

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.

```
The hashed key of 201337310: 1c5652d3463a918dc32922453b2f476429143db9cadd553b9329c34f5fdf1c69
```

(Using python's Hash library)

201337310

Generate

Clear All

MD5

SHA1

SHA512

Password Generator

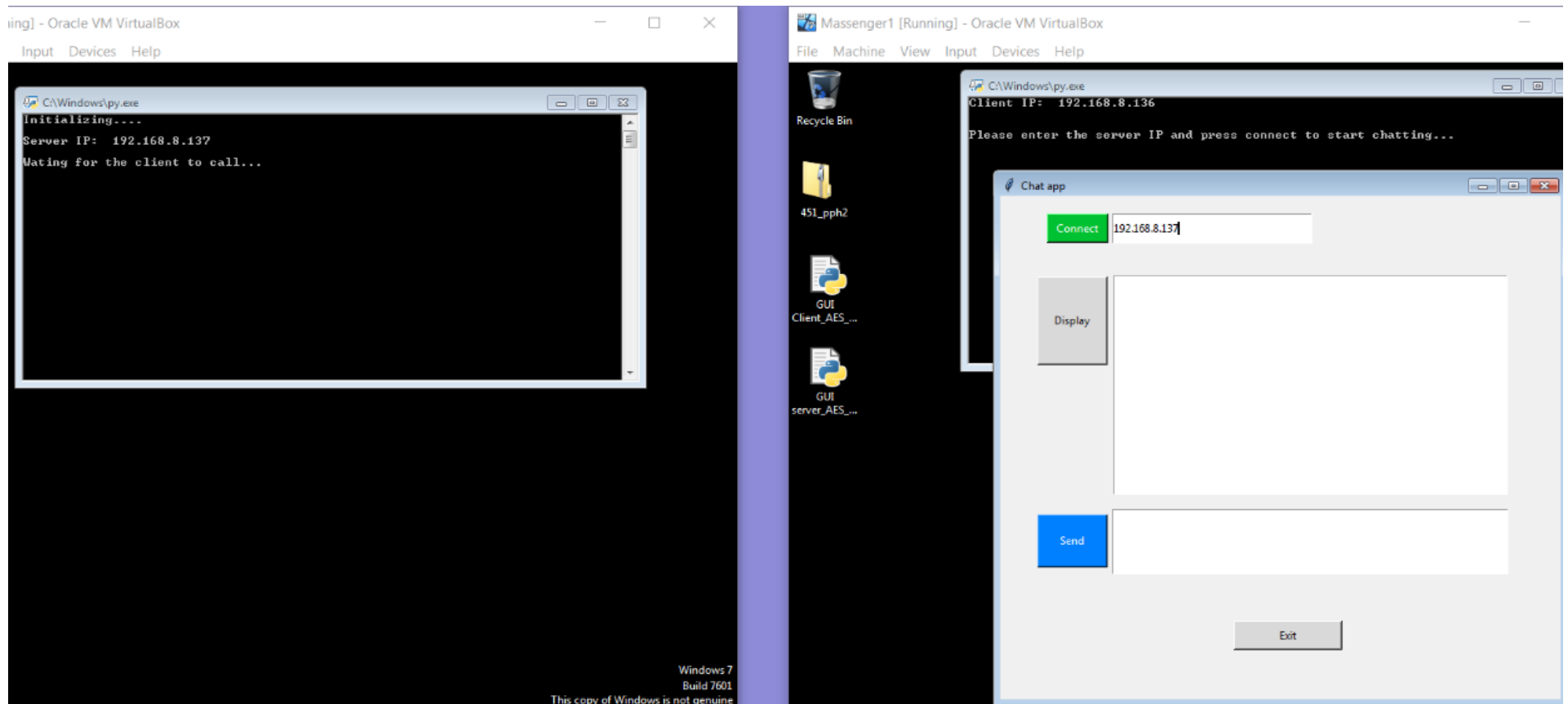
☐ Treat each line as a separate string ☒ Lowercase hash(es)

