15-110: Principles of Computing, Fall 2017

LOOK !

Problem Set 11 (PS11)

Due: Tuesday, April 24 by 2:30PM via Gradescope Hand-in

HANDIN INSTRUCTIONS

Download a copy of this PDF file. You have two ways to fill in your answers:

1. **Just edit (preferred) - Use any PDF editor (e.g., Preview on Mac, iAnnotate on mobile, Acrobat Pro on pretty much anything) to typeset your answers in the given spaces. You can even draw pictures or take a picture of a drawing and import it in the correct place in the document. That's it. (Acrobat Pro is available on all cluster machines.)**

2. **Print and Scan - Alternatively, print this file, write your answers neatly by hand, and then scan it into a PDF file. This is labor-intensive and must be done by the deadline.**

Once you have prepared your submission, submit it on Gradescope. A link to Gradescope is provided in our Canvas course portal.

Fill in your answers ONLY in the spaces provided. Any answers entered outside of the spaces provided may not be graded. Do not add additional pages. We will only score answers in the given answer spaces provided. If we cannot read your answer or it contains ambiguous information, you will not receive credit for that answer.

Be sure to enter your full name below along with your section letter (A, B, C, etc.) and your Andrew ID. Submit your work on Gradescope by 2:30PM on the Friday given above.

REMINDER: Sharing your answers with another student who is completing the assignment, even in another semester, is a violation of the academic integrity policies of this course. Please keep these answers to yourself.

Name (First Last) ____

Section __________ Andrew ID ______________________________

1. (1.5 pts) The Internet is based on a number of different communication protocols. Specifically, we saw that TCP/IP is used to send messages on the Internet from one device to another.

   a. What part of the communication process is handled by IP (Internet Protocol)?

   b. What parts of the communication process are handled by TCP (Transmission Control Protocol)?

   c. Why is TCP not designed to handle streaming real-time video data?

2. (1 pt) Using the original IPv4 addressing scheme, a computer at Carnegie Mellon University has the IP address `128.2.42.52` .

   a. For each of the four values in an IPv4 address, what is the maximum decimal value each can have? Why?

   b. In the original design of the IPv4 address, there were 3 classes of addresses.
   Class A addresses were IP addresses that started with the leftmost bit equal to 0.
   Class B addresses were IP addresses that started with the 2 leftmost bits equal to 10.
   Class C addresses were IP addresses that started with the 3 leftmost bits equal to 110.
   What class is the IP address `128.2.42.52` ? Show your work for full credit.

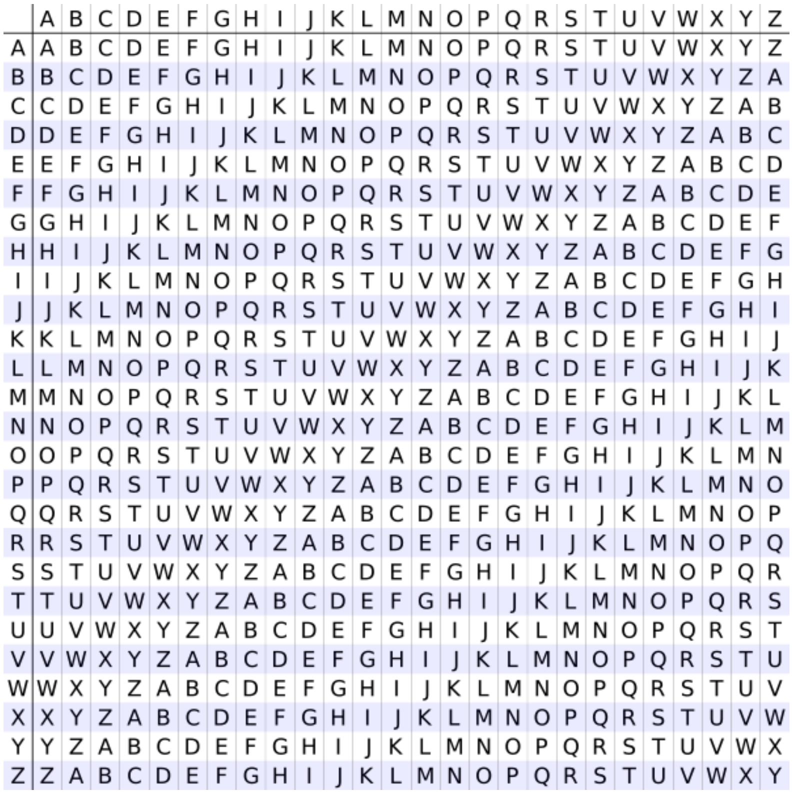
3. (1.5 pts) For early encryption, variations of shifting cyphers were used to encode and decode messages.

   a. The following message was encoded using a Caesar cypher. Decode it.

