

15-112 Fundamentals of Programming



جامعة كارنيجي ميلون في قطر
Carnegie Mellon Qatar

Announcements

- HW 6 will be posted tonight – Due date is October 29, Tuesday.
- Final Project



جامعة كارنيجي ميلون في قطر
Carnegie Mellon Qatar

What are we doing

- ❑ More practice with sockets
- ❑ Network Authentication
 - Challenge-Response Authentication (CRA)

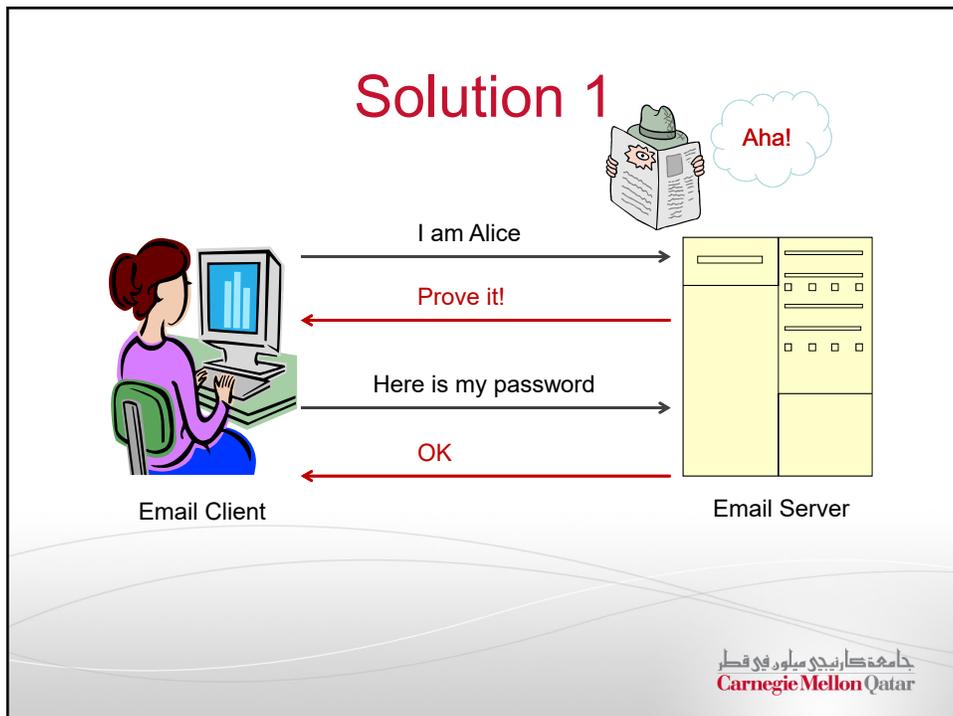
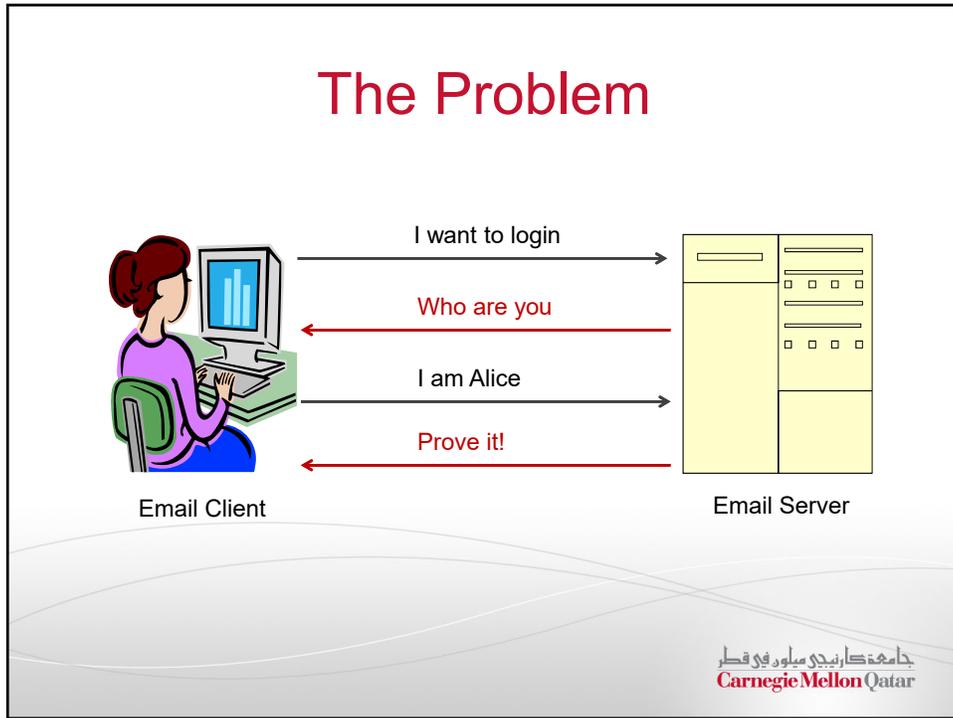
Reading/Writing to the socket

