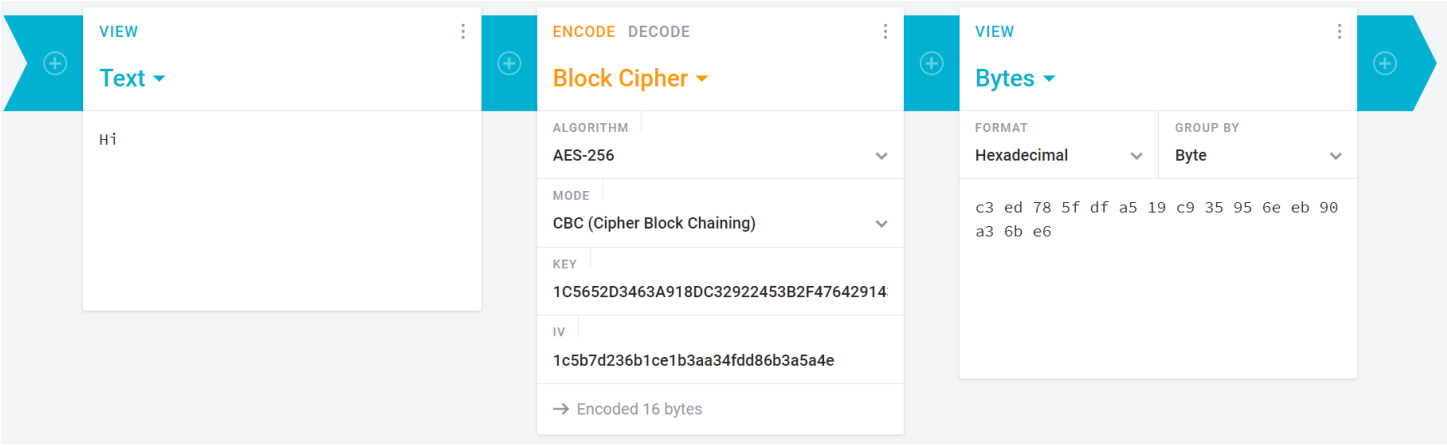


- When client side sends a message, in his chat window the following will be shown: the plaintext of his message, the shared IV and the ciphertext of his message.
- When Server clicks on display, in his chat window the following will be shown: the ciphertext of the client, the shared IV and the plaintext of the client.