SHA256 Hash of your string: [\[Copy to clipboard \]](#)

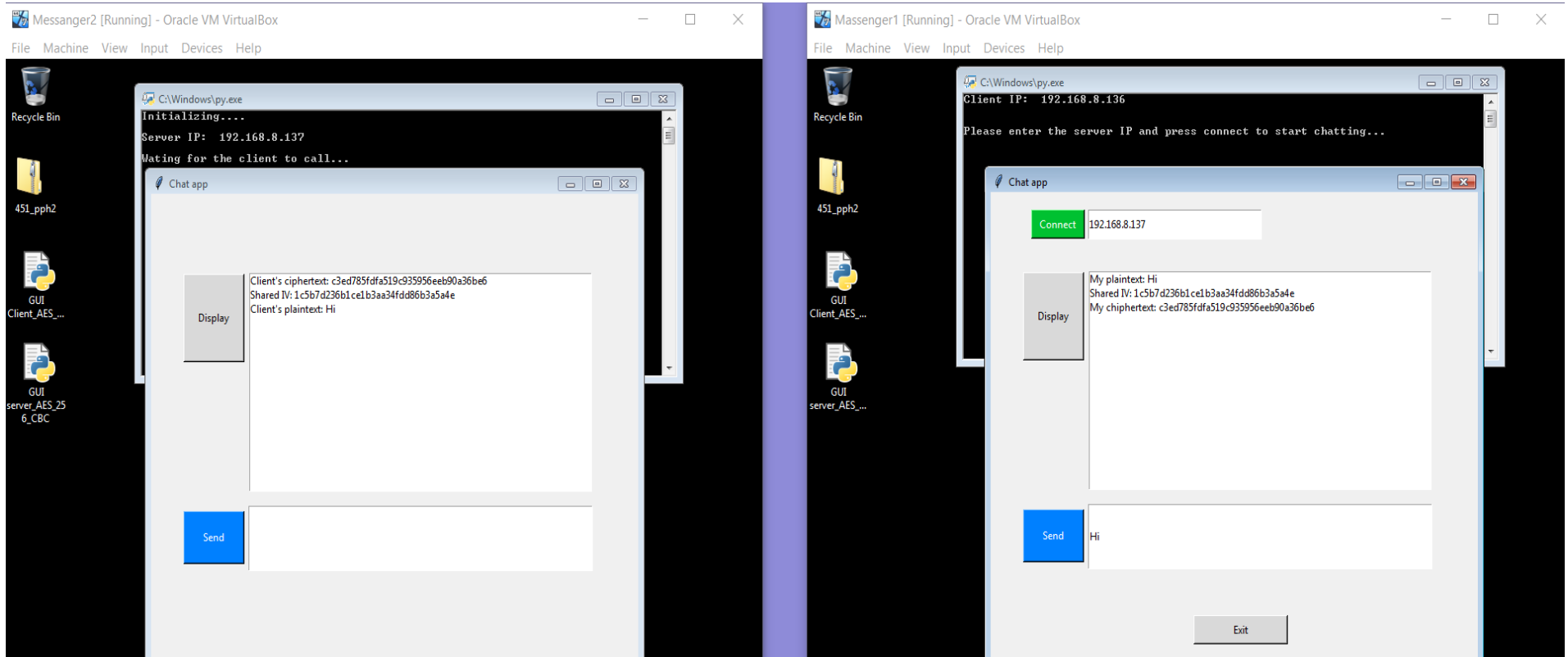
1c5652d3463a918dc32922453b2f476429143db9cadd553b9329c34f5fdf1c69

(Using the SHA256 online tool)