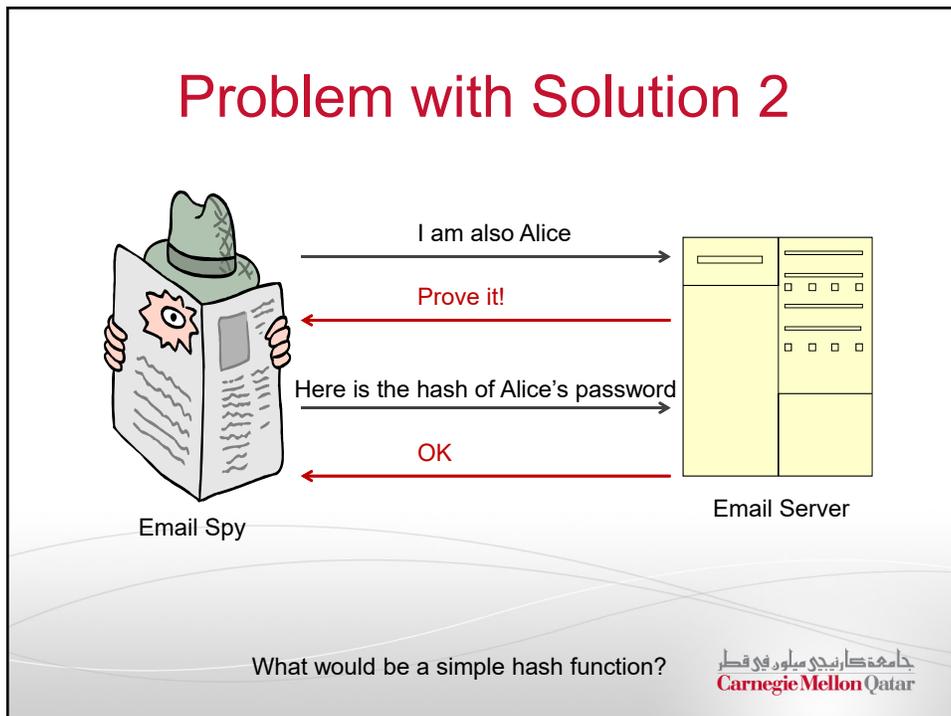
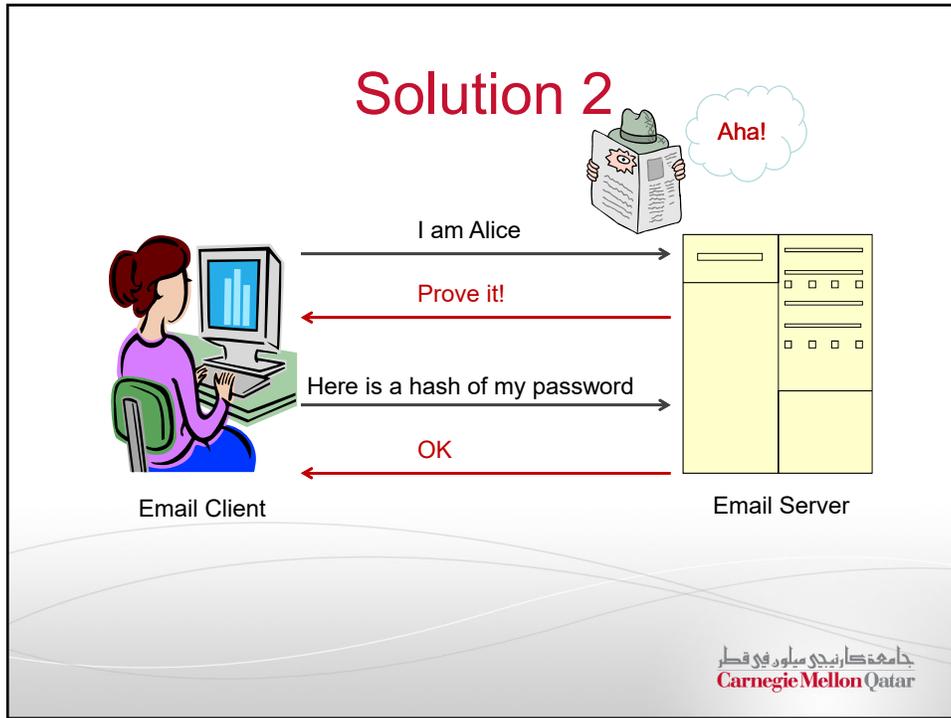
```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

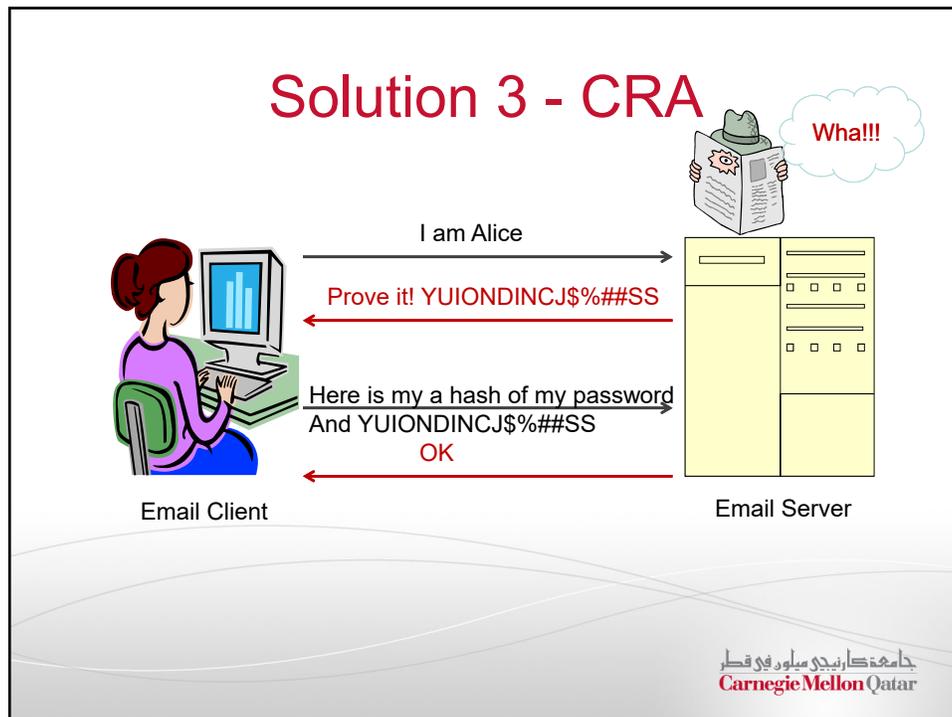
```
s.connect(('86.36.35.159', 15112))
```

