Homework 10, Due Wed July 29, 2015

WARNING- THE HW IS **THREE** PAGES.

THIS HW IS PRACTICE PROBLEMS FOR THE FINAL.

1. (15 points) The Venus alphabet has 20 letters.

   (a) If they want to use an affine cipher where x is coded by $ax + b \pmod{20}$ what values of a ARE allowed.

   (b) How many ways can they do a general substitution cipher?

2. (15 points) Alice and Bob are going to use Diffie Helman to establish a shared secret key. Alice says *lets use a prime p such that $p - 1 = 2q_1q_2$ where q_1, q_2 are primes.* Is this a good idea? Explain?

3. (20 points) Recall that there is a variant of Baby-Step Giant-Step that takes $p^{1/10}$ space and $p^{9/10}$ time. Try to come up with a variant that takes $p^{9/10}$ space and $p^{1/10}$ time. Either DO THIS OR tell us why you CAN"T DO THIS. (If its CAN'T DO THIS the reason can't be *because I didn't feel like it*, it has to be a math reason.)

4. (15 points) Alice and Bob and Eve are dealt cards from the deck $\{1, \ldots, 20\}$.

   Alice gets $\{1, 4, 11, 14, 15, 16, 20\}$.

   Bob gets $\{2, 3, 7, 8, 9, 18, 19\}$.

   Eve gets $\{5, 6, 10, 12, 13, 17\}$.

   Alice and Bob will attempt Secret Sharing with Cards. They agree ahead of time that if Alice has the lower card of a pair than the shared secret bit is 0, otherwise it is 1.

   (a) Assume that every time one of Alice or Bob says 'I have a BLAH or a BLAH' the other one says I HAVE THAT ALSO! How many shared secret bits do Alice and Bob share?

   (b) Assume that every time one of Alice or Bob says 'I have a BLAH or a BLAH' the other one says I DO NOT HAVE THAT! How many shared secret bits do Alice and Bob share?

GOTO NEXT PAGE

5. (20 points) Alice wants to send an 8-digit sequence of digits to Bob and wants to include some error detection. So she sends the 8 bits of content and also the bit

$$a_9 \equiv a_1 + 4a_2 + a_3 + 4a_4 + a_5 + 4a_6 + a_7 + 4a_8 \pmod{10}$$

   (a) Give an example of a single-digit error that goes undetected (and that digit that has the error is NOT a_9). Give both the 9-digits $a_1a_2 \cdots a_8a_9$ that were meant to be sent and the 9 digits that arrived (which is incorrect in one digit) and say why the error was not detected.

   (b) What is the probability that an adjacency-transposition error will NOT be detected?

6. (15 points) (READ both parts of the question before you do it.)

   (a) Make up a problem for this course on Huffman coding (coding so that more freq letters are shorter) where you give the students eight letters $\{a, b, c, d, e, f\}$ and their frequencies, and they produce the Huffman coding- BUT- you want the answer to be that

   a is coded by a string of length 1,

   b is coded by a string of length 2,

   c is coded by a string of length 3,

   d is coded by a string of length 4,

   e is coded by a string of length 5,

   f is coded by a string of length 5 (this is NOT a typo- it is 5).

   (b) DO the problem you just made up. Show your work. Do not refer to the work you did in the first part.

GOTO THE NEXT PAGE

7. (0 points but for your own benefit for the final) For every cipher we studied in the class

   (a) What values of the parameters are valid (e.g., for Affine, x goes to $ax + b \pmod{26}$, a has to be YOU SHOULD KNOW THIS).

   (b) What are some of the PROS of the cipher?

   (c) What are some of the CONS of the ciphers?

8. (0 points but for your own benefit for the final) Go over ALL of the HWs and the Midterm.