Applied Cryptography Project : Two-Factor Authentication using TOTP
Name : Radhika Narayana
CIS : 543

User Registration:

Server:

```
rady@vishwa-laptop:~/sem1_hw/Cryptography 70x55
[rady@vishwa-laptop Cryptography]$ python server_tls.py
Database not found, password entered below will be used to create DB
Enter Admin Password (minimum 4 char):
asdf
waiting for incoming connections...
TLS client connected: 127.0.0.1:57934
Server received user Jennifer
Storing user data in database..
Sending registration success
```

Client:

```
[rady@vishwa-laptop Cryptography]$ python client_tls.py
TLS connection established.

Welcome User! Enter 1 for Register, 2 for Login

1
Registering new user:

Please enter a Username (minimum 4 char):
Jennifer
Please enter a password (minimum 4 char):
pass123
Registration Complete, Thank you!


Scan this QR Code in Google Authenticator:
```

```
Select option 2 for login
```

User Login:

Server:

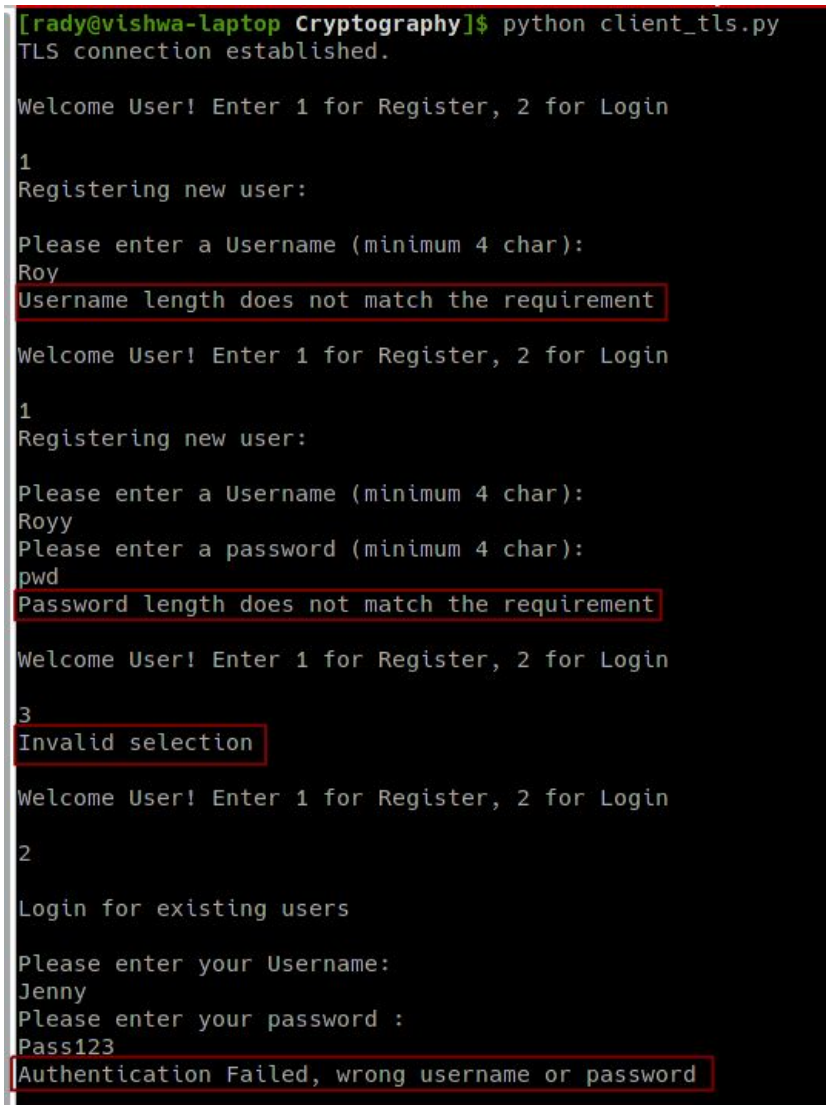
```
[rady@vishwa-laptop Cryptography]$ python server_tls.py
Existing database found
If you forgot password, delete database and try again
Enter Admin Password (minimum 4 char):
asdf
waiting for incoming connections...
TLS client connected: 127.0.0.1:57946
Checking if user exists
User found:
Generated B
receiving M

sending HAMK
User authenticated
TOTP received from client:  934510
TOTP generated by server:   934510
TOTP successfully verified
```

Client:

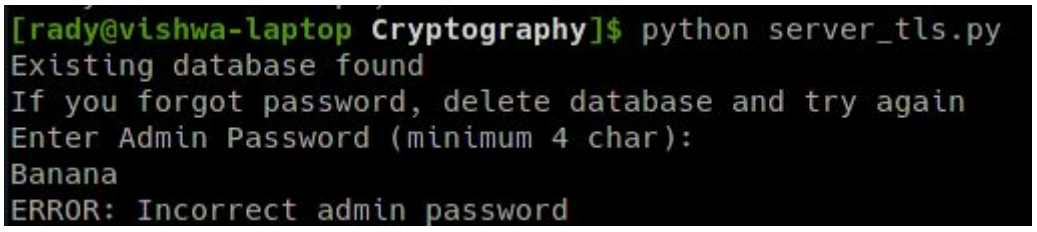
```
[rady@vishwa-laptop Cryptography]$ python client_tls.py
TLS connection established.

Welcome User! Enter 1 for Register, 2 for Login

2

Login for existing users

Please enter your Username:
Jennifer
Please enter your password :
pass123
User authenticated
Please enter 6 digit TOTP token from Google authenticator:
934510
Token verified successfully
Login successful

Welcome User! Enter 1 for Register, 2 for Login
```

Few validation errors:

Client



Server:



Incorrect TOTP:

Server:

```
[rady@vishwa-laptop Cryptography]$ python server_tls.py
Existing database found
If you forgot password, delete database and try again
Enter Admin Password (minimum 4 char):
asdf
waiting for incoming connections...
TLS client connected: 127.0.0.1:57986
Checking if user exists
User found:
Generated B
receiving M

sending HAMK
User authenticated
TOTP received from client:  123632
TOTP generated by server:   287643
TOTP did not match
```

Client:

```
[rady@vishwa-laptop Cryptography]$ python client_tls.py
TLS connection established.

Welcome User! Enter 1 for Register, 2 for Login

2

Login for existing users

Please enter your Username:
Jennifer
Please enter your password :
pass123
User authenticated
Please enter 6 digit TOTP token from Google authenticator:
123632
Entered TOTP did not match, please try again!

Welcome User! Enter 1 for Register, 2 for Login
```