

HW 2 CMSC 456. Morally DUE Sep 28
NOTE- THE HW IS FIVE PAGES LONG

1. (0 points)
 - (a) What is the day and time of the midterm?
 - (b) What is the day and time of the final?
 - (c) What is the *dead-cat policy*?
 - (d) What is the *mask policy*?

GOTO NEXT PAGE

2. (20 points) Alice and Bob are going to use the Vig cipher. (Note: Vig uses A is 0, B is 1, etc.) The keyword is *Kunal*. Alice wants to send *Bill's Ramsey Theory course is Awesome!*

What does Alice send?

Make it in blocks-of-five capital letters, though since its 32 letters it will be 6 blocks of 5 and then 2 letters.

You can either

- do this by hand,
- write a program to do it for you, or
- find software on the web to do it for you. If you do this then on the HW include the website of the software you used. ALSO say if the software you used leaked any information.

GOTO NEXT PAGE

3. (20 points) Let $\phi(n)$ be the number of numbers in $\{1, \dots, n\}$ that are relatively prime to n . EXAMPLES

$\phi(5) = 4$ since all the four elements $\{1, 2, 3, 4\}$ are rel prime to 5.

$\phi(p) = p - 1$ for any prime p .

$\phi(15) = 8$ since $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are the elements in $\{1, \dots, 15\}$ that are rel prime to 15.

NOTE: If p is a prime then p is rel prime to all $p - 1$ elements of $\{1, \dots, p - 1\}$ and hence $\phi(p) = p - 1$.

And now finally the problem

We will determine $\phi(143)$ without having to look at all of the numbers. We will need to factor $143 = 11 \times 13$. Note that a number is rel prime to 143 if it has *neither* 11 *nor* 13 as a factor.

- (a) (5 points) How many numbers in $\{1, \dots, 143\}$ have 11 as a factor. DO NOT do this by listing them all out. Show your work.
- (b) (5 points) How many numbers in $\{1, \dots, 143\}$ have 13 as a factor. DO NOT do this by listing them all out. Show your work.
- (c) (5 points) How many numbers in $\{1, \dots, 143\}$ have 11 AND 13 as a factor. DO NOT do this by listing them all out. Show your work.
- (d) (5 points) Using the information from the last three parts, and the law of inclusion-exclusion, find $\phi(143)$.
- (e) (0 points) Let p, q be two primes. Give a formula for $\phi(pq)$ in terms of p and q . Show your work.

GOTO NEXT PAGE

4. (20 points) Alice and Bob are using the Keyword-Shift Cipher with key the phrase

Mayim Bialik should host Jeopardy

and shift 1.

- (a) (7 points) Give the table that Alice uses to ENCODE messages.
- (b) (7 points) Give the table that Bob uses to DECODE messages.
- (c) (6 points) If Alice wants to send the message below, what does she send? (The answer should be in blocks of 5 all capitals.)
Almost all students have been vaccinated
- (d) (0 points- do not hand in) Does the ENCODE and DECODE tables look like this is a randomly generated permutation of $\{A, \dots, Z\}$ OR are there signs that it came from the keyword-Shift Cipher?

NOTE ON GRADING All three parts will be graded either 0 or full credit. If you get part 1 wrong and this leads to part 3 being wrong, we will get 0 on both parts. We will not check if YOUR part 3 is consistent with YOUR part 1. Hence **be careful and double check**.

GOTO NEXT PAGE

5. (40 points) Do the programming assignment that is just below this hw on the website and is labeled *Programming Assignment for HW 2*.