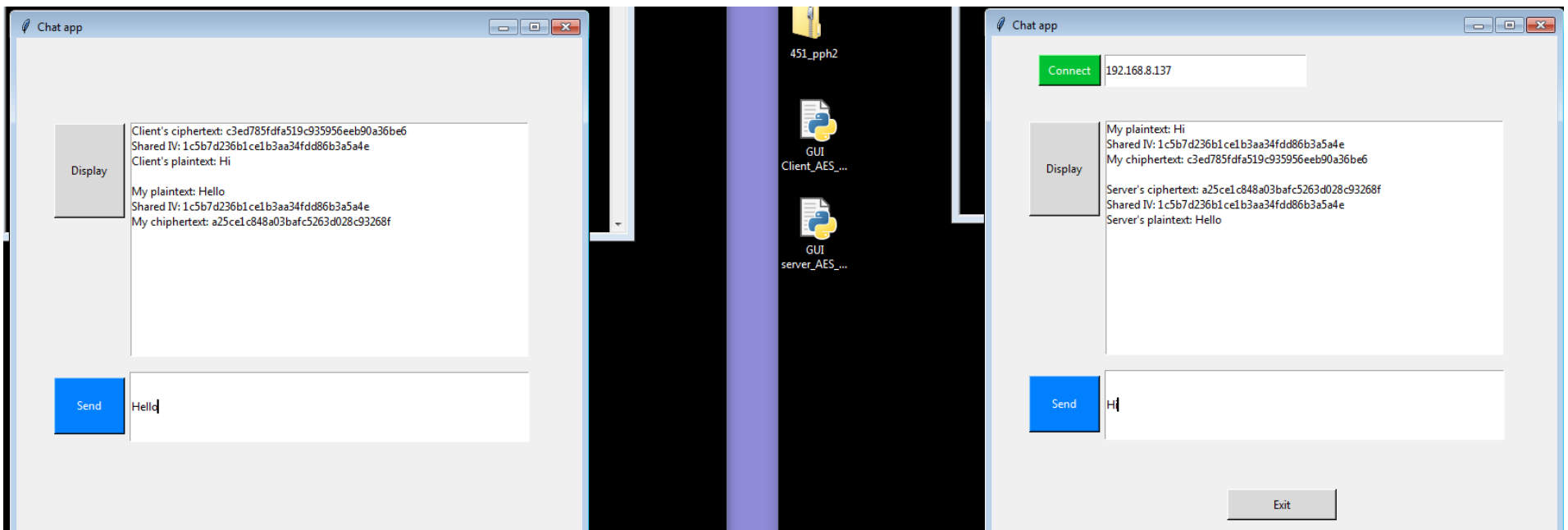
Testing: Chat session#1 (Left side: server, Right side: Client)



