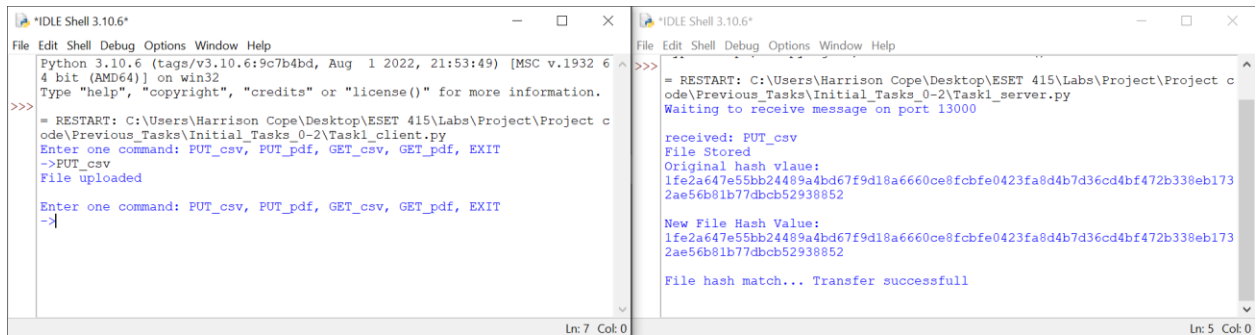


## Screenshots

- Task 1: Upload/Download File Transfer & Task 2: 384-bit hash sent and checked
  - o PUT\_csv



```
Python 3.10.6 (tags/v3.10.6:9c7b4bd, Aug 1 2022, 21:53:49) [MSC v.1932 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.

>>> = RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project code\Previous_Tasks\Initial_Tasks_0-2\Task1_client.py
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->PUT_csv
File uploaded

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->

= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project code\Previous_Tasks\Initial_Tasks_0-2\Task1_server.py
Waiting to receive message on port 13000

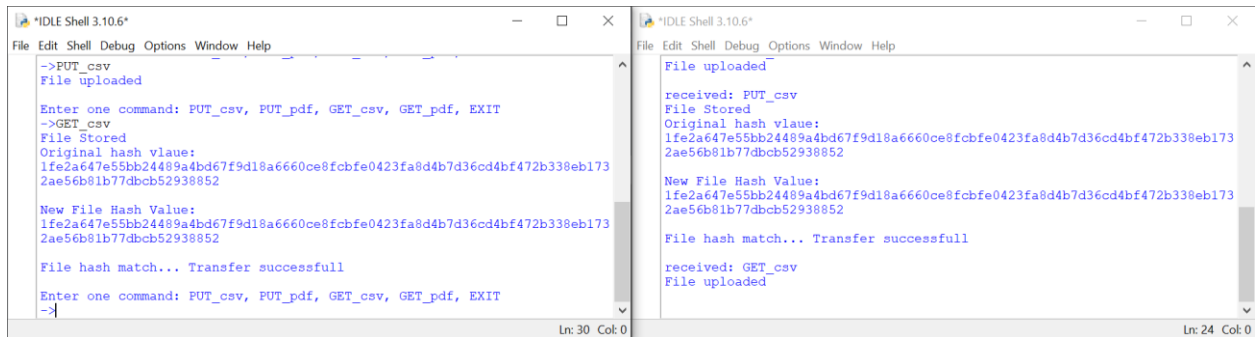
received: PUT_csv
File Stored
Original hash vlaue:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

New File Hash Value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

File hash match... Transfer successfull
```

Client uploads csv file to Server. Original hash is checked with newly created file's hash.

