MATH 132
HILL CIPHER (CRYPTOGRAPHY)

The Hill Cipher works as follows. We have an invertible matrix A of size 2×2 (or $3 \times 3, 4 \times 4$, etc.). This matrix serves as the secret encryption key. We assume our message has length $2n$ (or $3n, 4n$, etc.). If it doesn't have the right length, we can pad it with spaces at the end to obtain the right length. We convert our letters to numbers by space $= 0, a = 1, b = 2, \ldots, z = 26$, and put our message into a $2 \times n$ (or $3 \times n, 4 \times n$, etc.) matrix column by column. (Usually we discard spaces and work from 0 to 25, but not in this class.)

We then calculate $C = AM$. We read the numbers from C column by column and convert back to letters to get the encrypted ciphertext. (If the number is greater than 26, we can subtract 27 until the number lies in $[0, 26]$. If the number is less than 0, we can add 27 until the number lies in $[0, 26]$.)

To decrypt, we put our numbers into a matrix column by column. This matrix is the encrypted matrix C. We first calculate A^{-1} and then $A^{-1}C$. This will be equal to M since $A^{-1}C = A^{-1}(AM) = (A^{-1}A)M = IM = M$, where I is the identity matrix. We can then read the numbers out of M and convert back to letters.

In short, decryption is the same process as encryption, but with the matrix A^{-1} as the key instead of A.

Example: Let $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$. We will encrypt the message `midway`. This message has 6 letters, so we don't need to add any extra spaces at the end. Converting the letters to numbers, we have 13 9 4 23 1 25. Therefore,

$$M = \begin{pmatrix} 13 & 4 & 1 \\ 9 & 23 & 25 \end{pmatrix}.$$

You can calculate $AM = C = \begin{pmatrix} 31 & 50 & 51 \\ 40 & 73 & 76 \end{pmatrix}$. This means the encrypted message is 31 40 50 73 51 76. In order to convert this back to letters, we must "reduce" these numbers by subtracting multiples of 27 to get each number to lie in the interval $[0, 26]$. Doing so turns the numbers into 4 13 23 19 24 22. This corresponds to the ciphertext `DMWSXV`.

Now to decrypt, we just encrypt `DMWSXV` with the matrix A^{-1}. You can calculate $A^{-1} = \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix}$.

Converting `DMWSXV` to numbers gives 4 13 23 19 24 22, so $C = \begin{pmatrix} 4 & 23 & 24 \\ 13 & 19 & 22 \end{pmatrix}$. So we calculate $M = A^{-1}C = \begin{pmatrix} -14 & 31 & 28 \\ 9 & -4 & -2 \end{pmatrix}$. This means the decrypted message is -14 9 31 -4 28 -2. We must add (or subtract) 27 until each number lies in the interval $[0, 26]$. Doing so turns the numbers into 13 9 4 23 1 25, which corresponds to the plaintext message `midway`.