- 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

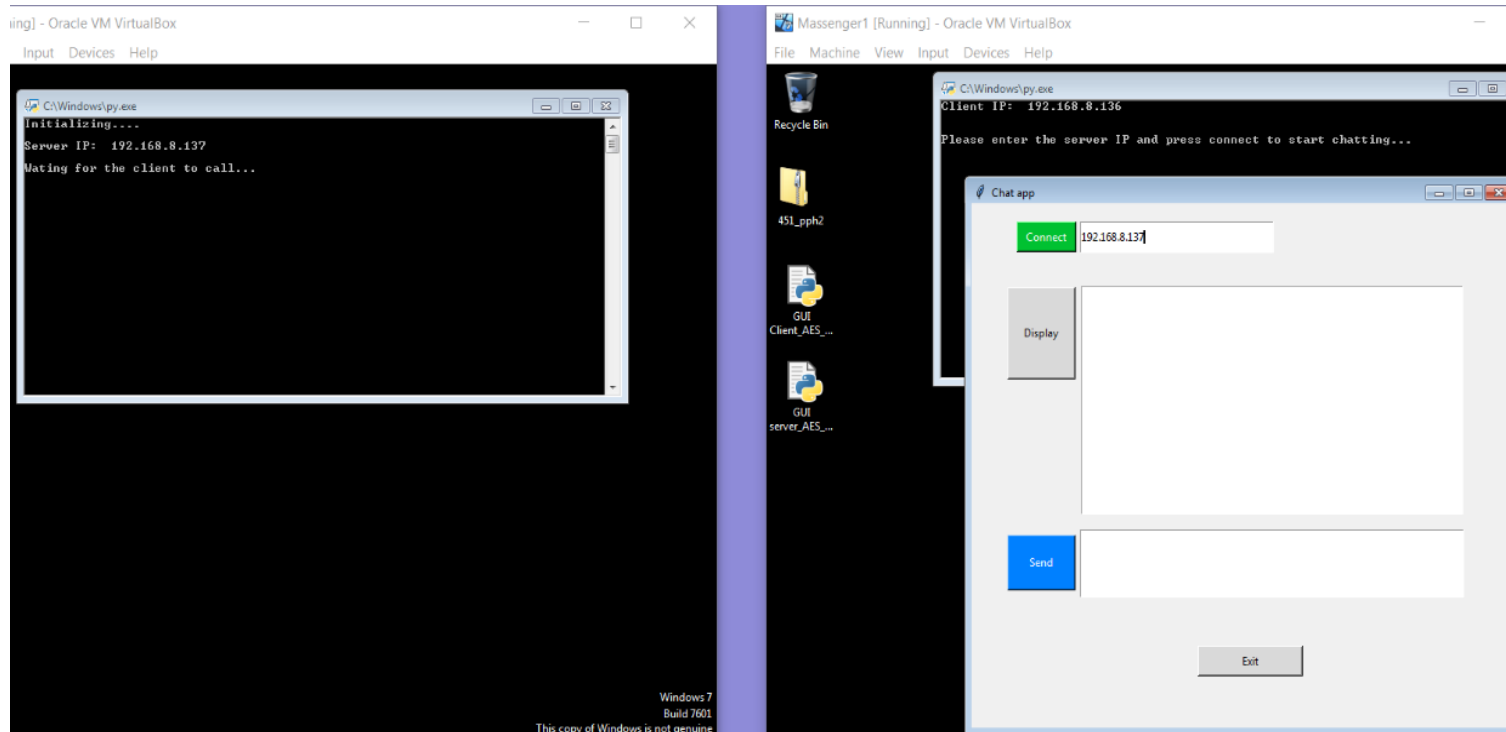
The interface consists of three main panels. The left panel, titled 'VIEW Text', contains the input text 'Hi'. The middle panel, titled 'ENCODE DECODE Block Cipher', shows the configuration for encoding: Algorithm is 'AES-256', Mode is 'CBC (Cipher Block Chaining)', Key is '1C5652D3463A918DC32922453B2F47642914', and IV is '1c5b7d236b1ce1b3aa34fdd86b3a5a4e'. A status bar at the bottom of this panel indicates '→ Encoded 16 bytes'. The right panel, titled 'VIEW Bytes', shows the resulting ciphertext in hexadecimal format: 'c3 ed 78 5f df a5 19 c9 35 95 6e eb 90 a3 6b e6'.