   BNWTPGIXHXCIWTLDGZ

   HINT: You can use a Python function like this to help you! (What does `ord` and `chr` do?)

```
def convert(message, shift):
#Assume message is all uppercase with no spaces/punctuation
    newmessage = ""
    for i in range(0, len(message)):
        distance = ord(message[i])-ord('A')  # distance from A
        newdistance = (distance + shift) % 26
        # append character at new distance
        newmessage = newmessage + chr(newdistance + ord('A'))
    return newmessage
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Vigenère table used for encoding and decoding messages. (Wikimedia Commons)

b. The Vigenère cypher is used to encode the following message with the key `FORBES`:

`PITTSBURGHPENNSYLVANIA`

Encode the message using the Vigenère table above and the given key.

c. Decode the following message encoded using the Vigenère table with the key `RIVERS`:

`RTGIXZVVTQFFFVBEYWCIJLZG`

(THINK CAREFULLY ABOUT HOW TO USE THE TABLE!)

4. (2.5 points) Ada uses a public key encryption system using RSA encryption that starts with two prime numbers p = 47 and q = 151. In this problem, you will compute values for Ada's public and private keys and then encode and decode a numerical message using these keys. (You should use python3 to help you with the large computations for this problem.)

   a. Compute the public key pair (e, n) and the private key pair (d, n) for this system. First compute n. Then compute r = (p-1)*(q-1). Then select the smallest value for e such that e and r are relatively prime. Finally select the smallest value for d such that (e*d) % r == 1. Show your work.

      HINT for e: divide 2 into r and see if it divides in evenly. If so, they're not relatively prime, so try 3 instead. If not 3, try 5, 7, 11, etc. until you find an e that does not divide in evenly. Then e and r are relatively prime (i.e. they do not share any common factors).

      HINT for d: once you know e, write a loop in Python that computes (e*d) % r for each d = 1,2,3, ... until you find a d such that the formula equals 1.

   b. Consider the numerical message 4117 (Tom's office number) that is to be transmitted to Ada. What is the encrypted message that should be transmitted to Ada using her public key pair (e,n) above? Fill in the blanks below to show the computation needed and the resulting encrypted message. (Use the Python3 interpreter to help with the arithmetic.)

      (______________ ** ______________) % _______________ = ________________

   c. Show how Ada decodes the encrypted message above using her private key pair (d,n). Fill in the blanks below to show the computation needed and the resulting decrypted numerical message. (Use the Python3 interpreter to check your answer.)

      (______________ ** ______________) % _______________ = ________________

5. (2 points) View the following videos on Youtube:

A System Designed For Answers	`https://www.youtube.com/watch?v=cU-AhmQ363I`
The Science Behind An Answer	`https://www.youtube.com/watch?v=DywO4zksfXw`
How It Works: IBM Watson	`https://www.youtube.com/watch?v=AtdJ1DGJjXA`

a. How does Watson use concurrency?

b. List the four main steps that Watson uses to answer a question on the *Jeopardy!* game show.

c. An example with a ship is used to illustrate how Watson has to determine meaning in a given input statement. List two ways that the sentence can be interpreted.

d. Just feeding Watson all available documents about a particular domain is not enough to build its knowledge base. What must also be done?

6. (1.5 points) As you learned from our guest lecture, robots and intelligent devices have to deal with a world of uncertainty in order to operate effectively to solve problems.

(a) Consider a robot with a camera that walks to a conference room each day, looking for a trash bin to pick up. Sometimes the bin is there, and sometimes it is not. Sometimes there are lunch meetings in the conference room.

Suppose the robot knows the following from observations of the past:

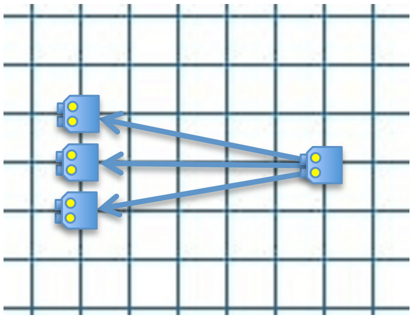
- The trash bin has been in the conference room for 10 of the past 20 days.
- There has been a lunch meeting in the conference room for 5 of the past 20 days.
- A lunch meeting has occurred 4 of the past 20 days when a trash bin has been present.

Given these observations, what is the probability that a trash bin is in the conference room given that there is a lunch meeting there? Express your final answer as a value between 0 and 1 or as a percentage chance between 0 and 100.

(HINT: Use Bayesian inference. Let A = 'trash bin is present', B = 'lunch meeting occurs', and you want to know P(A|B), the probability of A given B, which is equal to P(A) * P(B|A) / P(B).)

(b) The robot in the previous problem has to identify the trash bin in its video feed if the bin is there. For any particular, single frame of video, it may be difficult for the robot to identify the trash bin. Why?

(c) Consider another robot who walks forward 5 steps, then turns left 90 degrees. Let's assume that the robot can turn left 90 degrees accurately, but when it walks forward, it sometimes drifts so that it ends up in one of three locations, as shown below. (In all three cases, the robot is still facing forward, looking exactly in the same direction.)



The robot moves "forward" 5 steps and turns exactly left 90 degrees; it does this pair of instructions three more times to try to return to its starting location and orientation. How many different locations could the robot end up in when it is finally done?

(Try this out on graph paper if you get confused!)