EE4215 Cybersecurity Technology

Assignment 4 Due: Feb 15 (Wed) at 11 am

1. Alice and Bob use the Diffie-Hellman key exchange protocol with the common prime $p = 157$ and generator $g = 5$.

   a) (2 points) Suppose Alice picks her private number as $a = 64$. Determine the public message she should send to Bob. Show your steps.

   b) (2 points) Suppose Bob picks his private number as $b = 94$. During the key exchange phase, he received the number calculated in (a). Determine the shared secret key, $k_{AB}$. Show your steps.

2. Consider the RSA cryptosystem. Bob has public key $(N = 37 \times 47,\ e = 25)$.

   a) (2 marks) Use extended Euclidean algorithm to determine Bob's private key, $d$.

   b) (2 marks) Alice wants to send the message $m = 314$ to Bob. She encrypts the message using Bob's public key. What is the value of the ciphertext that Alice sends to Bob?