Due Sept 8, 2025

MATH 173B: Cryptology II
Homework 4: Lattice-related Encryption

Instructions: Show all your work to receive full credit. Write your answers clearly and justify each step. Please Provide proof for your answer unless other wise specified.

1 Superincreasing Sequence(30pts)

(a) Let Y be any solution for the subset sum problem, where M is a superincreasing set and S is the target sum. Let X be the result of the following code, where n is the length of M.

```
for i in range(n - 1, -1, -1):
    if S >= M[i]:
        X[i] = 1
        S = S - M[i]
    else:
        X[i] = 0
```

Show that $X = Y$.

(b) What would be the vector X returned by the above algorithm in each of the following case? Does part (a) still hold?

i. Let $M = (2, 5, 12, 28, 60, 131, 257)$ and $S = 334$.

ii. Let $M = (4, 12, 15, 36, 75, 162)$ and $S = 214$.

iii. Let $M = \{1, 2, 3, 5, 8, 11, 19\}$ and $S = 19$.

(c) Let M be any sequence. Assume that the solution for the Subset-sum Problem exists. Does the output of the above algorithm always return a valid solution?

2 NTRU Cryptosystems (Congruetial Public Key Cryptosystems) (40pts)

Alice chooses a modulus q and two small secret integers f and g. Her public key is the integer $h = 767748560$ and $q = 91829387$.

(a) How do f, g, h, and q relate to each other? Write down their relationship in one single expression.

(b) If Bob has a secret message $m = 10220$ and a secret number $r = 19564$, what is the encrypted message?

(c) Bob uses the same r for different messages. Can Eve detect this immediately? Why or why not?

(d) Eve knows the public values of q and h, and she wants to recover the private key f. One approach for Eve is to search for small vectors in the lattice L generated by

$$v_1 = (1, h), \qquad v_2 = (0, q).$$

That is,

$$L = \{\, av_1 + bv_2 : a, b \in \mathbb{Z} \,\}.$$

Find the solution f and g using Gaussian reduction.

3 Lattice(30pts)

Let L be a lattice generated by the following basis

$$B = \{(3, 1, -2),\ (1, -3, 5),\ (4, 2, 1)\}.$$

Answer the following question:

(a) Compute the volume of this lattice L.

(b) Which of the following sets of vectors are also bases for L?

$$B_1 = \{(5, 13, -13),\ (0, -4, 2),\ (-7, -13, 18)\}$$
$$B_2 = \{(4, -2, 3),\ (6, 6, -6),\ (-2, -4, 7)\}$$

(c) For those set that are indeed a new basis, express the new basis in terms of the basis B, and find the change of basis matrix.

4 GGH Cryptosystem(50pts)

Let $L \subset \mathbb{R}^2$ be the lattice given by the basis

$$v_1 = (213, -437), \qquad v_2 = (312, 105),$$

and let

$$w = (43127, 11349).$$

(a) Use Babai's algorithm to find a vector $v \in L$ that is close to w. Compute the distance $\|v - w\|$.

(b) What is the value of the Hadamard ratio

$$\frac{\det(L)}{\|v_1\|\,\|v_2\|}\ ?$$

Is the basis $\{v_1, v_2\}$ a "good" basis?

(c) Show that the vectors

$$v_1' = (2937, -1555), \qquad v_2' = (11223, -5888)$$

are also a basis for L by expressing them as linear combinations of v_1 and v_2 and checking that the change-of-basis matrix has integer coefficients and determinant ± 1.

(d) Use Babai's algorithm with the basis $\{v_1', v_2'\}$ to find a vector $v' \in L$. Compute the distance $\|v' - w\|$ and compare it to your answer from part (a).

(e) Compute the Hadamard ratio using v_1' and v_2'. Is $\{v_1', v_2'\}$ a good basis?