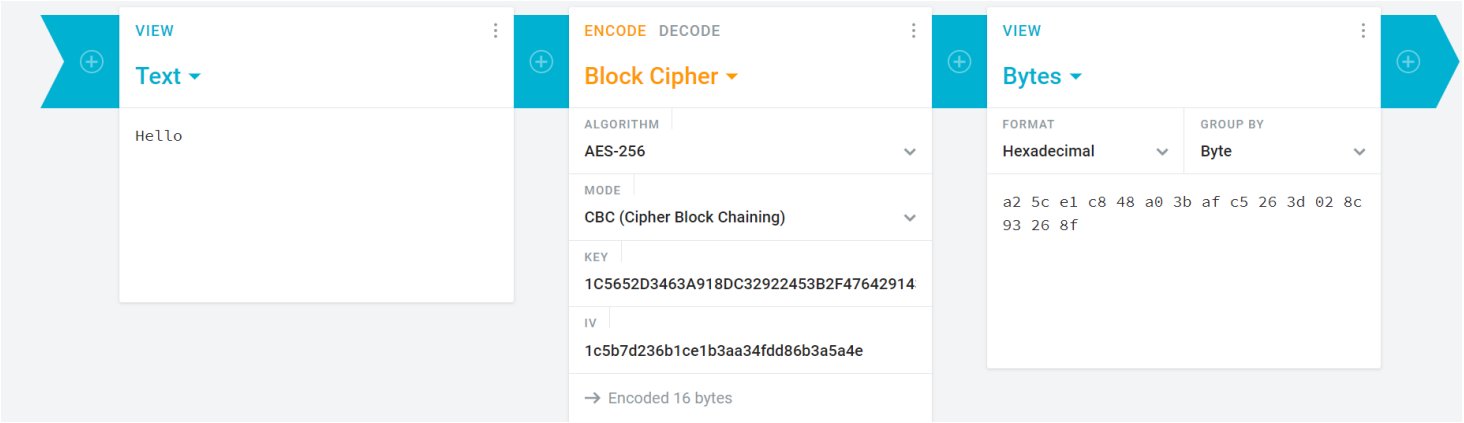


- When Server side sends a message, in his chat window the following will be shown: the plaintext of his message, the shared IV and the ciphertext of his message.
- When Client clicks on display, in his chat window the following will be shown: the ciphertext of the server, the shared IV and the plaintext of the server.