- o GET\_csv



```
->PUT_csv
File uploaded

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->GET_csv
File Stored
Original hash vlaue:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

New File Hash Value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

File hash match... Transfer successfull

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->

File uploaded

received: PUT_csv
File Stored
Original hash vlaue:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

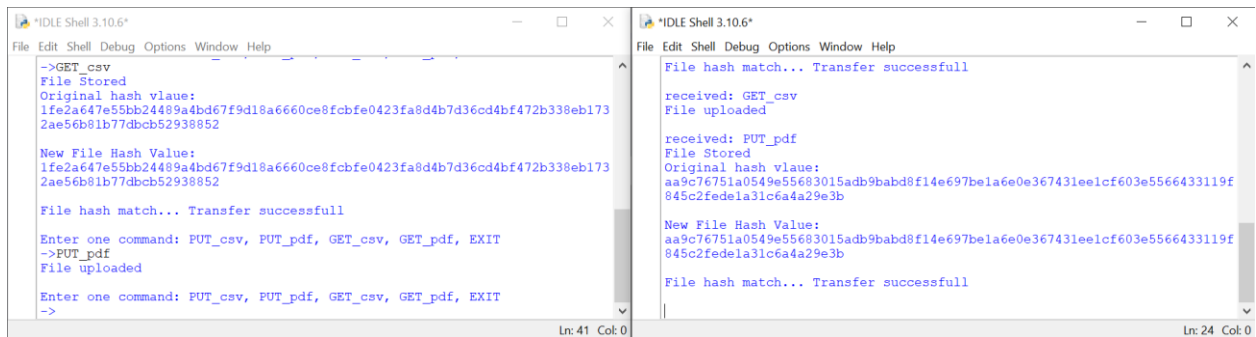
New File Hash Value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

File hash match... Transfer successfull

received: GET_csv
File uploaded
```

Client Downloads csv file from Server. Original hash is checked with newly created file's hash.

- o PUT\_pdf



```
->GET_csv
File Stored
Original hash vlaue:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

New File Hash Value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

File hash match... Transfer successfull

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->PUT_pdf
File uploaded

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->

File hash match... Transfer successfull

received: GET_csv
File uploaded

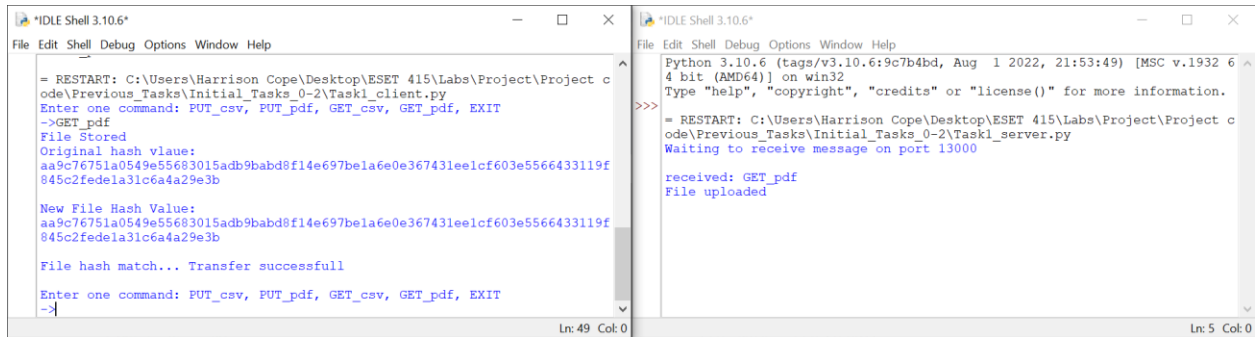
received: PUT_pdf
File Stored
Original hash vlaue:
aa9c76751a0549e55683015adb9babd8f14e697bela6e0e367431ee1cf603e5566433119f
845c2fedela31c6a4a29e3b

New File Hash Value:
aa9c76751a0549e55683015adb9babd8f14e697bela6e0e367431ee1cf603e5566433119f
845c2fedela31c6a4a29e3b

File hash match... Transfer successfull
```

Client uploads pdf file to Server. Original hash is checked with newly created file's hash.

## ○ GET\_pdf



```

= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Previous_Tasks\Initial_Tasks_0-2\Task1_client.py
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->GET_pdf
File Stored
Original hash vlaue:
aa9c76751a0549e55683015adb9babd8f14e697bela6e0e36743leelcf603e5566433119f
845c2fedela31c6a4a29e3b

New File Hash Value:
aa9c76751a0549e55683015adb9babd8f14e697bela6e0e36743leelcf603e5566433119f
845c2fedela31c6a4a29e3b

File hash match... Transfer successfull

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->

```

```

Python 3.10.6 (tags/v3.10.6:9c7b4bd, Aug 1 2022, 21:53:49) [MSC v.1932 6
4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Previous_Tasks\Initial_Tasks_0-2\Task1_server.py
Waiting to receive message on port 13000

received: GET_pdf
File uploaded

```

Client Downloads pdf file from Server. Original hash is checked with newly created file's hash.

