Goldreich, Goldwasser, Halevi (GGH) Encryption, based on CVP

- Alice: Key creation
  - Pick good basis $\vec{v}_1, \ldots, \vec{v}_n$ and put in rows of matrix V
  - Choose matrix U with integer coefficients such that $\det(U) = \pm 1$
  - Compute bad basis as rows $\vec{w}_1, \ldots, \vec{w}_n$ of $W = UV$
  - Publish public key $\vec{w}_1, \ldots, \vec{w}_n$
- Bob: Encryption
  - Plaintext vector $\vec{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n$
  - $\vec{v} = \vec{m}W = m_1\vec{w}_1 + \cdots + m_n\vec{w}_n \in L$
  - Choose small random vector $\vec{r} \in \mathbb{R}^n$
  - Send ciphertext $\vec{e} = \vec{v} + \vec{r} \in \mathbb{R}^n$
- Alice: Decryption
  - Use good basis to recover $\vec{v} \in L$ *(see Babai's on next slide)*
  - $\vec{m} = \vec{v}W^{-1}$

Theorem 7.34 (Babai's Closest Vertex Algorithm)

Let $L \subset \mathbb{R}^n$ be a lattice of dimension n with basis $\mathcal{B} = \left\{\vec{v_1}, \ldots, \vec{v_n}\right\}$ and let $\vec{e} \in \mathbb{R}^n$ be an arbitrary vector.

If the basis vectors are sufficiently orthogonal, the following $\vec{v}$ solves the CVP:

- Write $\vec{e} = t_1\vec{v_1} + \cdots + t_n\vec{v_n}$ with $t_1, \ldots, t_n \in \mathbb{R}$ $\quad (\vec{t} = \vec{e}.V^{-1})$
- Set $a_i = \lfloor t_i \rceil$ for $1 \leq i \leq n$ (i.e. round t_i) $\quad (\vec{a} =$Round$(\vec{t})$)
- Then $\vec{v} = a_1\vec{v_1} + \cdots a_n\vec{v_n}$ $\quad (\vec{v} = \vec{a}.V)$

1. Use the values of V and W given in the Mathematica notebook for today. Let $L \subset \mathbb{R}^3$ be the lattice with basis in the rows of V.

(a) Verify that W is also a basis for L.

(b) Compute the Hadamard ratios of V and W.
Is V a good choice for a private key for GGH?
Is W a good choice for a public key for GGH?

(c) Encrypt $m = \{3, 7, 8\}$ using the ephemeral $r = \{-1, 1, 1\}$
What is the ciphertext?

(d) Verify your ciphertext by decrypting using V.
What plaintext do you get if you decrypt using the skewed basis W?

(e) You receive the ciphertext $e = \{-828256, -634219, 467126\}$. Use V to decrypt.

2. Use the values given in the Mathematica notebook for the public basis W, plaintext m, random vector r, and message e_1.

(a) Compute the Hadamard ratio of W to confirm that it is a good choice for a public key.

(b) Encrypt the plaintext m using r. What is the ciphertext?

(c) Suppose Eve intercepts the message e_1 and tries to decrypt using W. What will Eve get for the plaintext?

(d) Now use Mathematica's LatticeReduce[W] to apply the LLL algorithm to generate a more orthogonal basis V for the lattice.

  (i) Compute the Hadamard ratio of V.

  (ii) Use V to decrypt e_1. What is the plaintext recovered in this situation?