Computer Science Department - Rutgers University **Fall 2018**

CS 205: Homework Set 4

16:198:205 (Sections 4 - 6)

Complete each of the following problems to the best of your ability. Remember, you can't be graded on what you don't write down so (unless you are just making stuff up) something is better than nothing. Discussing problems between each other is fine, but your final writeup and work must be your own.

- **Modular Arithmetic and RSA** Recall the setup of an RSA cryptosystem: it consists of five numbers (p, q, n, e, d) such that p, q are prime,

$$\begin{aligned} n &= p * q \\ \text{GCD}(e, (p-1)(q-1)) &= 1 \\ ed &\equiv 1 \pmod{(p-1)(q-1)} \end{aligned} \tag{1}$$

The pair (e, n) are published for all to see, while (p, q, d) are held privately by you; these are the public encryption keys and the private decryption keys respectively.

To encrypt a message like 'ABCDEF', translate that into a series of digits (for instance A to 01, B to 02, Z to 26) etc, so the message becomes 010203040506 and partition that into a sequence of *blocks* numbers such that each number is less than n. In this case, you might have 010, 203, 040, 506. A block M is then encrypted using the following map:

$$M \mapsto M^e \pmod{n}, \tag{2}$$

and an encrypted block C (C for ciphertext) is decrypted by the following map:

$$C \mapsto C^d \pmod{n}. \tag{3}$$

Once each block of a message is decrypted, the digits can be worked backwards into the original message (potentially padding things out with 0's as necessary, $10 \mapsto 010$ for example).

The functionality of the system rests on the fact that if $C \equiv M^e \pmod{n}$, then $M \equiv C^d \pmod{n}$. The *security* of the system rests on the fact that if all an attacker knows is e, n, and the encrypted message C, is is very hard computationally to work backwards and determine M.

1) Your published encryption keys are $n = 2881$, and $e = 13$. Note, this corresponds to $p = 67, q = 43$. Show that $\text{GCD}(e, (p-1)(q-1)) = 1$, and show your steps.
2) Determine a decryption key d for this system. Show your steps.
3) You receive the following encrypted message (a sequence of encrypted C blocks):

   1481, 470, 2093, 2804, 1286, 1526, 1170, 1437, 2350, 585, 1864, 1436, 203

   Decrypt each block to reveal the original block M, and then reconstruct the original message. Obviously, you're going to want to try to compute C^d mod n as efficiently as possible.
4) Suppose that someone sent you a message using an encryption key that you had stopped using a long time ago, so long in fact that all you remembered was the value of e, and the value of p. What steps could you go through to try to decrypt the message? In short, given a value of e and p, and an encrypted message C, how could you find (or at least narrow down the range of possible suspects) for the values of q, n, and d? Don't forget the fact that (ideally) C represents an encrypted message in some natural language.

- **Induction** Recall that any proof by induction generally functions in two parts: a) show that if a smaller version of the problem can be solved, then a larger version of the problem can be solved; c) show that the 'smallest' version or versions of the problem can be solved.

  1) You want to buy some cats, but cats are only sold in batches of 3 or 5. Prove inductively that for any $n \geq 8$, there is a way to purchase exactly n cats.

  2) Let $F(n)$ be the number of ways of arranging $n \geq 1$ unique items in a row. Prove inductively that $F(n) = n!$.

  3) Prove inductively that for any real number $x \neq 1$, for any integer $n \geq 0$ we have

  $$1 + x + x^2 + \ldots + x^{n-1} + x^n = \frac{x^{n+1} - 1}{x - 1}. \tag{4}$$

  4) Use the result of the previous problem to argue that if $|x| < 1$, then

  $$\sum_{i=0}^{\infty} x^i = \frac{1}{1 - x}. \tag{5}$$

     What can you conclude from the previous problem if $x = 1$ or $x = -1$ though?

  5) In class, it was argued that for $n \geq 4$, a knight can reach every square on an $n \times n$ size chessboard. Are there any $3 \times n$ chessboards that have the same property? What can you prove for these rectangular boards?