NSC Assignment 3

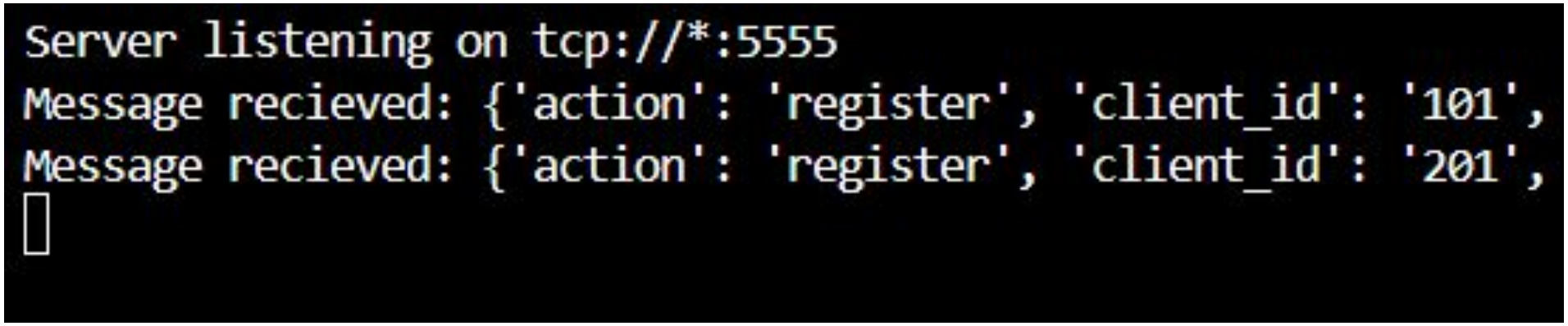
Arpan Kumar(2021020)
Pranav Tanwar(2022368)

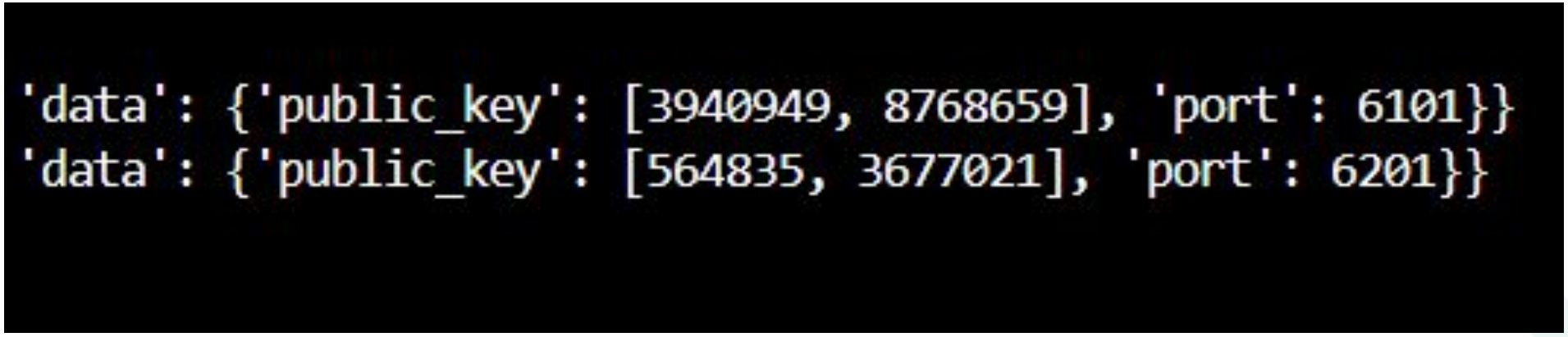
INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY
DELHI

Distribution of Public Keys

- The clients register themselves with a certification authority (CA).
- The CA generates certificates for the clients using its private key and a hash function.
- The clients request for the certificate of the system they want to send a message to, and acquire its public key to encrypt the message.
- The clients communicate with each other using the acquired keys.