Verifying: Chat session#1

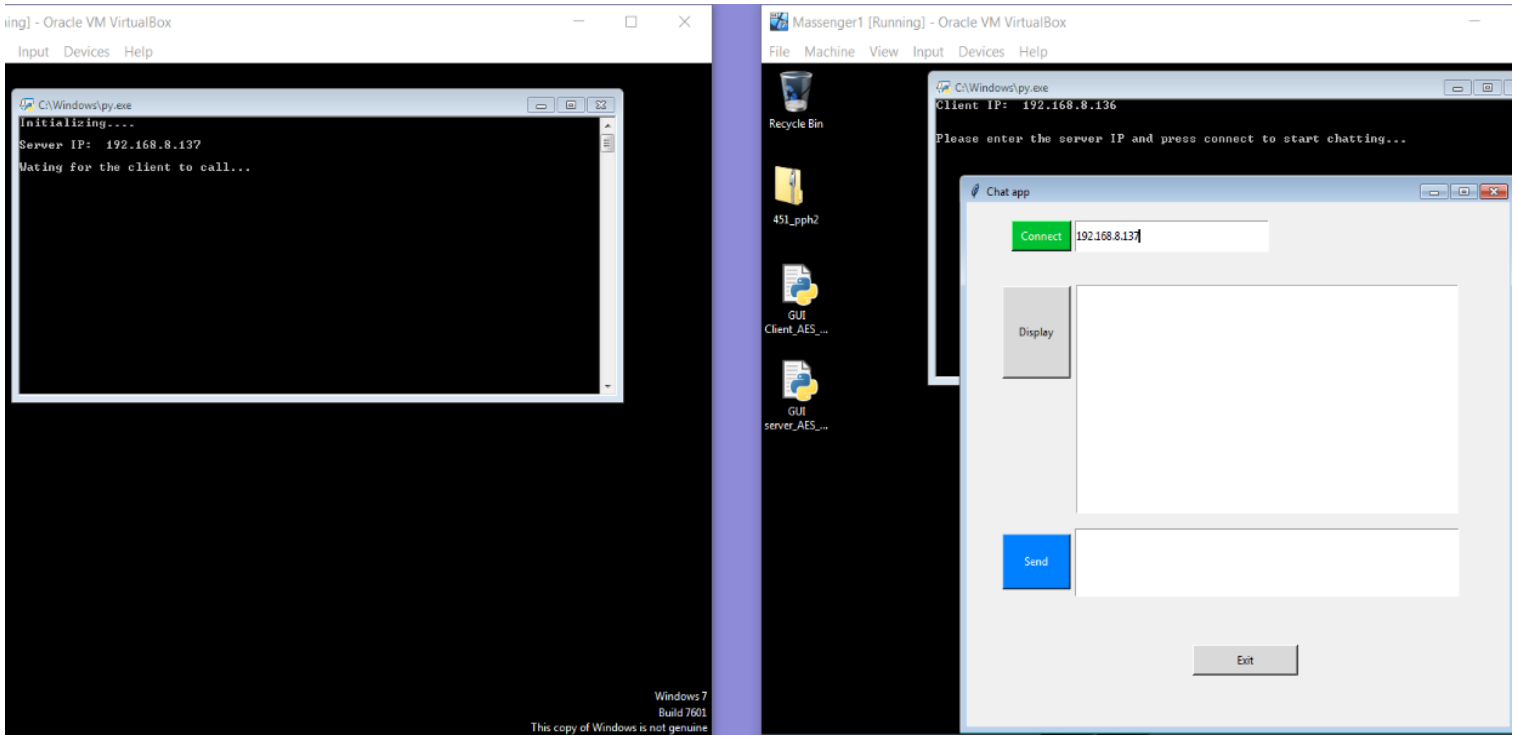


Client's ciphertext

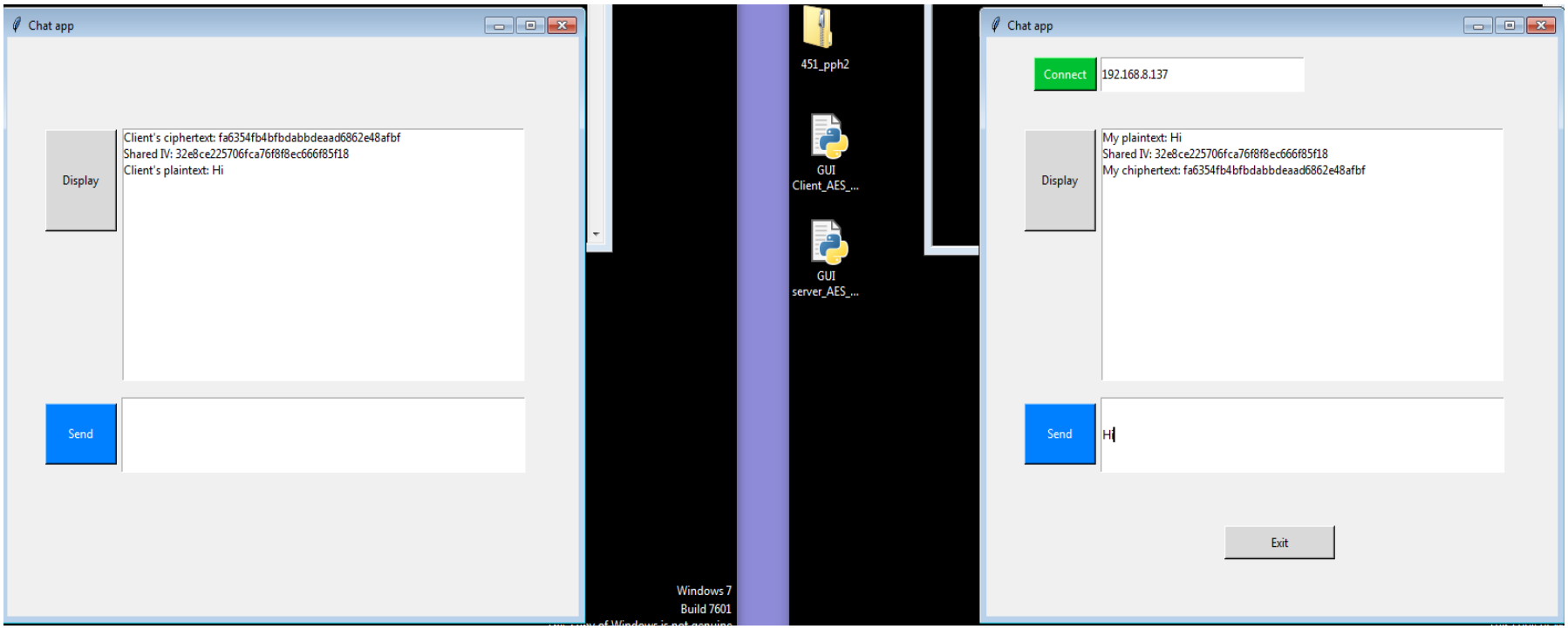


Server's ciphertext

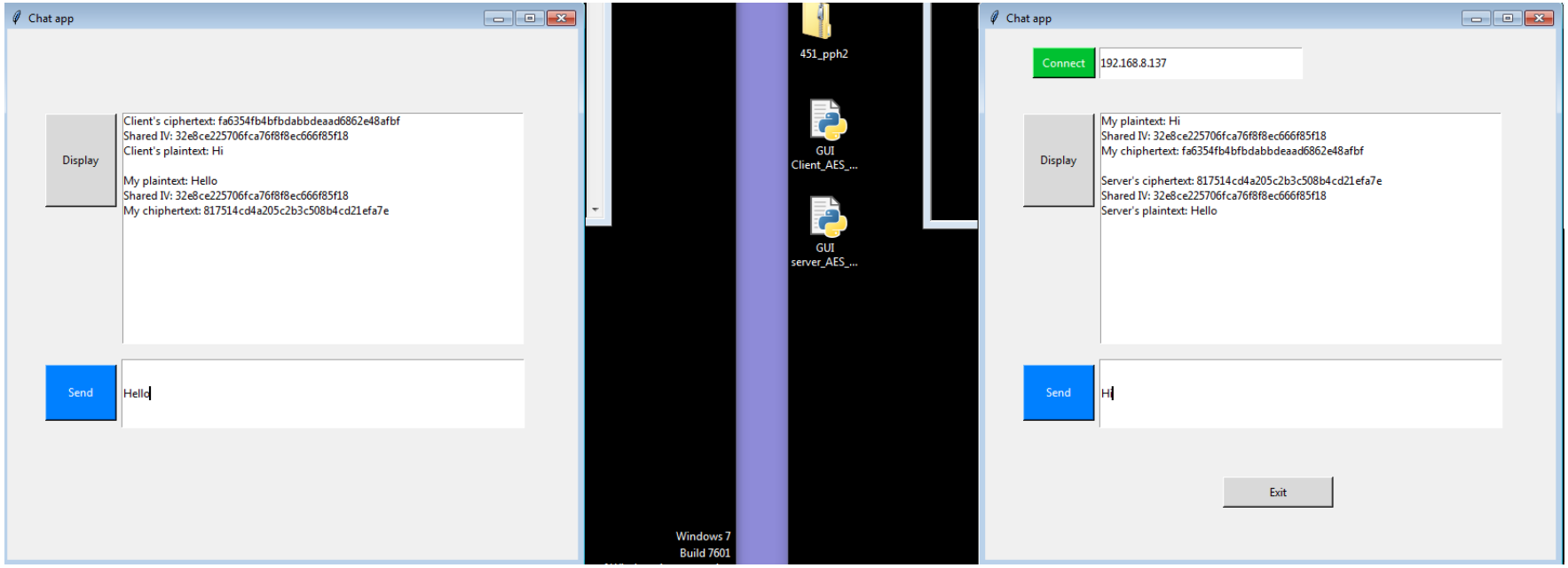
Testing: Chat session#2 (Left side: server, Right side: Client)



Client side initiates the chat session by connecting to the server, when connect is pressed the IV will be received by the server