- Task 3: Knapsack Encryption

Plaintext “Hello” is encrypted and decrypted with the clients key and then the servers key with knapsack encryption. For both keys the plaintext is encrypted and then successfully decrypted.

○ Encryption/decryption with Client’s Key

KNAPSACK ENCRYPTION

```
Plaintext: Hello
Private Key: [2, 7, 11, 21, 42, 89, 180, 354]
n: 588
m: 881
Inverse mod n: 442
Public Key: [295, 592, 301, 14, 28, 353, 120, 236]

Ciphertext: [620, 1482, 1274, 1274, 1630]
```

KNAPSACK DECRYPTION

```
Ciphertext: [620, 1482, 1274, 1274, 1630]
Private Key: [2, 7, 11, 21, 42, 89, 180, 354]
Public Key: [295, 592, 301, 14, 28, 353, 120, 236]
n: 588
m: 881

Plaintext: Hello

Encryption ciphertext: [620, 1482, 1274, 1274, 1630]
Decryption plaintext: Hello
```

○ Encryption/decryption with Server’s Key

KNAPSACK ENCRYPTION

```
Plaintext: Hello
Private Key: [2, 3, 6, 13, 27, 52, 105, 210]
n: 588
m: 881
Inverse mod n: 442
Public Key: [295, 2, 4, 596, 18, 622, 70, 140]

Ciphertext: [20, 768, 646, 646, 856]
```

KNAPSACK DECRYPTION

```
Ciphertext: [20, 768, 646, 646, 856]
Private Key: [2, 3, 6, 13, 27, 52, 105, 210]
Public Key: [79, 328, 237, 304, 19, 378, 167]
n: 588
m: 881

Plaintext: Hello

Encryption ciphertext: [20, 768, 646, 646, 856]
Decryption plaintext: Hello
```

- Full Integration
  - o PUT\_csv

The screenshot shows two IDLE Shell 3.10.6 windows and a file explorer. The top window shows the client's perspective: it starts with a restart of the program, displays the client's public key list, prompts for a command, and shows the successful upload of a CSV file. The bottom window shows the server's perspective: it waits for a message on port 13001, receives the client's public key list, prompts for a command, and shows the successful download and storage of the CSV file. The file explorer at the bottom shows the directory structure: ESET 415 > Labs > Project > Project code > Server\_Directory, with a file named 'test\_data' (195 KB) listed.

```

*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help
4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Task1_client.py
Clients public key will be sent to server: [295, 592, 301, 14, 28, 353,
120, 236]

Sent client's public key

Server's public key list: [79, 328, 237, 304, 19, 378, 167, 334]
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->PUT_csv
Uploading CSV file to server...
File uploaded

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->

Ln: 13 Col: 0

*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help
Waiting to receive message on port 13001

Client's public key list: [295, 592, 301, 14, 28, 353, 120, 236]
Sent server's public key
received: PUT_csv
Downloading CSV file from client...
File Stored
Original hash value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

New File Hash Value:
ca8301d3fa0f5f18cfef6cb459ee5a3a1e6728a481b16a65413fba02422d79892b31132b5
5a6f84501ab1b81e070385a

File hash mismatch...

Ln: 5 Col: 0

> ESET 415 > Labs > Project > Project code > Server_Directory

```

Name	Date modified	Type	Size
test_data	12/11/2022 11:18 PM	Microsoft Excel Com...	195 KB

Client uploads csv file to Server. Original hash is checked with newly created file's hash. The uploaded file is shown in the server directory. The file is exactly the same size, but the encryption may have messed with the hash value.

## ○ GET\_csv

```

*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help
Server's public key list: [79, 328, 237, 304, 19, 378, 167, 334]
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->GET_csv
Downloading CSV file from server...

File Stored
Original hash value:
1fe2a647e55bb24489a4bd67f9d18a6660ce8fcbfe0423fa8d4b7d36cd4bf472b338eb173
2ae56b81b77dbcb52938852

New File Hash Value:
e51c1c31a783bbb0904347c962f35582cab3a848d278a91c90e4b524296ac3376031748c8
6fe0aed3ed8b9fa98fddlee

File hash mismatch...

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->
Ln: 13 Col: 0

*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help
Python 3.10.6 (tags/v3.10.6:9c7b4bd, Aug 1 2022, 21:53:49) [MSC v.1932 6
4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Task1_server.py
Server's public key will be sent to client: [79, 328, 237, 304, 19, 378,
167, 334]
Waiting to receive message on port 13001

Client's public key list: [295, 592, 301, 14, 28, 353, 120, 236]
Sent server's public key
received: GET_csv
Uploading CSV file to client...
File uploaded
Ln: 5 Col: 0

```

ESET 415 > Labs > Project > Project code > Client_Directory			
Name	Date modified	Type	Size
test_data	12/11/2022 11:26 PM	Microsoft Excel Com...	153 KB

Client downloads csv file from Server. Original hash is checked with newly created file's hash. The uploaded file is shown in the client directory. The file did not transfer completely for some reason although it is using the same code as PUT\_csv.