```
data = s.recv(512) → Reads max of 512 bytes
```

```
s.send('Hello\n') → Writes "Hello" as a line
```







Challenge Response Authentication

- The client connects to the server
- The server makes up some random data
- The server sends this data (X) to client
- The client sends the $mD(P, X)$ – Message Digest based on password and X
- Sever compares the Message Digest with its own calculations

Exercise

- ❑ Connect to server 86.36.46.10 port 15112
- ❑ Send command "Login username\n"
 - Use your username that you emailed me
- ❑ Receive the following response
 - "Login username challenge"
- ❑ Calculate a message digest (messagedigest) based on your password and challenge
 - Set TotalSum to 0
 - Index i goes from 0 to length of password
 - + Get the ASCII value of element i of password
 - + Get the ASCII value of element i of challenge
 - + Find the Sum of these two ASCII values
 - + Mod the Sum with 26
 - + If your password is longer than the challenge, start from the beginning of challenge once it runs out
 - + Add the result to a TotalSum
 - Mod the TotalSum with 1000.
- ❑ Send the command "Login username messagedigest\n" to the server
- ❑ If the server responds with "Login Successful\n", you are successfully logged in.
- ❑ Change your password by sending command "CHPWD newpassword\n"
- ❑ If the server responds with "OK: password Changed\n", your password has been successfully changed.
- ❑ Close the connection
- ❑ Try logging in with the new password.