CSE 115
Introduction to Computer Science I
FINAL EXAM

Tuesday, December 11, 2018
7:15 PM - 10:15 PM
SOUTH CAMPUS

(Factor in travel time!!)
Room assignments will be published on the last day of classes.
CONFLICT?

E-mail documentation to:

alphonce@buffalo.edu

Subject: CSE115 FINAL EXAM CONFLICT

no later than 5:00 PM Friday November 30
CONFLICT?

Alternate date/time

Friday December 14
11:45 AM - 2:45 PM
room TBA
Accessibility Resources

Schedule exam to overlap with alternate exam time

Friday December 14
11:45 AM - 2:45 PM
room TBA
EXAM RULES

Bring your UB Card

No arrivals after the first 30 minutes

No departures in first 30 minutes

No electronics
(phones, laptops, calculators, earbuds, etc)

Closed books. Closed notes. Closed neighbors
Road map

▸ Review ◀

Designing the app

Needed libraries

Code walkthrough
Encryption

A and B want to communicate privately

With a decryption key B can read the encrypted message
Without a decryption key C cannot read the encrypted message
Encrypt the plain text password in transmission, store salted hash

The password encrypted during transmission, then hashed by B. The password hash is stored together with its salt.
Road map

Review

▶️ Designing the app

Needed libraries

Code walkthrough
Designing the app

There are several steps:
Designing the app

What do we need to put into our app to make this happen?

A

Client

B

Web Server
Designing the app

Activity #1:

What does client have?

Before first communication between client and server, what does the client (browser) have?
Designing the app

Activity #1:

What does client have?

Before first communication between client and server, what does the client (browser) have?

The ability to request resources from the web server (such as index.html)
Designing the app

Activity #1:

What does client need?

a) in our sample applications, what resources has the client requested from the web server?
Designing the app

Activity #1:

What does client need?

a) in our sample applications, what resources has the client requested from the web server?

Typically:
index.html
code.js
Designing the app

Activity #1:

What does client need?

b) what additional resources are needed to send an encrypted message to the web server?
Designing the app

Activity #1:

What does client need?

b) what additional resources are needed to send an encrypted message to the web server?

At least:

- an encryption library
- the web server's public key
Designing the app

Activity #1:
What does the server have?
Designing the app

Activity #1:
What does the server have?

index.html
frontEnd.js
server.py
backEnd.py
public key
private key
database
Designing the app

Activity #1:

What does the server share?
Designing the app

Activity #1:
What does the server share?

index.html
frontEnd.js
server.py
backEnd.py
public key
private key
database
Designing the app

Activity #1:

Where do the keys come from?

Client

index.html
frontEnd.js
server.py
backEnd.py
public key
private key

database

Web Server
Designing the app

Activity #1:

Where do the keys come from?

The keys are generated in pairs from a key generator.

This could be done outside of app, or inside app itself.
Designing the app

Activity #1:
Where are the keys stored?

Client

Web Server
Designing the app

Activity #1:

Where are the keys stored?

NOT IN THE CODE!

The keys should be persisted in a safe place, such as files or a database.

Client

Web Server
Road map

Review

Designing the app

- Needed libraries

Code walkthrough
Encryption libraries

There are many to choose from.

We'll explore one each for Python and JavaScript.
Encryption libraries

For JavaScript

for browser:

https://cdn.jsdelivr.net/npm/node-forge@0.7.0/dist/forge.min.js

for node:

npm install node-forge
var forge = require('node-forge');
Encryption libraries
For Python

pip install --user pycrypto
Road map

Review

Designing the app

Needed libraries

▶ Code walkthrough ▶
Code walkthrough

- Request: index.html
- Request: frontEnd.js
- Request: public key

Web Server:
- index.html
- frontEnd.js
- public key

- server.py
- backEnd.py
- private key
- database
Friday

Authentication