

CS 103000

Prof. Madeline Blount

Week 8:

MID-TERM & REVIEW

(no attendance today)



Dall-E 2: cats learning C++ in the forest on '90's technology



housekeeping: lab + attendance!

- Recitation = required!
- On-site labs are for practice *on that day* - and are counted as part of your attendance/participation grade (15% - see syllabus!)
- If you cannot attend Wednesday lab on any given day, the on-site problems are for your own practice.
- If you consistently miss recitation attendance or on-site lab completion, it will affect your grade.

MIDTERM!





Mid-term exam!

- Take home, Wednesday 3PM - Friday 12PM
- In zyBooks platform, like labs
- You may:
 - Look @ zyBooks for reference, documentation
 - Use resources linked in the syllabus
 - Use class notes, slides, code from class
 - Submit multiple times (like labs)
 - Use all the time you need until deadline



Mid-term exam

- You may not:
 - Turn in the mid-term late
 - Work with others; ask others for help; this is solo work
 - Use search engines or websites to search **specifically** for problems + solutions
 - Use ChatGPT, other generative AI tools to code solutions



Mid-term exam

- You may not:
 - Use methods from outside of class **without citation**
 - Examples:
 - using `#include <algorithm>`
 - using `.reverse, .begin(), .end()`
 - using `.map()`
 - Programs should include in comments **why** you chose this method, vs. another method we've studied
 - Solutions that use such methods **without citation/explanation** will lose points



Mid-term exam

- Academic honesty
- Discord: no q's about mid-term Wed-Fri!




Grades

- 3 passes: autograder (zyBooks), similarity checker, and me 🙄
- Mid-term = 20% (same as all reading!)
- If helps class average, I will curve
- After mid-term, will learn current class grade in Blackboard



Mid-term exam

- How to study?
 - Come to class this week!
 - Look over notes, slides, resources in syllabus 
 - zyBooks: Ch. 17
 - Go back over labs, problems that were challenging to you
 - Break down problems into steps, see if you can now solve with more knowledge

"CRAPS" AT CAMP

5116-11





PRACTICE: DICE GAME

Write a program that simulates a dice rolling game.

Your program should receive 3 integers as input:

```
3 4 5
```

The 1st number is the number of dice rolls. The 2nd number is the seed for a pseudorandom number generator. The 3rd number is what the user "bets," the number they want.

The program should output the roll for each round on a separate line. The last line should show the number of times the users' number (5, in example) was rolled.



PRACTICE:

OUTPUT:

```
Roll 1: 3
```

```
Roll 2: 5
```

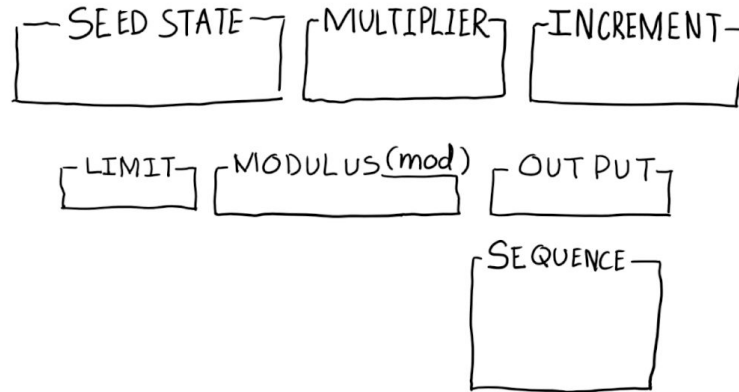
```
Roll 3: 6
```

```
5 was rolled 1 time
```

- `rand()` and `srand()`
- `for` loop
- Counter variable

pseudorandom!

- `rand()` = Linear Congruential Generator (LCG)
- $x = ((a * x) + c) \% m$
- Next number based on the previous (**state**)





`srand()` = SEED



PRACTICE: DATA ANALYSIS

You have 2 parallel vectors: one is the scientific name of a species, and the other vector is whether that Latin name is animal (true) or plant (false).

```
{"Psittaciformes", "Bubo virginianus", "Malus domestica",  
"Rhinoceros unicornis", "Allium sativum", "Ficus benghalensis",  
"Asteroidea"}
```

```
{true, true, false, true, false, false, true}
```

First print the size of my data set. Then print out the Latin name in all caps and whether it is animal or plant, on 1 line each, but starting with the end of the dataset. Then tell me the number of animals.





PRACTICE:

- Vectors, parallel vectors, iterating
- For loops (including 1 nested ...)
- Boolean variables
- String/char functions: toupper



PRACTICE: DRAWING GRIDS

Write a program that draws a square grid of  emojis. You can imagine this square is a room. One wall of this room will have a different color, written with  emojis.