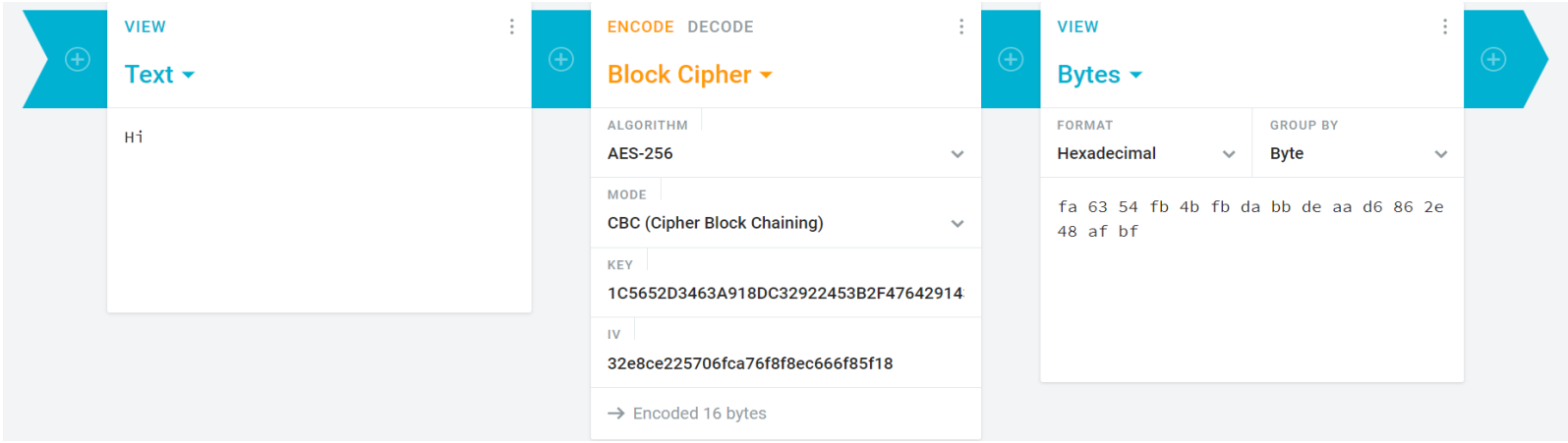


- When client side sends a message, in his chat window the following will be shown: the plaintext of his message, the shared IV and the ciphertext of his message.
- When Server clicks on display, in his chat window the following will be shown: the ciphertext of the client, the shared IV and the plaintext of the client.

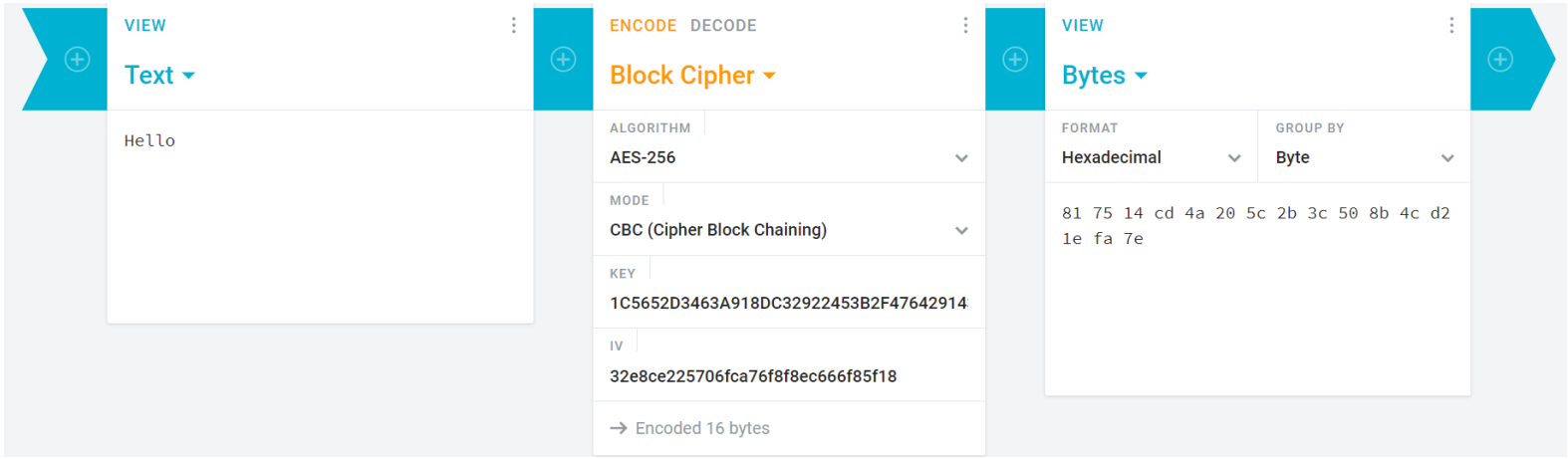


- When Server side sends a message, in his chat window the following will be shown: the plaintext of his message, the shared IV and the ciphertext of his message.
- When Client clicks on display, in his chat window the following will be shown: the ciphertext of the server, the shared IV and the plaintext of the server.

Verifying: Chat session#2



Client's ciphertext



Server's ciphertext