Hill Ciphers

Hill ciphers (invented in 1929) are a type of *block cipher*: the ciphertext character that replaces a particular plaintext character in the encryption will depend on the neighboring plaintext characters. The encryption is accomplished using matrix arithmetic.

The encryption key for a Hill cipher is a square matrix of integers. These integers are taken from the set $\{0, 1, \ldots, n-1\}$, where n is the size of the character set used for the plaintext message. (If this is the usual English alphabet, then $n = 26$.) It is important to note that not all such square matrices are valid keys for a Hill cipher. We'll discuss what is needed to create a valid key a bit later.

For now, suppose the key is the matrix $\kappa = \begin{bmatrix} 1 & 4 & 0 \\ 7 & 11 & 2 \\ 0 & 5 & 1 \end{bmatrix}$ and we want to encrypt the message "time to study" using a Hill cipher with this key. Using the conversion table:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

we represent our plaintext message as $19 \quad 8 \quad 12 \quad 4 \quad 19 \quad 14 \quad 18 \quad 19 \quad 20 \quad 3 \quad 24$. Now we take this sequence of numbers and break it up into rows of length 3 (the size of κ) to get

$$\begin{matrix} 19 & 8 & 12 \\ 4 & 19 & 14 \\ 18 & 19 & 20 \\ 3 & 24 & ? \end{matrix}$$

In order for the encryption to proceed, we must do something about the "?" that appears in the last row. It is customary to replace it with the integer representing a plaintext letter that will be easily identified as extraneous when the message is received. Here, we'll use 23, the representative of the letter "x." We form a matrix from the resulting four rows:

$$\mu = \begin{bmatrix} 19 & 8 & 12 \\ 4 & 19 & 14 \\ 18 & 19 & 20 \\ 3 & 24 & 23 \end{bmatrix}.$$

Now we compute $\gamma = \mu\kappa$ using ordinary matrix multiplication, except that whenever an entry x does not satisfy $0 \leq x \leq 25$, we replace x with the integer $y \in \{0, \ldots, 25\}$ such that $y \equiv x \pmod{26}$. In the current example, this results in

$$\gamma = \begin{bmatrix} 23 & 16 & 2 \\ 7 & 9 & 0 \\ 21 & 17 & 6 \\ 15 & 1 & 19 \end{bmatrix}.$$

Now concatenate the rows of γ to get the sequence $23 \quad 16 \quad 2 \quad 7 \quad 9 \quad 0 \quad 21 \quad 17 \quad 6 \quad 15 \quad 1 \quad 19$, and replace each integer with the letter it represents to obtain the ciphertext XQCHJAVRGPBT.

For practice, try encrypting the plaintext "finals are coming" using a Hill cipher with the encryption key κ above, and see if you can get the ciphertext JRDZDOPZMWOOVXG.

The following ciphertext was produced using a Hill cipher with the same encryption key κ we used above:

COAOVZOZWJBH.

How do we decrypt it?

First, replace each ciphertext letter with the integer that represents it to get the sequence

$$2 \quad 14 \quad 0 \quad 14 \quad 21 \quad 25 \quad 14 \quad 25 \quad 22 \quad 9 \quad 1 \quad 7,$$

which yields

$$\gamma = \begin{bmatrix} 2 & 14 & 0 \\ 14 & 21 & 25 \\ 14 & 25 & 22 \\ 9 & 1 & 7 \end{bmatrix}.$$

Now we must obtain μ from γ and κ. If the relationship $\gamma \equiv \mu\kappa \pmod{26}$ were an equation instead of a congruence and κ were an invertible matrix, we could solve:

$$\begin{aligned} \gamma &= \mu\kappa \\ \gamma\kappa^{-1} &= \mu. \end{aligned}$$

Since we have a congruence and *not* an equation, we have to take more care than this! There are two issues: do we have an inverse for κ, and, if so, what do we do if, (as is likely), κ^{-1} has non-integer entries?

In this case, (as you can verify), we do have an inverse for κ:

$$\kappa^{-1} = \frac{1}{27} \begin{bmatrix} -1 & 4 & -8 \\ 7 & -1 & 2 \\ -35 & 5 & 17 \end{bmatrix}.$$

However, this inverse doesn't have integer entries. To proceed with our decryption, we need to replace $\frac{1}{27}$ with an integer that has the same behavior, i.e., that produces an answer congruent to 1 modulo 26 when multiplied by 27. (See the discussion on affine ciphers for more about this.) Fortunately, since $27 \equiv 1 \pmod{26}$, we may replace $\frac{1}{27}$ with 1 to obtain:

$$\begin{aligned} \mu &\equiv \gamma \begin{bmatrix} -1 & 4 & -8 \\ 7 & -1 & 2 \\ -35 & 5 & 17 \end{bmatrix} \pmod{26} \\ &\equiv \begin{bmatrix} 18 & 20 & 12 \\ 12 & 4 & 17 \\ 15 & 11 & 0 \\ 13 & 18 & 23 \end{bmatrix} \pmod{26}. \end{aligned}$$

From here, we recover the plaintext "summerplansx," from which we deduce that the message was "summer plans."

At this point, we can specify what is required of a square matrix of integers κ in order for it to be a valid key for a Hill cipher. For the decryption process to succeed, we need κ to be invertible modulo 26, which amounts to requiring that the determinant of κ satisfy $\gcd(\det \kappa, 26) = 1$. (We're using a fact from linear algebra about the relationship between determinants and inverses; if this seems mysterious, check out the classical adjoint of a matrix in your favorite linear algebra text.)

Here's a little more practice. The following ciphertext was produced by a Hill cipher with key $\kappa = \begin{bmatrix} 2 & 7 \\ 5 & 22 \end{bmatrix}$: EMRISXCAEGOHJEVI. See if you can recover the plaintext. (Note that with a 2×2 key, your matrices μ and γ must have 2 columns!)

While Hill ciphers provide a significant improvement in security over Vigenère ciphers, they are very easily attacked if a few correct characters of plaintext are already matched to a ciphertext message, a so-called *known plaintext attack*. For this reason, Hill ciphers are not considered sufficiently secure for sensitive applications.