HW 7 CMSC 389. DUE Jan 11

WARNING- THIS HW IS TWO PAGES

1. (0 points) What is your name? Write it clearly. Staple your HW. What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)

2. (50 points) We will look at various scenarios with Secret Sharing with Cards. The expression (a, b, c) will mean Alice has a cards, Bob has b cards, and Eve has c cards. You may assume that if the scenario is $(a, b, 0)$ then the number of bits Alice and Bob can share is $FLOOR(\log_2(\frac{(a+b)!}{a!b!}))$. For each of the following scenarios we want to know (1) What is the LEAST number of bits that Alice and Bob may end up sharing? (2) What is the LARGEST number of bits that Alice and Bob may end up sharing?

   (a) (6,6,10)

   (b) (6,6,9)

   (c) (6,6,8)

   (d) (6,6,7)

   (e) (6,6,6)

   (f) (6,6,5)

   (g) (6,6,4)

   (h) (6,6,3)

   (i) (6,6,2)

3. (50 points)

   (a) Find e such that the following happens: (1) for $(6, 6, e)$ the LEAST number of bits that Alice and Bob end up sharing is ZERO, (2) for $(6, 6, e-1)$ the LEAST number of bits that Alice and Bob end up sharing is NONZERO (probably just 1).

   (b) Find e such that the following happens: (1) for $(10, 10, e)$ the LEAST number of bits that Alice and Bob end up sharing is ZERO, (2) for $(10, 10, e - 1)$ the LEAST number of bitts that Alice and Bob end up sharing is NONZERO (probably 1).

(c) (Not to hand in) For a variety of numbers n find e such that the following happens: (1) for (n, n, e) the LEAST number of bits that Alice and Bob end up sharing is ZERO, (2) for $(n, n, e-1)$ the LEAST number of bits that Alice and Bob end up sharing is NONZERO (probably 1).

(d) Make a CONJECTURE about what $f(n)$ is such that (1) for $(n, n, f(n))$ the LEAST number of bits that Alice and Bob end up sharing is ZERO, (2) for $(n, n, f(n)-1)$ the LEAST number of bits that Alice and Bob end up sharing is NONZERO (probably 1). If this is difficult then make a conjecture about $f(n) + \Theta(1)$ or $O(f(n))$. (If you don't know what that means than just try to get an $f(n)$ that is APPROX right.)

4. (ONLY for those who on problem 1c on the exam wrote "1/7 is better" but DID not say why and hence got 5 points off. I annouced that you need to say why during the exam but some students (I think three) they didn't hear it. So if those students do THIS problem they can get back their 5 points.) Hand in the exam WITH your HW.

   (a) If Alice and Bob use 1/8 for their fraction then How would they encode 11010101000010101?

   (b) If Alice and Bob use 1/9 for their fraction then How would they encode 11010101000010101?

   (c) Which Faux-1-time-pad is better to use? AND WHY IS THAT?

5. (ONLY for those who on problem 5a wrong but did it quite clearly and just made a minor arithmetic mistake.) Find a linear function $f(x) = ax + b \pmod{26}$ such that $f(1) = 1$ and $f(2) = 8$. Show your work. Be VERY CLEAR. THIS problem they can get back their however many points we took off. Hand in the exam WITH your HW.