CS 458 Homework 3
Due Date: 11 November 2024, 11:59 pm

Question 1: (5 points)

Part 1: By Hand

1. **Compute $7^{13} \mod 23$ using the square-and-multiply algorithm.**
   - Write down the binary representation of the exponent 13.
   - Follow the steps of the algorithm, showing each squaring and multiplication step.
   - Write your answer as $7^{13} \mod 23$.

Part 2: Programming

2. **Implement the square-and-multiply algorithm in a programming language of your choice (e.g., Python, Java, or C++) to compute $x^y \mod n$.**
   - Your function should take three inputs: base x, exponent y, and modulus n.
   - The function should output $x^y \mod n$.

   Sample Input and Output:
   - For inputs $x = 5$, $y = 20$, and $n = 35$, your function should output 25, as shown in the slide.
3. **Test Cases**
   - Use your program to compute the following:
     - $5^{13} \mod 23$
     - $12^{17} \mod 29$
     - $10^{25} \mod 37$

4. **Analysis**
    - Compare the output of your program with hand calculations (if possible) for one of the test cases.
    - Discuss why the square-and-multiply algorithm is more efficient than directly calculating x^y before taking the modulus.

Additional Instructions

- Show all intermediate steps in Part 1 to demonstrate your understanding of the square-and-multiply process.
- Include comments in your code explaining each part of the algorithm.

Example Solution Format

For Part 1:

- Write out the binary representation of the exponent.
- Show each step in the sequence, including each square and multiply operation.

For Part 2:

- Include your code, formatted and commented.

Question 2: (5 points)

Objective: Understand the steps of the Diffie-Hellman Key Exchange (DHKE) protocol and perform the calculations manually.

Given:

1. **Public Parameters**:
   - Prime number $p = 23$
   - Base $\alpha = 5$
2. **Private Keys**:
   - Alice's private key $a = 6$
   - Bob's private key $b = 15$

Tasks:

1. **Public Key Calculation**:
   - Calculate Alice's public key $A = \alpha^a \mod p$.
   - Calculate Bob's public key $B = \alpha^b \mod p$.
2. **Exchange Public Keys**:
   - Imagine that Alice and Bob exchange their public keys. Write down the values of A and B that each party receives.
3. **Common Secret Calculation**:
   - Calculate the common secret key K_{AB} that Alice and Bob will use for secure communication.
     - For Alice: $K_{AB} = B^a \mod p$.
     - For Bob: $K_{AB} = A^b \mod p$.

- Verify that both parties obtain the same shared secret key K_{AB}.

4. **Explanation**:
    - Explain why the common secret K_{AB} is the same for both Alice and Bob, even though they used different calculations.

Solution Format:

- Show all steps of the calculations clearly.
- Explain the concepts where needed to demonstrate your understanding of the DHKE protocol.