HW 2 CMSC 456. Morally DUE Sep 28
NOTE- THE HW IS SEVEN 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*?

GOTO NEXT PAGE FOR NEXT PROBLEM

2. (20 points–4 points each) Zan has two 4-sided dice d_1 and d_2.

   d_1 is NOT a fair die!

   $\Pr(d_1 = 1) = 0.1$

   $\Pr(d_1 = 2) = 0.2$

   $\Pr(d_1 = 3) = 0.3$

   $\Pr(d_1 = 4) = 0.4$

   d_2 is NOT a fair die!

   $\Pr(d_2 = 1) = 0.4$

   $\Pr(d_2 = 2) = 0.3$

   $\Pr(d_2 = 3) = 0.2$

   $\Pr(d_2 = 4) = 0.1$

   Zan will roll the two 4-sided dice and then take their sum s. What are the following (Express as both an exact fraction and decimal approximations):

   (a) $\Pr(s = 3)$

   (b) $\Pr(s = 3 \mid d_1 = 1)$

   (c) $\Pr(s = 3 \mid d_1 = 2)$

   (d) $\Pr(s = 3 \mid s \equiv 1 \pmod 2)$

3. (20 points—4 points each) For each of the following linear functions over mod 26 either give its inverse or tell me correctly that there is no inverse. Show your work.

   Here is an example of how we want the answer: If I ask about $f(x) = 9x + 8$ then do the following

   $y = 9x + 8$

   The inverse of 9 mod 26 is 3 so mult both sides by 3

   $3y = 27x + 24 = x + 24$

   $x = 3y - 24 = 3y + 2$.

   So answer is $g(y) = 3y + 2$.

   (a) $f(x) = x + 1$

   (b) $f(x) = 2x + 1$

   (c) $f(x) = 3x + 1$

   (d) $f(x) = 4x + 1$

   (e) $f(x) = 5x + 1$

GOTO NEXT PAGE

4. (20 points–10 points each.. BASED ON SLIDES Gen Sub and Random Looking Cipher) Let $c \geq 2$. Let $\Sigma = \{0, \ldots, c-1\}$ be the alphabet. Alice and Eve play the following game.

   - Alice flips a coin to get either RP (for Random Permutation) or SH (for Shift).
     – If she gets RP then she generates a random perm of Σ and sends it to Eve.
     – If she gets SH then she generates a random number $s \in \{0, \ldots, c-1\}$ and finds the permutation where $x \in \Sigma$ maps to $x + s \pmod{c}$, and sends that perm to Eve.
   - Eve looks at the perm she gets and yells out either RP or SH. If she is correct she wins. If not then Alice wins.

   (SOME STUDENTS thought that Alice would do a perm and THEN a shift of the perm. NO. The question clearly says that EITHER Alice's coin is RP, in which case she generates a random perm OR Alice's coin is SH, in which case she generates a shift s. SHE DOES NOT DO BOTH.)

   And now finally the problem:

   (a) Come up with a strategy for Eve that will win over half of the time (she will probability win a lot more than that). You may assume has Eve has unlimited computing power.

   (b) Given c find the probability that Eve loses when using the strategy above as a function of c. Show your work.

   GOTO NEXT PAGE FOR NEXT PROBLEM

5. (20 points. BASED ON SLIDES: Vig Cipher) Alice and Bob are going to use the Vig cipher. The keyword is *josh.* Alice wants to send

   Bill's course on Ramsey Theory last spring was awesome!

   Format it as blocks of 5, all capital, no punctuation. (NOTE: In the future I will not remind you of this.)

   What does Alice send? (You can either (1) do this by hand, (2) write a program to do it for you, or (3) find software on the web to do it for you. Let us know which one you did. If (3) then give us the website where you found it and say if the answer leaked information.)

   For the next problem

GOTO NEXT PAGE

6. (20 points—4 points each. NO SLIDES NEEDED) Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are relatively prime to n. EXAMPLES

   $\phi(5) = 4$ since all four elts of $\{1, 2, 3, 4\}$ 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 elts in $\{1, \ldots, 14\}$ that are rel prime to 15.

   And now finally the problem

   We will determine $\phi(91)$ without having to look at all of the numbers. We will need to factor $91 = 7 \times 13$. Note that a number is rel prime to 91 if it has *neither* 7 *nor* 13 as a factor.

   (a) (4 points) How many numbers in $\{1, \ldots, 91\}$ have 7 as a factor. DO NOT do this by listing them all out. Show your work.

   (b) (4 points) How many numbers in $\{1, \ldots, 91\}$ have 13 as a factor. DO NOT do this by listing them all out. Show your work.

   (c) (4 points) How many numbers in $\{1, \ldots, 91\}$ have 7 AND 13 as a factor. DO NOT do this by listing them all out. Show your work.

   (d) (4 points) Using the information from the last three parts, and the law of inclusion-exclusion, find $\phi(91)$.

   (e) (4 points) Let p, q be two primes. Give a formula for $\phi(pq)$ in terms of p and q.