Problem Set 3

This problem set is due **at 8:00pm** on **Friday, December 6, 2024**.

- The TAs will provide a detailed document describing how you should submit your PDF and code on Google Classroom (we may use gradescope for some things). Make sure you read it! We suggest that you perform a trial submission prior to the deadline to make sure that everything works for you – you can overwrite that submission with a new one up to the deadline.
- We require that written solutions are submitted as a PDF file, **typeset on LaTeX**, using the template available on Google Classroom. You must **show your work** for written solutions. Each solution should start on a new page.
- We will occasionally ask you to "give an algorithm" to solve a problem. Your write-up should take the form of a short essay. Start by defining the problem you are solving and stating what your results are. Then provide: (a) a description of the algorithm in English and, if helpful, pseudo-code; (b) a proof sketch for the correctness of the algorithm; and (c) an analysis of the running time.
- We will give full credit **only** for correct solutions that are described clearly and convincingly.

Problem 3-1. Some basics [60 points]

(a) [20 points]

An element $a \in Z_n - 0$ is said to be a zero divisor modulo n if $ab \equiv 0 \mod n$ for some $b \in Z_n - 0$. Each of the following questions is worth 4 points.

1. Explain why there are no zero divisors in Z_p when p is prime.
2. Find a zero divisor in Z_{39}.
3. What is the value of the first element to repeat: $5^1, 5^2, 5^3, \ldots \mod 39$?
4. Do you think it is possible to find a non-zero number $x \in Z_{39}$ and a number $k \geq 0$ such that $x^k \equiv 0 \mod 39$? Why or why not? Would your answer change for some RSA modulus n other than 39?
5. Suppose n is not required to be an RSA modulus. Can you find numbers n, x, k such that $x \not\equiv 0$ but $x^k \equiv 0 \mod n$?

In all cases, justify your answers.

(b) [10 points] The definition of greatest common divisor can be extended naturally to a sequence of numbers $(a_1, a_2, a_3, \ldots, a_k)$, not all of which are zero. Namely, it is the largest integer $d \geq 1$ such that $d|a_j \forall j = 1, 2, \ldots, k$. Describe an efficient algorithm for computing $gcd(a_1, a_2, a_3, \ldots, a_k)$, and explain why it computes the correct answer.

(c) [15 points]

Each of the following problems is worth 5 points. You must show your work (you will get 0 otherwise).

1. Euler's totient function: Compute $\phi(2200)$;
2. Euler theorem: Compute $3^{591207} \mod 2200$
3. Use the extended Euclidean algorithm to solve the Diaphantine equation: $539x - 1387y = 1$

(d) [15 points]

Bob's public RSA key is $n = 1501, e = 323$. Eve manages to learn that his decryption key is $d = 539$. Implement the randomized factoring algorithm from your slides. Use your program to factor n. Once you have the factorization of n, compute $\phi(n)$, and check your answer by verifying that $ed \equiv 1 \mod \phi(n)$.

Problem 3-2. Primitive Roots [15 points]

(a) [7 points] Find a primitive root g of $p = 761$ and use the Lucas test to prove that you have one.

(b) [8 points] Find a non-trivial (not 1 or $p - 1$) number $g \in Z^*_{761}$ that fails to be a primitive root of p, and use the Lucas test to prove your answer correct.

Problem 3-3. Secret Sharing [25 points]

Implement simple k out of n Shamir secret sharing as described in class. You don't need any network communication: just start with a secret value s and whatever public values you need (primes etc.), and then demonstrate: splitting, reconstruction, addition of two shares, addition of a share with a public value, multiplication of a share with a public value. Comment your code in detail.

For 25 points of extra credit, you can implement multiplication of two shares. For a further 15 points, you can implement Beaver triples.