Math 470 section 502, Spring 2023
Exam 1

FIRST NAME: _____

LAST NAME: _____

UIN:_____

Instructions:

- No calculators, notes, formula sheets, phones, tablets, etc.
- Justify your answers, unless explicitly stated otherwise.
- The exam will be graded out of 50 points. There are a total of 53 points available.

---

1. (a) (2 points) Decode the following Caesar cipher:
RERXXZVUFVJEFKCZVTYVRKFIJKVRCFIKFCVIRKVKYFJVNYFUF

   (b) (1 point) Draw/write your signature below if you promise to abide by the message you decoded in part (a) for the duration of this exam.

SIGNATURE: _____

2. **NO JUSTIFICATION REQUIRED.**

(a) (2 points) Let m be a positive integer and let a be an integer. Write the definition of an "inverse of a modulo m".

(b) (2 points) Let p be a prime and let a be an integer not divisible by p. Write the definition of "the order of a modulo p".

(c) (2 points) You publish a prime p and primitive root g mod p. You choose a secret exponent s and publish g^s mod p as your Elgamal public key. Alice sends you a ciphertext (c_1, c_2). How do you decrypt this ciphertext to recover Alice's message?

(d) (2 points) Bob has published a pair of integers (N, e) as his RSA public key. You want to send Bob a message m. How do you encrypt your message?

3. Show your steps. **Your final answer should be an integer between 0 and 49 (if it exists).**

(a) (3 points) Compute the inverse of 19 modulo 50, or explain why it does not exist.

(b) (3 points) Compute the inverse of 18 modulo 50, or explain why it does not exist.

(c) (3 points) Compute 2^{17} modulo 50, or explain why it does not exist.

4. (8 points total, 2 points each) For each of the following statements, write
   - "True" if the statement is known to be unconditionally true,
   - "False" if the statement is known to be unconditionally false,
   - "Unknown" if it is not known (according to public knowledge) whether the statement is true or false.

   In this problem, "efficiently" means "in polynomially many steps with respect to the input size."
   NO JUSTIFICATION REQUIRED.

   (a) There does not exist an algorithm that can always efficiently solve the Discrete Logarithm Problem.

   (b) If Eve can efficiently solve the Discrete Logarithm Problem, then Eve can efficiently break the Diffie-Hellman key exchange protocol as a passive eavesdropper.

   (c) If Eve can efficiently compute shared secret values in the Diffie-Hellman protocol as a passive eavesdropper, then Eve can efficiently solve the Discrete Logarithm Problem.

   (d) If Eve can efficiently decrypt ciphertexts in the Elgamal encryption protocol, then Eve can efficiently solve the Diffie-Hellman Problem.

5. (8 points) Prove that if p, q are distinct primes and m is an integer such that $p|m$ and $q|m$, then $pq|m$.

6. (8 points) Find an integer x such that $2^x \equiv 9 \mod 53$ **using the Pohlig-Hellman algorithm.** (if you find it by other means, or if you don't show the steps of the Pohlig-Hellman algorithm, you will get 0 points)

   Note that 53 is prime, $53 = 4 \cdot 13 + 1$, and 13 is prime.

   You may use some of the following congruences modulo 53:

   - $2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^{13} \equiv 30, \quad 2^{26} \equiv 52, \quad 2^{39} \equiv 23 \quad$ (all mod 53)
   - $9^2 \equiv 28, \quad 9^4 \equiv 42, \quad 9^{13} \equiv 52, \quad 9^{26} \equiv 1, \quad 9^{39} \equiv 52 \quad$ (all mod 53)
   - $4^2 \equiv 16, \quad 16^2 \equiv 44, \quad 30^2 \equiv 52, \quad 52^2 \equiv 1, \quad 23^2 \equiv 52 \quad$ (all mod 53)
   - $4^8 \equiv 28, \quad 16^8 \equiv 42, \quad 30^8 \equiv 1, \quad 52^8 \equiv 1, \quad 23^8 \equiv 1 \quad$ (all mod 53)

---

7. (a) (3 points) Alice and Bob run the Diffie-Hellman key exchange protocol using the following prime p and primitive root g modulo p:

$$p = 145679513119433700633158339007149501 39$$
$$g = 2$$

Note that the prime factorization of $p - 1$ is

$$p - 1 = 2 \cdot 151 \cdot 653 \cdot 738717448350626758988866155224 23$$

Based on what you have seen in lectures, do you believe that a passive eavesdropper Eve can quickly compute their shared secret (say with at most a billion arithmetic operations)? Give a brief justification.

(b) (3 points) Alice and Bob run the Elgamal encryption protocol using the following prime p and primitive root g modulo p:

$$p = 145679513119433700633158339007149506 57$$
$$g = 7$$

Note that

$$p = 2^{87} \cdot 3^{23} + 1$$

Based on what you have seen in lectures, do you believe that a passive eavesdropper Eve can quickly decrypt their Elgamal ciphertexts (say with at most a billion arithmetic operations)? Give a brief justification.

8. (Bonus 3 points) Recall the Collision algorithm for computing discrete logarithms on primitive roots:
   - Input: prime p, primitive root g mod p, and target value $h \in (\mathbb{Z}/p\mathbb{Z})^*$.
   - Output: an integer x such that $g^x \equiv h \mod p$ computed as follows:
     1. Let $n = \lfloor \sqrt{p} \rfloor + 1$.
     2. Make two lists:

        $$\text{List 1: } 1, g, g^2, g^3, \ldots, g^n \pmod{p}$$
        $$\text{List 2: } h, hg^{-n}, hg^{-2n}, hg^{-3n}, \ldots, hg^{-n^2} \pmod{p}$$

     3. Find a match $g^i = hg^{-jn}$ between the two lists.
     4. Output $x = i + jn$.

   Suppose that you want to speed up this algorithm, so you modify it by choosing $n = \lfloor \sqrt[3]{p} \rfloor + 1$ instead of $n = \lfloor \sqrt{p} \rfloor + 1$ in Step 1 of the algorithm. Does the algorithm still work with this modification? Justify your answer.

SCRAP PAPER