Client's ciphertext

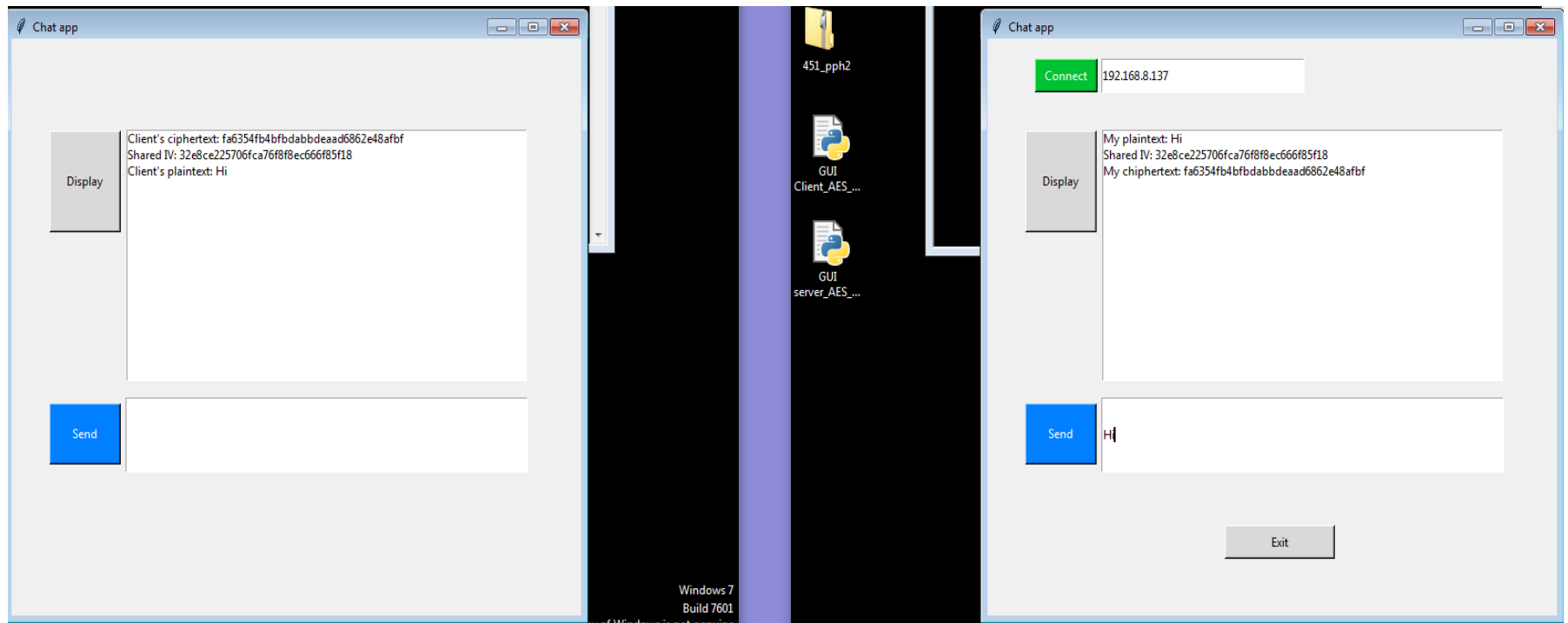
The interface is identical to the one above, but the input text in the left panel is 'Hello'. The middle panel shows the same configuration: Algorithm 'AES-256', Mode 'CBC (Cipher Block Chaining)', Key '1C5652D3463A918DC32922453B2F47642914', and IV '1c5b7d236b1ce1b3aa34fdd86b3a5a4e'. The status bar indicates '→ Encoded 16 bytes'. The right panel shows the resulting ciphertext in hexadecimal format: 'a2 5c e1 c8 48 a0 3b af c5 26 3d 02 8c 93 26 8f'.

