

# NSC Assignment 3

---

Arpan Kumar(2021020)  
Pranav Tanwar(2022368)



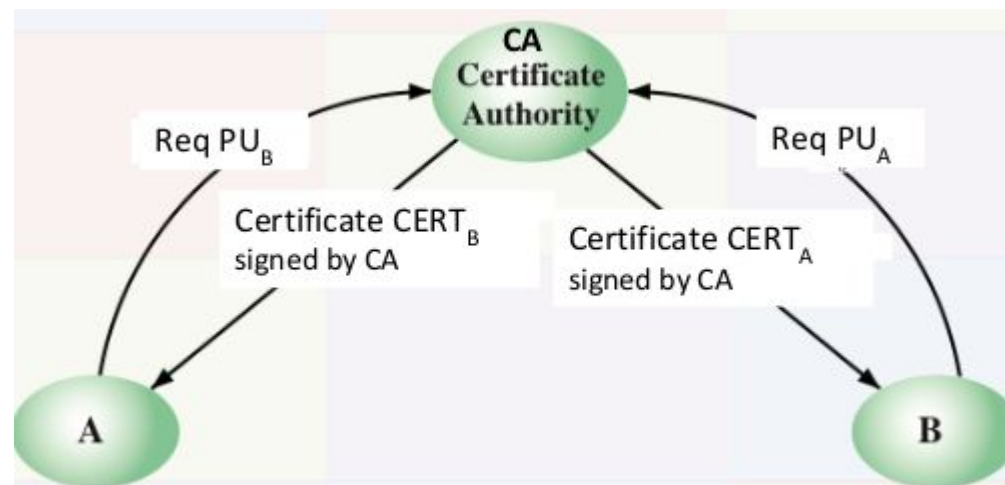
INDRAPRASTHA INSTITUTE *of*  
INFORMATION TECHNOLOGY  
DELHI



# 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



```
Server listening on tcp://*:5555
Message recieved: {'action': 'register', 'client_id': '101',
Message recieved: {'action': 'register', 'client_id': '201',
█
```

```
'data': {'public_key': [3940949, 8768659], 'port': 6101}}
'data': {'public_key': [564835, 3677021], 'port': 6201}}
```

# Clients 101 and 201 setup



```
Request : {'action': 'register', 'client_id': '101', 'data': {'public_key': (3940949, 8768659), 'port': 6101}}
Response : {'status': 'success', 'authority_key': [518015, 4802767], 'message': 'Client registered and certificate generated'}
```

```
*****Menu*****
```

- 1) Request certificate
- 2) Send message to some client
- 3) Check for incoming messages
- 4) Exit

```
Enter option: 
```

```
Request : {'action': 'register', 'client_id': '201', 'data': {'public_key': (564835, 3677021), 'port': 6201}}
Response : {'status': 'success', 'authority_key': [518015, 4802767], 'message': 'Client registered and certificate generated'}
```

```
*****Menu*****
```

- 1) Request certificate
- 2) Send message to some client
- 3) Check for incoming messages
- 4) Exit

```
Enter option: 
```



Enter target client\_id: 201

```
Response : {'status': 'success', 'certificate': {'plain_data': {'client_id': '201', 'public_key'
```

75, 1691951, 2433804, 4770599, 1691951, 4288638, 3984479, 3214771, 1691951, 89115, 4770599, 1691951

7195, 414793, 156345, 771596, 1691951, 2433804, 4770599, 3211711, 495604, 1976929, 1678601, 231609

4344, 3984479, 4288638, 3214771, 1481597, 89115, 4770599, 1691951, 3912037, 2159378, 3976618, 1623

3214771, 89115, 4770599, 1691951, 1623641, 2074510, 2489176, 156345, 771635, 1623641, 3942192, 248

1678601, 4131, 4131, 495604, 495604, 231605, 1976929, 1562826, 89115, 4770599, 1691951, 4706575,

69, 1691951, 2433804, 4770599, 4131, 1976929, 3984479, 3984479, 89115, 4770599, 1691951, 4322000.

99. 1691951. 3556924. 858966. 4500955. 4483474. 3707195. 1563272. 858966. 3707195. 4288638. 398447

1. *Journal of the American Medical Association*, 1997; 278: 1961-1965.

# 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



```
*****Menu*****
```

- 1) Request certificate
- 2) Send message to some client
- 3) Check for incoming messages
- 4) Exit

```
Enter option: 2
```

```
Enter target client_id: 101
```

```
Enter message to send: hello4
```

```
Error sending message: Cannot send message. No valid certificate for 101
```

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