Problem Sheet 5

1. For each of the following sequences and volumes V, decide whether the knapsack problem is superincreasing and how many solutions (if any) it has.

   (a) $\{2, 3, 7, 20, 35, 69\}$, $V = 45$.
   (b) $\{1, 2, 5, 9, 20, 49\}$, $V = 73$.
   (c) $\{1, 3, 7, 12, 22, 45\}$, $V = 67$.
   (d) $\{2, 3, 6, 11, 21, 40\}$, $V = 39$.

2. Suppose in a Merkle-Hellman knapsack cryptosystem that plaintext message units are single letters in the usual alphabet A, ..., Z, with decimal numerical equivalents $0, 1, \ldots, 25$. A user receives the following sequence of ciphertext message units:

   $$14, 25, 89, 3, 65, 24, 3, 49, 89, 24, 41, 25, 68, 41, 71$$

   The user's public key is the sequence $57, 14, 3, 24, 8$, and the secret decryption key is $b = 23$, $m = 61$.

   (a) Decrypt the message using the decryption key and the algorithm for solving a superincreasing knapsack problem.
   (b) Use the public key to send the message TENFOUR.

3. Still working with a Merkle-Hellman cryptosystem, suppose plaintext message units are of length 3 in the alphabet

   $$A, B, \ldots, Z, \sqcup, ?, !, ., ', \$$$

   with decimal numerical equivalents $0, 1, \ldots, 31$. You receive the sequence of ciphertext message units $152472, 116116, 68546, 165420, 168261$. The public key is the sequence

   $$24038, 29756, 34172, 34286, 38334, 1824, 18255, 19723, 143, 17146, 35366, 11204, 32395, 12958, 6479$$

   and the secret key is $b = 30966$, $m = 47107$. Decrypt the message.

4. A knapsack cryptosystem with m = 41, a = 7, and decryption key

   $$v_1 = 1, v_2 = 3, v_3 = 5, v_4 = 10, v_5 = 21$$

   is used on single symbol message units in the 26-letter alphabet
   A = 0, ..., Z = 25.

   (a) Find the encyption key and use it to encrypt the message "ALGEBRA".
   (b) Determine the plaintext corresponding to the ciphertext

   $$28, 0, 53$$