CMPS/MATH 2170 Discrete Mathematics – Fall 13

10/28/13

8. Homework

Due **11/6/13** at the beginning of class

1. **Linear Congruence (2 points)**
   Solve the congruence $3x \equiv 5 \pmod{11}$.

2. **Prime (3 points)**
   Prove that if n is a positive integer such that the sum of the divisors of n is $n+1$, then n is prime.

3. **RSA (8 points)**
   The following problem walks you through the cryptanalysis of a message sent with the RSA cryptosystem. Suppose two people are communicating, call them Carola and Ellis, and Carola sends Ellis a message with RSA. She accidentally forwards you a copy of this message: "8 9 17 17 25 21 12 25 24 9 3 8 1 24 3 13 23 12 25 25 14 7 21 14 2, I've encrypted the cipher key with your RSA public key, and the encrypted cypher key is 62". You know Carola is notorious for having poor security practices – she sends messages with a *shift cipher*, where every letter is represented by a number between 1-26 ($A \equiv 1 \pmod{26}, B \equiv 2 \pmod{26}, \ldots, Z \equiv 0 \equiv 26 \pmod{26}$), and each such letter-number is decrypted by adding a cipher key, modulo 26, to it. Carola's message is obviously shifted with some key; if you convert the numbers above to letters you get "H I Q Q Y U L Y X I C H A X C M W L Y Y N G U N B", which does not make any sense. So, if you can find the cipher key, a number between 0 and 25, you can add it to each number above, and then the resulting number will represent each letter in the message! You go to Ellis' website and look up his RSA public key and see that it is $(43, 77)$. You notice that Ellis' public key is 43 and he has chosen $n = 77$, which is a shockingly low number (he must be very bad at crypto, too), so you suspect you can break the cryptosystem, and you hope the message has some secret information about the final exam. We will break the system and find the message, step by step.

   (a) (1 point) n is small – factor it into prime numbers, and find p, q prime such that $p \cdot q = n$. Our inability to do this step for sufficiently large n is what protects the security of RSA.

   (b) (1 point) The exponents work modulo $\phi(n)$, so find $\phi(n) = (p-1)(q-1)$.

   (c) (2 points) Ellis' public key is 43, so his private key must be the inverse of 43, $(\text{mod } \phi(n))$. Find it.

   (d) (3 points) Now you have Ellis' private key, d. Use it to decrypt the cipher key. (Here, the message is 62, the encrypted cipher key. Remember, the clear text you are looking for should be the ciphertext $c = 62$, raised to Ellis' private key, which you found in the last step, reduced modulo $n = 77$.

Flip over to back page $\Longrightarrow$

(e) (1 point) Now that you have the cipher key, add it to every number in the original message, convert each to a letter, and write the final message.

(f) (Bonus; 1 bonus point) Now that you have Ellis' private key, you can pretend to be him. Take the number $'2'$ and encrypt it with Ellis' private key, so Carola will think only he could have sent it. (Carola recently asked Ellis, on a scale of 1-10, how hard the next homework should be. You are sending $'2'$ because sending $'1'$ would be too suspicious).

4. **Counting (5 points)**

   (a) (1 point) How many license plates can be made using either three digits followed by three letters, or three letters followed by three digits?

   (b) (1 point) How many Boolean functions are there with m input bits, and one output bit?

   (c) (1 point) How many onto functions are there from $\{1, 2, \ldots, m\}$ to $\{1, 2\}$? *(Hint: How many functions are there, and how many are not onto?)*

   (d) (1 point) How many bit strings of length seven begin with two 0s or end with three 1s?

   (e) (1 point) How many different initials can someone have if a person has at least two, but no more than five, different initials? Assume that there are 26 letters in the alphabet.