Final Exam – Math 173A

Instructor: Liam Hardiman

July 28, 2022

Instructions:

- You must show your work and clearly explain your line of reasoning.
- You may use a calculator, but only for basic arithmetic. If you didn't bring a calculator, you may use your phone, but it must be set to airplane/flight mode and you must clear all notifications before you start.
- You may use one sheet (front and back) of handwritten notes (or a printed sheet of digitally handwritten notes).
- You have 90 minutes to complete the exam.

GOOD LUCK!

1. (10 points)

   (a) (4 points) Show that if $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$, then $\gcd(x + y, n)$ is a nontrivial factor of n

   (b) (6 points) Let $N = pq$ be a product of two large, distinct, and unknown primes. Suppose you have access to an oracle that accepts as input an integer a and returns an integer b such that $b^2 \equiv a \pmod{N}$. If no such b exists, the oracle returns the symbol $\perp$.

   Explain how you can use this oracle to factor N. You may use results from your homework or lecture about square roots modulo N without proof (be sure to state them clearly, though).

2. (10 points)

   (a) (4 points) Show that the RSA encryption scheme that we've studied is *homomorphic*. That is, show that if we know the encryptions of messages m_1 and m_2, then we can easily obtain the encryption of the message $m_1 m_2$ *without learning the private key.*

   (b) (6 points) Bob uses RSA to receive a single ciphertext c corresponding to the message m. His public modulus is N and his public encryption exponent is e. Bob agrees to decrypt any ciphertext Eve sends to him and show her the result as long as Eve does not send him c. Eve sends Bob the ciphertext $2^e c \pmod{N}$. Show how Eve can use this to find m.

3. (10 points)

   (a) (4 points) What kinds of numbers are Pollard's $p-1$ algorithm particularly good at factoring? Why?

   (b) (6 points) Use Pollard's $p-1$ algorithm to factor 1649.

4. (10 points) Samantha sets up the parameters so she can sign documents with the ElGamal signature scheme. She publishes a large prime p, a primitive root g modulo p, and a verification key $A \equiv g^a \pmod{p}$ corresponding to her private signing key $1 \leq a \leq p-1$.

   Eve chooses u and v such that $\gcd(v, p-1) = 1$ and computes

$$S_1 \equiv A^v g^u \pmod{p} \qquad \text{and} \qquad S_2 \equiv -S_1 v^{-1} \pmod{p-1}.$$

   (a) (7 points) Show that the pair (S_1, S_2) is a valid signature for the document $D \equiv S_2 u \pmod{p-1}$. Of course, it's likely that D is a meaningless document.

   (b) (3 points) Recall that a *hash function* takes in a document of arbitrary size and returns an integer of a fixed size (assume it returns an integer modulo $p-1$ for this problem). This function is difficult to invert.

   Suppose a hash function h is used so that Samantha's signature must be valid for $h(D)$ instead of for the document D itself. Explain how this protects against the forgery outlined in part (a).

5. (10 points) Alice chooses two large primes p and q. She chooses an integer e relatively prime to $(p-1)(q-1)$ and computes d such that $de \equiv 1 \pmod{(p-1)(q-1)}$. Her RSA public key is $N = pq$ and e.

   Suppose Alice also computes the following values

$$d_p \equiv d \pmod{p-1} \qquad \text{and} \qquad d_q \equiv d \pmod{q-1}.$$

   (a) (7 points) Bob chooses a message m and sends Alice the ciphertext $c \equiv m^e \pmod{N}$. Instead of computing $c^d \pmod{N}$ to recover m, Alice instead computes

$$m_1 \equiv c^{d_p} \pmod{p} \qquad \text{and} \qquad m_2 \equiv c^{d_q} \pmod{q}.$$

   Explain how she can use m_1 and m_2 to recover m.

   (b) (3 points) Do you think this method is more or less efficient than just computing $c^d \pmod{N}$? Why?

6. (10 points) Let p be a prime and let g be an integer. The *Decision Diffie-Hellman Problem* is as follows. Suppose that you are given three numbers A, B, and C, and suppose that A and B are equal to

$$A \equiv g^a \pmod{p} \qquad \text{and} \qquad B \equiv g^b \pmod{p},$$

but that you don't necessarily know the values of the exponents a and b. Determine whether C is equal to $g^{ab} \pmod{p}$.

Prove that an algorithm that solves the Diffie-Hellman problem can be used to solve the decision Diffie-Hellman problem.