Assignment #7

Announcement: Office hours this week (May 24-28): Monday, May 24, 11:00-12:00; Wednesday 11:00-12:00 as usual; Thursday 1:30-2:00 (and I can't be available informally after discussion section).

Reading: §10B and §§13A-E.

These problems are due **Friday, May 28**. (I had said they would be due the following Monday, but that's Memorial Day, so instead this is a shorter assignment due on the usual day.)

To do but not hand in:

M-1, M-3, M-4, and M-6.

To hand in:

M-2, M-5, M-7, and M-8.

Problem M-1. The Amazon public modulus is listed as 1024 bits but the number given in the printout is in decimal. See if it has the expected number of digits. (Of course, if the first decimal digit were 0 it could be a little shorter. Method: Use logs. What is the relationship between the number of decimal digits of a positive integer and its log to the base 10? Binary digits [bits] and its log to the base 2? Between logs to different bases?)

Problem M-2. For this problem, my public key consists of the modulus $n = 22548521$ and exponent $e = 17$. Choose an English word of up to four letters, encode it using the simple code A = 01, B = 02, etc. (as in Problem I-3), RSA-encrypt it using the calculator on the class home page, and send the ciphertext to me in email at `baker@math.ucla.edu` . I'll try to decrypt.

Problem M-3. In the text (p. 201, Ex. 15) a *safeprime* is defined to be a prime p such that $(p-1)/2$ is also prime. If p_1 and p_2 are distinct safeprimes, describe the prime factorization of $\phi(n)$ for $n = p_1 p_2$. (An RSA public modulus n is considered safer if it doesn't have lots of small prime factors.)

Problem M-4. Some parts of the Rijndael algorithm treat bytes as as elements of $\mathbb{F}_{2^8}$, using the particular basis $\alpha^7, \alpha^6, \ldots, \alpha, 1$ of $\mathbb{F}_{2^8}$ over $\mathbb{F}_2$ where $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$. If $r =$ `00010001` and $s =$ `00010010`, (a) Find $r + s$ and (b) find rs, as bytes.

Problem M-5. Suppose you put the byte `00000010` (which is α itself) into Step 1 of Rijndael. What byte comes out?

(Method: To find α^{-1}, take the equation $\alpha^8 = \ldots$ in Handout L §4, multiply through by α^{-1}, solve for it, and express it as a byte. Then do 1(b), 1(c).)

Problem M-6. For $\mathbb{F}_{2^8}$, list the possible orders of nonzero elements. (See Handout H, (d)-(iii) and the example.)

Problem M-7. With RSA, Alice chooses secret primes p, q and makes $n = pq$ public, but keeps $\phi(n) = (p-1)(q-1)$ secret and uses it for decryption. We are told that the security of RSA depends on the difficulty of factoring n to find p and q. But here's a thought: Might it be possible just to find $\phi(n)$ directly somehow, and might that not be easier than factoring n? No, this thought is not helpful, because from knowing $\phi(n)$ and n you can find p and q anyway, by combining the following steps (a) and (b):

(a) Show that for $n = pq$, if you know n and $\phi(n)$ (but not p and q), then from easy algebra you can find $p + q$, so you know both $p + q$ and pq.

(b) For unknown numbers r_1 and r_2, if you know their sum S and product P, give expressions for r_1 and r_2 in terms of S and P. Assume $r_1 < r_2$.

(Method: Find a quadratic polynomial whose roots are r_1 and r_2 and solve for the roots using the quadratic formula.)

(c) Find primes p, q such that $n = 3551$ and $\phi(n) = 3432$. (Use the specific method of (a) and (b) and show the calculation. You may use a calculator for the arithmetic and square root.)

Problem M-8. This problem concerns vector spaces over $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

(a) List all the 1-dimensional subspaces of F^3. Each subspace can be described as consisting of two triples.

(Recall that a 1-dimensional subspace has a basis consisting of a single vector $\mathbf{v}$ and so consists of all scalar multiples $r\mathbf{v}$. But for $F = \mathbb{F}_2$ the only scalars are 0 and 1.)

(b) List all the 2-dimensional subspaces of F^3. There should be seven, each with four elements. (Try possible two-element bases and find their spans, while avoiding bases that are entirely inside a subspace you have already listed.)

(c) Show how to solve Problem G-2 by using 1-dimensional subspaces to correspond to plants and 2-dimensional subspaces to correspond to blocks. The plants in a block consists of all 1-dimensional subspaces contained in the given 2-dimensional subspace.