Homework 6, 550.371 Cryptology and Coding, Spring 2017

You may discuss generalities of mathematics and MATLAB with others in the class, but the solutions and code that you submit should be entirely your own.

Problem 1: Prove that for any prime p and integer $k \geq 1$ it holds that $\phi(p^k) = (p-1)p^{k-1}$.

Problem 2: Write a MATLAB function that performs fast exponentiation. The input consists of positive integer n, $a \in \mathbf{Z}_n$, and a positive integer power k. The output is a^k mod n. Be sure to provide nontrivial examples to illustrate that your code is working properly.

Problem 3: Suppose p and q are different prime numbers, and let $n := p \cdot q$. Give a very simple formula for finding p and q using only n and $\phi(n)$. Explain why this illustrates that there (almost assuredly) isn't an efficient algorithm for computing $\phi(n)$, if you are only given the number n and nothing more.

Problem 4: Suppose Bob has public RSA key $(n, e) = (8439833, 5711029)$ and Alice sends him the ciphertext $c = 62472$ encrypted with Bob's key. Find the corresponding plaintext m. (Hint: MATLAB can factor the RSA modulus n because it isn't big enough.)

Problem 5: Write a MATLAB program whose input consists of two primes $p, q \equiv 3 \bmod 4$ and $c \in \mathbf{Z}_{pq}$. The output should be the four square roots of c mod pq, if they exist (in other words, your program does Rabin decryption). Use your code to find the four square roots of 6245706 mod 9353881. (Hint: The number 9353881 isnt too big for MATLAB to factor; use the command "factor." Also, the command "format rat" will ensure that all data is displayed and stored as integers.)

Problem 6: Let p and q be primes such that $q = 2p + 1$, and consider any $a \in \mathbf{Z}_q$ such that $a \neq 0, 1, -1 \bmod q$. Prove that a is primitive mod q if and only if $a^p = -1 \bmod q$.