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 last day of classes
E-mail documentation to:

alphonce@buffalo.edu

Subject: CSE115 FINAL EXAM CONFLICT

no later than 5:00 PM TODAY
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)

Road map

▶ Review ◀

Handling passwords

Session data

Software Design
One-way encrypted communication
Road map

Review

▶ Designing the app ◀

Needed libraries

Code walkthrough
Designing the app

What does the server have?

- index.html
- frontEnd.js
- server.py
- backEnd.py
- public key
- private key
- database
- web server library
- encryption library

Client

Web Server
Designing the app

What does the server share?

index.html

frontEnd.js

server.py
backEnd.py

public key
private key
database

web server library
encryption library
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`
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');

For Python

pip install --user pycrypto
Road map

Review

- Handling passwords

Session data

Software Design
Account creation

If user has no account they need to register on the site.
Account creation

User chooses username and password.
Account creation

These are sent encrypted to the server
Account creation

The server decrypts the username and password, and does some sanity checks on these (e.g. make sure the username is not in use).
Account creation

Assuming all is good the server stores the new username together with the salt & password hash.
User login

username
User login
User login
User login
Road map

Review

Handling passwords

▶ Session data ◀

Software Design
User login

HTTP is stateless
Each request is independent:
there is no memory if previous requests
User login

Use an encrypted session cookie to store session data, like a username.
User login

Now we can allow the request to be tied to a specific user.
Need library

Hashing library

pip install --user bcrypt

This library handles the generation of random salt, hashing of salt + password, and verification of a password.
Road map

Review

Handling passwords

Session data

▶ Software Design ◀
Software design

Encapsulated functionality (functions)

Code organization (files, folders)