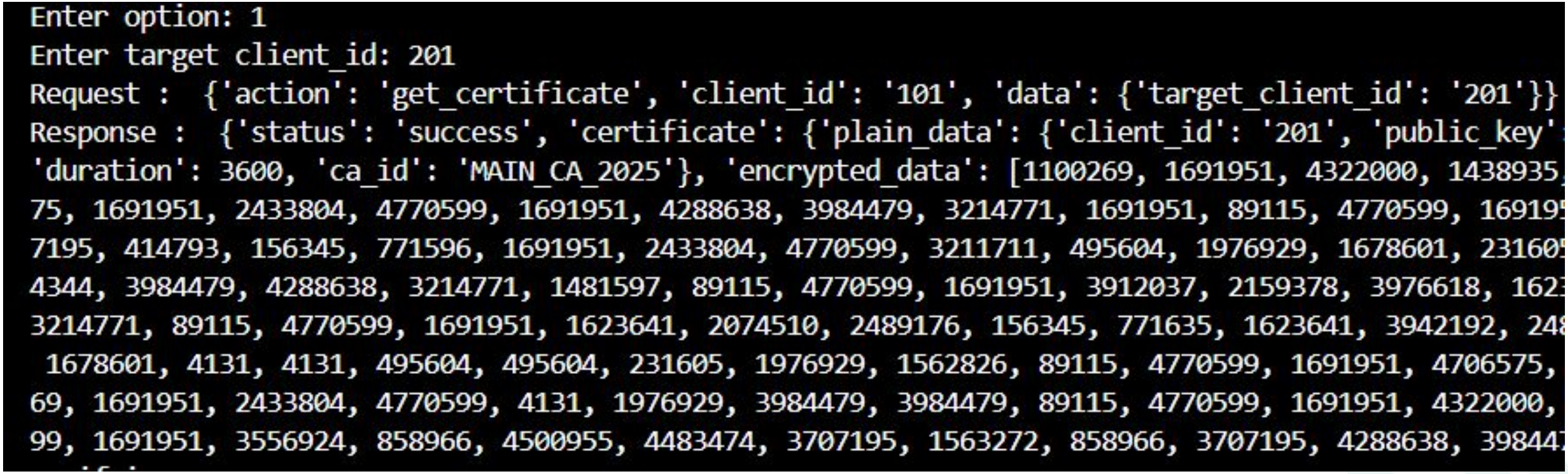
Certification Authority





Clients 101 and 201 setup

Requesting Target Client Public Key

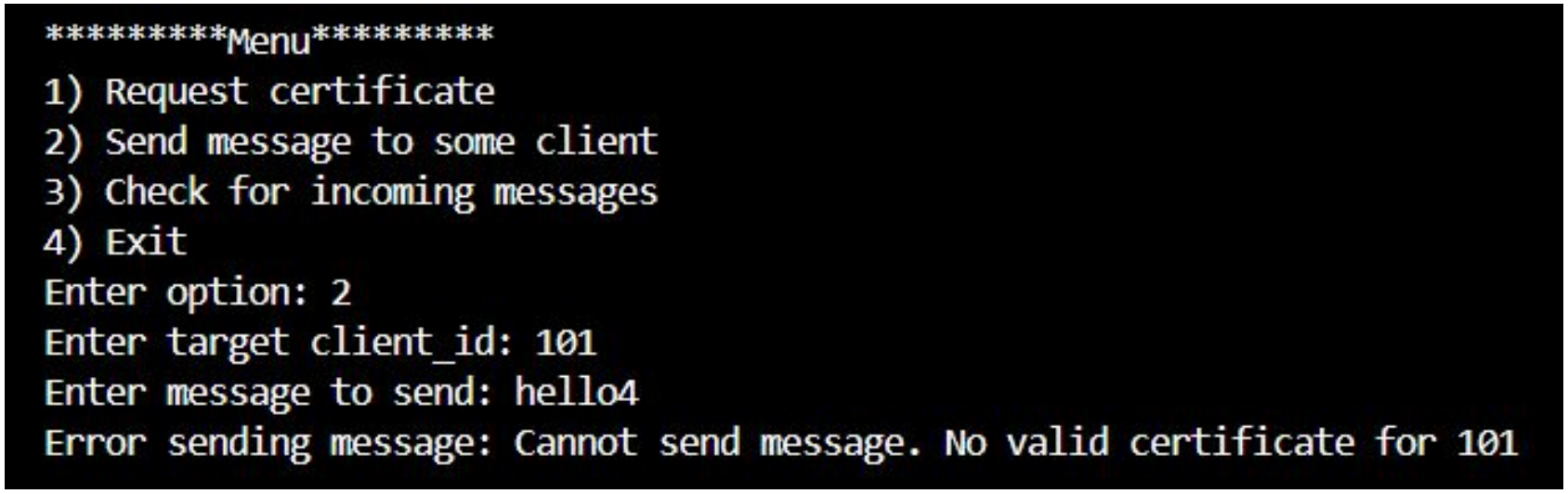


Sending Message with certificate

```
*********Menu*********
1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 2
Enter target client_id: 201
Enter message to send: hello1
Message sent. Acknowledgment: {'status': 'received'}

1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 2
Enter target client_id: 201
Enter message to send: hello2
Message sent. Acknowledgment: {'status': 'received'}

1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 2
Enter target client_id: 201
Enter message to send: hello3
Message sent. Acknowledgment: {'status': 'received'}
```

```
*********Menu*********
1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 3
Checking for messages (waiting for 5 seconds)...

Received message from 101: hello1

1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 3
Checking for messages (waiting for 5 seconds)...

Received message from 101: hello2

1) Request certificate
2) Send message to some client
3) Check for incoming messages
4) Exit
Enter option: 3
Checking for messages (waiting for 5 seconds)...

Received message from 101: hello3
```

Sending message without certificate



Results in error as Client 201 does not have the public key for Client 101