The program takes 2 user inputs:

5 north

The integer is the size dimension of the square, and the string input is the wall which should be the green color. (Top = north, right = east, bottom = south, left = west.)



PRACTICE: TEXT ANALYSIS

Write a program that counts the number of each vowel in this text:

"So died these men as became Athenians. You, their survivors, must determine to have as unfaltering a resolution in the field, though you may pray that it may have a happier issue. And not contented with ideas derived only from words of the advantages which are bound up with the defense of your country, though these would furnish a valuable text to a speaker even before an audience so alive to them as the present, you must yourselves realize the power of Athens, and feed your eyes upon her from day to day, till love of her fills your hearts; and then, when all her greatness shall break upon you, you must reflect that it was by courage, sense of duty, and a keen feeling of honor in action that men were enabled to win all this, and that no personal failure in an enterprise could make them consent to deprive their country of their valor, but they laid it at her feet as the most glorious contribution that they could offer."

Also tell me how many alphabetic characters this string has. Finally, print the text out at the end, with every vowel replaced with an "@" sign.



PRACTICE:

- Strings
- Multiple vectors: vowels, frequencies
- Nested for loops
- String functions: isalpha, tolower



PRACTICE:

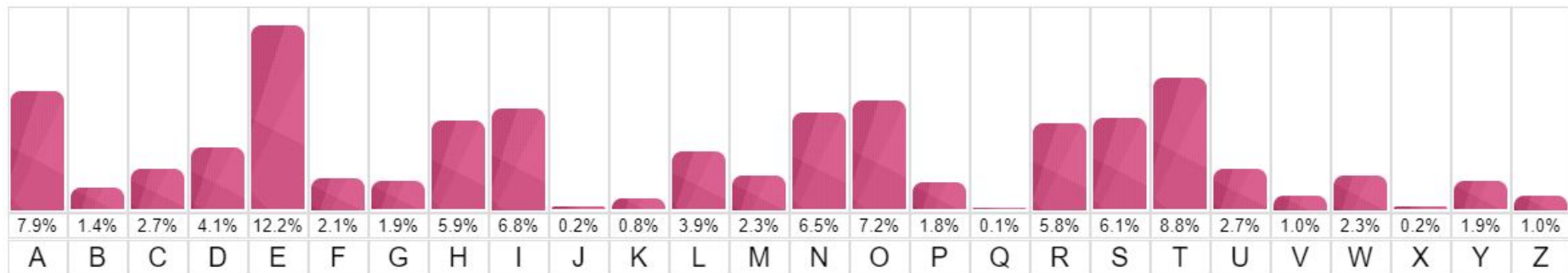
- a: 61
- e: 102
- i: 40
- o: 60
- u: 36

743 alphabetic characters.



CRYPTOGRAPHY: FREQUENCY ANALYSIS AND THE ONE-TIME PAD

How to hack a Caesar cipher?





CRYPTOGRAPHY: FREQUENCY ANALYSIS AND THE ONE-TIME PAD

"On Decrypting Encrypted Correspondence" - Al-Kindi, Baghdad, 850 CE



- Look @ encrypted text, count frequencies
- Which letter comes up the most? Compare that to "fingerprint" of frequencies you already know about your language ...
- Famously, Mary Queen of Scots beheaded, 1587 because linguist under Queen Elizabeth (Thomas Phelippes) cracked code using frequency analysis

a b c d e f g h i k l m n o p q r s t u x y z
 o † ‡ # a □ θ ∞ i ð n // ø ∇ s m f Δ ε c 7 8 9

Nulles ff. — . — . d.

Dowbleth σ

and for with that if but where as of the from by

2 3 4 4 4 3 3 n m 8 x ∞

so not when there this in wich is what say me my wyr

3 x † ‡ 6 x 6 m n m m d

send lre receave bearer I pray you Mte your name myne

1 2 3 4 5 6 7 8 9

Mary Queen of Scots - plot w/Anthony Babington



CRYPTOGRAPHY: FREQUENCY ANALYSIS AND THE ONE-TIME PAD

- What would make this monoalphabetic substitution (Caesar cipher) harder to crack?
- Randomness ... think brute force, also!



CRYPTOGRAPHY: FREQUENCY ANALYSIS AND THE ONE-TIME PAD

- With Caesar shift, only 26 possibilities to crack
- If every letter was shifted by its own shift, based on a random number ... $26 * \text{NUMBER OF LETTERS}$.
- Gets large very quickly
- One-time pad (1880s), pad of paper (or similar - 🔍 small, flammable, etc.)