Server's ciphertext

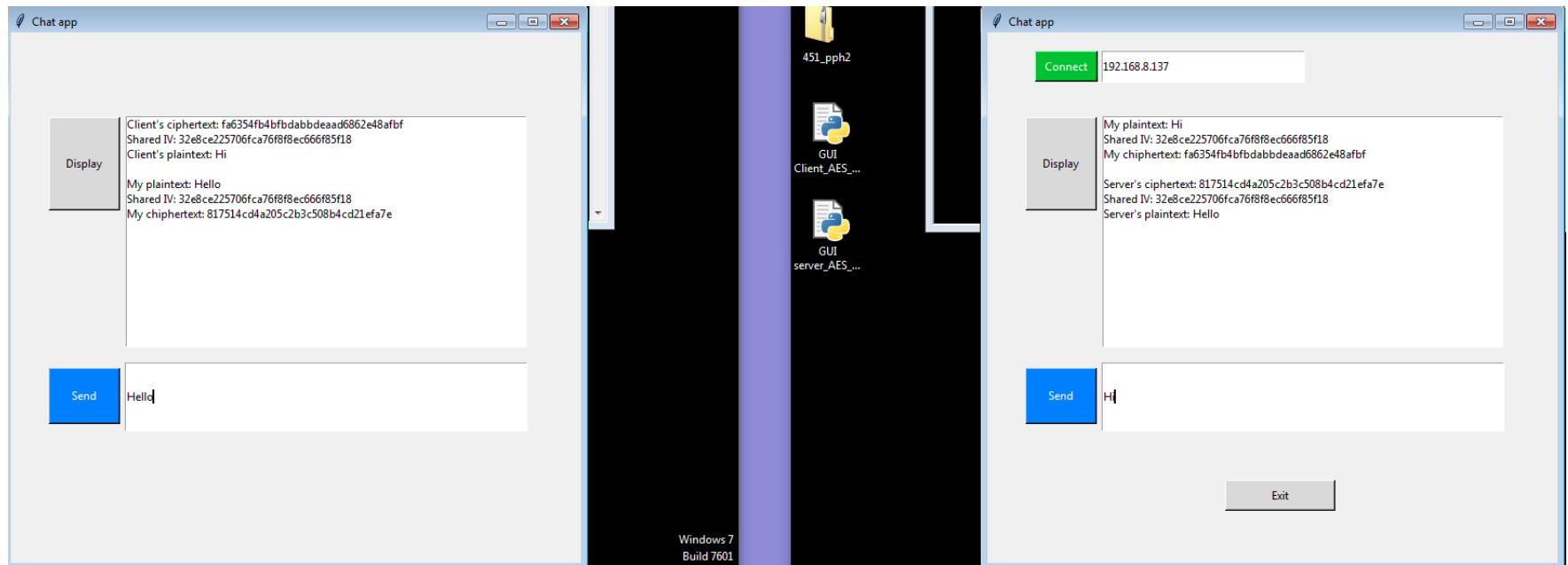
Testing: Chat session#2 (Left side: server, Right side: Client)



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

<div>VIEW</div> <div>Text</div> <div>Hi</div>	<div>ENCODE DECODE</div> <div>Block Cipher</div> <div>ALGORITHM</div> <div>AES-256</div> <div>MODE</div> <div>CBC (Cipher Block Chaining)</div> <div>KEY</div> <div>1C5652D3463A918DC32922453B2F47642914</div> <div>IV</div> <div>32e8ce225706fca76f8f8ec666f85f18</div> <div>→ Encoded 16 bytes</div>	<div>VIEW</div> <div>Bytes</div> <div>FORMAT</div> <div>Hexadecimal</div> <div>GROUP BY</div> <div>Byte</div> <div>fa 63 54 fb 4b fb da bb de aa d6 86 2e 48 af bf</div>
---	--	--

Client's ciphertext

<div>VIEW</div> <div>Text</div> <div>Hello</div>	<div>ENCODE DECODE</div> <div>Block Cipher</div> <div>ALGORITHM</div> <div>AES-256</div> <div>MODE</div> <div>CBC (Cipher Block Chaining)</div> <div>KEY</div> <div>1C5652D3463A918DC32922453B2F47642914</div> <div>IV</div> <div>32e8ce225706fca76f8f8ec666f85f18</div> <div>→ Encoded 16 bytes</div>	<div>VIEW</div> <div>Bytes</div> <div>FORMAT</div> <div>Hexadecimal</div> <div>GROUP BY</div> <div>Byte</div> <div>81 75 14 cd 4a 20 5c 2b 3c 50 8b 4c d2 1e fa 7e</div>
--	--	--

Server's ciphertext