

Math 400 Fall 2018
Cryptology HW 9
Due Thursday, November 1

1. Solve the following knapsack problems:

- (a) $\mathbf{M} = (3, 7, 19, 43, 89, 195), S = 260$
- (b) $\mathbf{M} = (5, 11, 25, 61, 125, 261), S = 402$
- (c) $\mathbf{M} = (4, 12, 15, 36, 75, 162), S = 214$

2. Alice publishes the public key $\mathbf{M} = (18, 89, 90, 110, 185, 141)$

- (a) Suppose you wish to send the message $\mathbf{x} = (1, 1, 0, 1, 1, 0)$ (corresponding to 27 in binary). What ciphertext should you send?
- (b) Suppose you intercept someone else's message of $S = 430$. Express the problem of decrypting this message as a shortest-vector problem, as in section 9.5 of the notes.
- (c) Now decrypt the message corresponding to $S = 430$. You don't need to use lattice methods to do this.

3. Alice chooses the superincreasing sequence

$$\mathbf{r} = (2, 5, 13, 28, 60, 144)$$

with the numbers $A = 53$ and $B = 300$.

- (a) What public key does Alice publish?
- (b) Alice receives the ciphertext $S = 681$. What is the plaintext message?

4. Suppose Alice's public key for a knapsack cryptosystem is

$$\mathbf{M} = (5186, 2779, 5955, 2307, 6599, 6771, 6296, 7306, 4115, 7039).$$

Eve intercepts the encrypted message $S = 26560$. She also manages to steal from Alice the secret numbers $A = 4392$ and $B = 8387$. Use this information to find Alice's superincreasing sequence \mathbf{r} and then decrypt the message.

5. Which of the following matrices are invertible over \mathbb{Z} ? Find inverses for the ones that are.

(a) $\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$

(b) $\begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix}$

(c) $\begin{bmatrix} 3 & 2 & 2 \\ 2 & 1 & 2 \\ -1 & 3 & 1 \end{bmatrix}$

(d) $\begin{bmatrix} -3 & -1 & 2 \\ 1 & -3 & -1 \\ 3 & 0 & 2 \end{bmatrix}$

6. Let L be the lattice generated by the basis $B = \{(3, 1, -2), (1, -3, 5), (4, 2, 1)\}$. Which of the following sets of vectors are also bases for L ? For each one that is, find the change of basis matrix and write the new basis in terms of the basis B .

(a) $B_1 = \{(5, 13, -13), (0, -4, 2), (-7, -13, 18)\}$

(b) $B_2 = \{(4, -2, 3), (6, 6, -6), (-2, -4, 7)\}$.

7. A lattice L has dimension $n = 251$ and determinant $\det(L) \approx 2^{2251.58}$. How long do you expect the shortest vector to be?