CSCI3381 Cryptography-Assignment 4
Basic Number Theory

due Wednesday, March 15 at 11:59 PM

February 28, 2017

1 Pencil and Paper Problems

Note: You MUST use either LaTeX or the equation editor in MS Word for this (no .txt or .md files.)

1. Find $x, y \in \mathbf{Z}$ such that $17x + 101y = 1$.

2. Find $17^{-1} \bmod 101$.

3. Compute $\gcd(4883, 4369)$.

4. Use the result of the preceding problem to factor 4883 and 4369 into primes.

5. Evaluate $7^7 \bmod 4$.

6. Use the preceding problem to find the last digit of 7^{7^7}. (Keep in mind that 7^{7^7} means $7^{(7^7)}$.)

7. Find the last two digits of 123^{562}, without having to write down any number with more than 3 digits. (HINT: Use the Chinese Remainder theorem to convert this into a problem about two smaller, relatively prime, moduli.)

8. (Factoring with primes that are too close together.) This is a somewhat harder math problem. The result will be used in one of the computer problems below, but you do not need to have completed the proof here to tackle the computer problem.

   Suppose $N = pq$, where $p < q$ are primes, and $q - p < \sqrt[4]{N}$. Let us take $A = \frac{p+q}{2}$, so that $p = A - x$, $q = A + x$, and thus

   $$N = A^2 - x^2,$$

or, equivalently,

$$x = \sqrt{A^2 - N}.$$

Prove that $A = \lceil \sqrt{N} \rceil$. Thus if the primes p, q are too close together, we can efficiently compute from N (see below) both A and x, and thus the factors p and q.

2 Computer Problems

1. Let $K < N$ be relatively prime to N, where $N = pq$ is the product of two distinct unknown primes p and q. You can find the factors of N, provided the square roots are not additive inverses (*i.e.*,

   $$x^2 \equiv y^2 \equiv K \pmod{N},$$

   but $x \not\equiv \pm y \pmod{N}$. The reason, recall, is that in this case

   $$N | x^2 - y^2 = (x - y)(x + y),$$

   but N divides neither of the factors $x - y, x + y$, and thus has a nontrivial factor in common with N. Show Python computations demonstrating that x, y given in the accompanying text file have the same square mod N, and find the factorization of N.

2. While it is in general difficult to find square roots, cube roots, and the like modulo some divisor N, it is easy to find integer square roots and cube roots in ordinary, rather than modular arithmetic. Write an *efficient* function `kthroot(N,k)` which on input of an integer N and an exponent k, returns $m = \lfloor \sqrt[k]{N} \rfloor$. Observe that k must be reasonably small (less than $\log_2 N$) for the answer to be anything but 1, so you may assume $k < \log_2 N$. (HINT: Use binary search.)

3. The integer M in the attached text file has 202 decimal digits, and is the product of two primes p, q, each with 101 digits. I chose p and q by fixing the high-order 61 digits of each number and then generating the last 40 digits randomly, picking the smallest prime greater than the result. Use the attack described in the last problem of the written part, as well as the function you wrote in the preceding problem, to find p and q.