Exercises

1. For each of the following sequences and "volumes," 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) $\{2,3,6,11,21,40\}$, $V = 39$; (e) $\{4,5,10,30,50,101\}$, $V = 186$; (f) $\{3,5,8,15,28,60\}$, $V = 43$;
2. (a) Show that the superincreasing sequence with the smallest v_i's is the one with $v_i = 2^i$.

   (b) Show that a superincreasing knapsack problem with $v_i = 2^i$ always has a solution n, namely $n = V$, and that for no other superincreasing sequence does the corresponding knapsack problem always have a solution.
3. Show that any sequence of positive integers $\{v_i\}$ with $v_{i+1} \geq 2v_i$ for all i is superincreasing.
4. Suppose that plaintext message units are single letters in the usual 26-letter alphabet with A—Z corresponding to 0—25. You receive the sequence of ciphertext message units 14, 25, 89, 3, 65, 24, 3, 49, 89, 24, 41, 25, 68, 41, 71. The public key is the sequence $\{57,14,3,24,8\}$ and the secret key is $b = 23$, $m = 61$.

   (a) Try to decipher the message without using the deciphering key; check by using the deciphering key and the algorithm for a superincreasing knapsack problem.

   (b) Use the above public key to send the message TENFOUR.
5. Suppose that plaintext message units are trigraphs in the 32-letter alphabet with A—Z corresponding to 0—25, blank=26, ?=27, !=28, .=29, '=30, $=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 $b = 30966$, $m = 47107$. Decipher the message.
6. Suppose that plaintext message units are digraphs in the 32-letter alphabet of Exercise 5. You receive the sequence of ciphertext message units 33219, 7067, 18127, 43099, 37953, which were enciphered using a two-iteration knapsack system with public key $\{23161, 6726, 4326, 16848, 21805, 11073, 120, 15708, 2608, 341\}$. The secret key is $b_1 = 533$, $m_1 = 2617$, $b_2 = 10175$, $m_2 = 27103$. Decipher the message.

References for § IV.4

1. E. Brickell, "Breaking iterated knapsacks," *Advances in Cryptology — Crypto '84*, Springer-Verlag, 1985, 342–358.
2. E. Brickell and A. Odlyzko, "Cryptanalysis: A survey of recent results," *Proc. IEEE* **76** (1988), 578–593.
3. B. Chor and R. Rivest, "A knapsack-type public key cryptosystem based on arithmetic in finite fields," *Advances in Cryptology — Crypto*