Homework 6

● Graded

Student

Kevin Vuong

View or edit group

Total Points

24.5 / 25 pts

Question 1

Question # 1

3.5 / 4 pts

– 0 pts Correct

✓ **– 0.5 pts** Hadamard Ratio incorrect

– 0.5 pts "Good" vs. "Bad" incorrect

– 1 pt Incorrect Work

Question 2

Question # 2

5 / 5 pts

✓ **– 0 pts** Correct

– 0.5 pts #2a incorrect

– 0.5 pts #2b incorrect

Question 3

Question # 3

8 / 8 pts

✓ **– 0 pts** Correct

– 0.5 pts #3a Hadamard Ratio incorrect

– 0.5 pts #3b incorrect

– 0.5 pts #3c incorrect

– 0.5 pts #3d decryption incorrect

– 4 pts Lack of work

Question 4

Question # 4

8 / 8 pts

✓ **– 0 pts** Correct

– 0.5 pts #2b partially incorrect

– 0.75 pts #2b incorrect

– 0.75 pts #2c incorrect

– 0.75 pts #2d incorrect

No questions assigned to the following page.

Homework 6

Instructions: Solutions must be typed using LaTeX. All work should be uploaded to Gradescope by 11:59PM on Friday, March 1, 2024. If you use Python, include a link to your Google Colab file in your PDF and be sure that your permissions are updated to allow anyone with the link to run your code.

1. (4 pts) Let $\mathbf{v}_1 = \begin{bmatrix} 10 \\ -9 \\ 4 \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} 17 \\ 11 \\ -3 \end{bmatrix}$, and $\mathbf{v}_3 = \begin{bmatrix} -6 \\ 13 \\ 5 \end{bmatrix}$.

   (a) Verify that $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is a basis for some lattice $\mathcal{L}$. Please Go to THIS Colab

   (b) Determine if this is a "good" basis or a "bad" one. Justify your response. Please Go to THIS Colab

2. (5 pts) Let $\mathcal{L}$ be the lattice generated by $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ and $\mathbf{v}_2 = \begin{bmatrix} 7 \\ -1 \end{bmatrix}$.

   (a) Verify that $\mathbf{v}_1$ and $\mathbf{v}_2$ are reasonably orthogonal. Please Go to THIS Colab

   (b) Find the closest vector in $\mathcal{L}$ to the target point $\mathbf{w} = \begin{bmatrix} 328 \\ 133 \end{bmatrix}$. Please Go to THIS Colab

3. (8 pts) Suppose Alice uses the GGH Cryptosystem with a private basis of $\mathcal{B} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 4 \\ 13 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} -57 \\ -45 \end{bmatrix} \right\}$ and public basis $\mathcal{B}' = \left\{ \mathbf{v}_1' = \begin{bmatrix} 25453 \\ 9091 \end{bmatrix}, \mathbf{v}_2' = \begin{bmatrix} -16096 \\ -5749 \end{bmatrix} \right\}$.

   (a) Compute the Hadamard Ratio of $\mathcal{B}$ and $\mathcal{B}'$. Interpret the meaning of each Hadamard Ratio. Please Go to THIS Colab

   (b) Bob sends Alice the encrypted message $\mathbf{c} = \begin{bmatrix} 155340 \\ 55483 \end{bmatrix}$. Use Alice's private basis to decrypt the message and recover the plaintext. Please Go to THIS Colab

   (c) Determine Bob's perturbation vector $\mathbf{r}$. Please Go to THIS Colab

   (d) Eve intercepts the encrypted message. Use the public basis to try to decrypt the message. Is the output equal to the plaintext message? Why or why not? Please Go to THIS Colab

4. (8 pts) Alice and Bob are using the GGH Cryptosystem to exchange messages. Alice chooses a good basis of $\mathcal{B} = \left\{ \mathbf{v}_1 = \begin{bmatrix} 234 \\ -673 \\ 254 \end{bmatrix}, \mathbf{v}_2 = \begin{bmatrix} -112 \\ 422 \\ 177 \end{bmatrix}, \mathbf{v}_3 = \begin{bmatrix} 43 \\ 633 \\ 79 \end{bmatrix} \right\}$.

   (a) Let $U = \begin{bmatrix} 2 & 3 & 5 \\ 3 & 2 & 3 \\ 9 & 5 & 7 \end{bmatrix}$. Verify that U is unimodular. Please Go to THIS Colab

   (b) Let $V = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \mathbf{v}_3 \end{bmatrix}$. Compute $V' = VU$ to get the public basis, $\mathcal{B}'$. Give your basis as a set of vectors, not a matrix. Please Go to THIS Colab

   (c) Bob wants to send Alice the plaintext message $P = (163, 97, 246)$. Encrypt this message using the noise vector $\mathbf{r} = \begin{bmatrix} -1 \\ 3 \\ 2 \end{bmatrix}$. Please Go to THIS Colab

   (d) Decrypt the ciphertext using Alice's private basis. Please Go to THIS Colab