**HW 12, Due Jan 21**

READ THE NOTES ON SECRET SHARING WITH CARDS

THIS HW IS TWO PAGES LONG!!!!!!

**You may use: If Alice has $a$ cards and Bob has $b$ card and Eve has 0 cards then Alice and Bob can Share $\lfloor \binom{a+b}{b} \rfloor$ secret bits.**

1. (30 points) Alice has 4 cards, Bob has 2 cards, and Eve has 1 card.
   (a) Do the tree-of-scenarios noting for each leaf how many secret bits Alice and Bob share.
   (b) What is the most number of secret bits Alice and Bob can share?
   (c) What is the most least number of secret bits Alice and Bob can share?
   (d) What is the most average number of secret bits Alice and Bob can share?
2. (30 points) Alice has 3 cards, Bob has 3 cards, and Eve has 1 card.
   (a) Do the tree-of-scenarios noting for each leaf how many secret bits Alice and Bob share.
   (b) What is the most number of secret bits Alice and Bob can share?
   (c) What is the most least number of secret bits Alice and Bob can share?
   (d) What is the most average number of secret bits Alice and Bob can share?
3. (0 points but do for review) Assume that there are $n$ cards and Eve will be getting $e$ cards. Alice and Bob may get the same number of cards (called SAME) or a diff number of cards (DIFF).
   (a) Alice and Bob want to maximize the number of bits they get in the best case. Should they do SAME or DIFF?
   (b) Alice and Bob want to maximize the number of bits they get in the worst case. Should they do SAME or DIFF?
   (c) Alice and Bob want to maximize the number of bits they get in the avg case. Should they do SAME or DIFF?

4. (20 points) Alice has $n$ cards, Bob has $n$ cards, Eve has $n$ cards.

   (a) Assume that EVERY time Alice or Bob says *I have a* $c_1$ *or* $c_2$ the other says I DO ALSO! How many secret bits will they share?

   (b) Assume that EVERY time Alice or Bob says *I have a* $c_1$ *or* $c_2$ the other says I DO NOT! How many secret bits will they share? (You can use the web to see how to approximate factorials.)

5. (20 points) Give $a, b, c, n$ such that $a, b, c \in \{1, \ldots, n-1\}$, $n \geq 2016$, and the equation $ax^2 + bx + c \equiv 0 \pmod{n}$ has at least $\sqrt{n}$ solutions in the set $\{0, 1, \ldots, n-1\}$.