Knapsack Homework Problems

1. Suppose that Bob’s knapsack public key is

   \[ T = [168, 280, 560, 393, 171, 230, 684, 418]. \]

   Suppose that Alice encrypts a message with Bob’s public key and the resulting ciphertext is \( C_1 = 1135 \). Implement the LLL attack and use your program to solve for the plaintext \( P_1 \). For the same public key, find the plaintext \( P_2 \) for the ciphertext \( C_2 = 2055 \). Can you determine the private key?

2. Suppose that Bob’s knapsack public key is

   \[ T = [2195, 4390, 1318, 2197, 7467, 5716, 3974, 3996, 7551, 668]. \]

   Suppose that Alice encrypts a message with Bob’s public key and the resulting ciphertext is \( C_1 = 8155 \). Implement the LLL attack and use your program to solve for the plaintext \( P_1 \). For the same public key, find the plaintext \( P_2 \) for the ciphertext \( C_2 = 14748 \). Can you determine the private key?