## ○ PUT\_pdf

The image shows two IDLE Shell 3.10.6 windows and a file explorer. The top window shows the client's perspective, where the user enters the command 'PUT\_pdf' to upload a PDF file. The bottom window shows the server's perspective, where it receives the file, checks the hash, and confirms the successful transfer. The file explorer at the bottom shows the 'Server\_Directory' containing 'ESET415\_Syllabus\_Fall22' and 'test\_data'.

```
*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help

4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Task1_client.py
Clients public key will be sent to server: [295, 592, 301, 14, 28, 353,
120, 236]

Sent client's public key

Server's public key list: [79, 328, 237, 304, 19, 378, 167, 334]
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->PUT_pdf
Uploading PDF file to server...
File uploaded

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->
```

```
*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help

Waiting to receive message on port 13001

Client's public key list: [295, 592, 301, 14, 28, 353, 120, 236]
Sent server's public key
received: PUT_pdf
Downloading PDF file from client...
File Stored
Original hash value:
118ff088beb951797ea2a9e3c6998d8c071dee4354ab49d12bae06f7ffd6369ab97924b95
bb7b0a81e6ebc464eb8aadb

New File Hash Value:
118ff088beb951797ea2a9e3c6998d8c071dee4354ab49d12bae06f7ffd6369ab97924b95
bb7b0a81e6ebc464eb8aadb

File hash match... Transfer successfull
```

File Explorer: ESET 415 > Labs > Project > Project code > Server\_Directory

Name	Date modified	Type	Size
ESET415_Syllabus_Fall22	12/11/2022 11:23 PM	Adobe Acrobat Docu...	492 KB
test_data	12/11/2022 11:18 PM	Microsoft Excel Com...	195 KB

Client uploads pdf file to Server. Original hash is checked with newly created file's hash. The uploaded file is shown in the server directory. The file transferred successfully through the encryption.

- GET\_pdf

```

*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help

Server's public key list: [79, 328, 237, 304, 19, 378, 167, 334]
Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->GET_pdf
Downloading PDF file from server...
File Stored
Original hash value:
118ff088beb951797ea2a9e3c6998d8c071dee4354ab49d12bae06f7ffd6369ab97924b95
bb7b0a81e6ebc464eb8aadb

New File Hash Value:
7b8eacd9def3c6c3b365273d14d6c3fee8425fccd7a37a0b4469d79e4cfcafb85041ac54
4e7188f218a085949148432

File hash mismatch...

Enter one command: PUT_csv, PUT_pdf, GET_csv, GET_pdf, EXIT
->
Ln: 13 Col: 0



*IDLE Shell 3.10.6*
File Edit Shell Debug Options Window Help

Python 3.10.6 (tags/v3.10.6:9c7b4bd, Aug 1 2022, 21:53:49) [MSC v.1932 6
4 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Harrison Cope\Desktop\ESET 415\Labs\Project\Project c
ode\Task1_server.py
Server's public key will be sent to client: [79, 328, 237, 304, 19, 378,
167, 334]
Waiting to receive message on port 13001

Client's public key list: [295, 592, 301, 14, 28, 353, 120, 236]
Sent server's public key
received: GET_pdf
Uploading PDF file to client...
File uploaded
Ln: 5 Col: 0

```

File Explorer: ESET 415 > Labs > Project > Project code > Client\_Directory

Name	Date modified	Type	Size
 ESET415_Syllabus_Fall22	12/11/2022 11:28 PM	Adobe Acrobat Docu...	292 KB
 test_data	12/11/2022 11:26 PM	Microsoft Excel Com...	153 KB

Client downloads pdf file from Server. Original hash is checked with newly created file's hash. The uploaded file is shown in the client directory. The file did not transfer completely for some reason although it is using the same code as PUT\_pdf.