Cryptography

Briefly, cryptography is the study and practice of secure communication. And in the information age, it has become vitally important. Unfortunately a full discussion of its applicability is beyond the scope of the course. We'll instead be focusing on classical cryptography (encoding and decoding messages) using a simple version of the Hill Cipher invented in 1929 by Lester Hill.

Before we begin, we need a little background in modular arithmetic (or clock arithmetic).

Definition: Let m be a positive integer (called the *modulus*), and let a and b be any integers. Then we say that a is *equivalent* to b modulo m, denoted

$$a = b \pmod{m}$$

if and only if their difference $a - b$ is a multiple of m.

In other words, a and b are equivalent modulo m exactly when a and b have the same remainder after division by the modulus m. Consequently, for any modulus m, every integer is equivalent modulo m to exactly one of $0, 1, 2, \ldots, m-1$. We call this number the *residue* of a modulo m.

Definition: Given an integer a, then a number a^{-1} is called the *multiplicative inverse* of a modulo m if and only if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

Note that a has a multiplicative inverse modulo m if and only if a and m are relatively prime (i.e. they have no common factors other than 1). As with ordinary arithmetic, we would like to extend this definition to matrices. First, we say two integer matrices are equivalent modulo m if and only if all their corresponding entries are equivalent. Then we can make the following definition.

Definition: Given an integer matrix A, then an integer matrix A^{-1} is called the *multiplicative inverse* of A modulo m if and only if $AA^{-1} = A^{-1}A = I \pmod{m}$.

Note that A is invertible precisely when its determinant is invertible modulo m. And for 2×2 matrices, we can easily compute the inverse of A.

$$\text{If } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ then } A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad \text{when } ad - bc \text{ is invertible modulo } m.$$

For our purposes, we'll be working modulo 26, and we'll use the substitution table below to transform any message into a sequence of residues modulo 26 (ignoring spacing and punctuation).

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

And here's the list of inverses modulo 26 for all invertible residues.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

The idea behind a Hill-2 cipher is simple. The original message (called the plaintext) is converted into numbers using the substitution table above, and broken down into pairs as column vectors with 2 components. For instance the message HELP ME is first transformed into the sequence of numbers 8 5 12 16 13 5 and then into $\vec{p_1} = \begin{bmatrix}8\\5\end{bmatrix}$, $\vec{p_2} = \begin{bmatrix}12\\16\end{bmatrix}$ and $\vec{p_3} = \begin{bmatrix}13\\5\end{bmatrix}$.

To encrypt (or encipher) a message, we need an encryption matrix A that is invertible modulo 26. We obtain our ciphertext (encoded message) by multiplying A by the column vectors, converting the numbers back into letters and writing out the sequence with spacing removed.

Let $A = \begin{bmatrix}1 & 3\\2 & 5\end{bmatrix}$ be our encryption matrix. Then

$$A\vec{p_1} = \begin{bmatrix}1 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}8\\5\end{bmatrix} = \begin{bmatrix}23\\15\end{bmatrix},\ A\vec{p_2} = \begin{bmatrix}1 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}12\\16\end{bmatrix} = \begin{bmatrix}8\\0\end{bmatrix} \text{ and } A\vec{p_3} = \begin{bmatrix}1 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}13\\5\end{bmatrix} = \begin{bmatrix}2\\25\end{bmatrix} \pmod{26}$$

corresponding to the pairs of letters WO HZ BY. Removing spacing, the ciphertext is WOHZBY

Remarks: Note that one can encipher using an $n \times n$ matrix as well (Hill-n cipher) and grouping the plaintext into groups of size n. Also, if we wanted to do, we could use a bigger modulus so that we could assign residues to spaces or punctuation.

To decrypt (or decipher) a ciphertext, we will use the fact that $A^{-1}A = I$, which means that $A^{-1}A\vec{p} = \vec{p}$ for all vectors p. In other words, to decrypt, we convert the ciphertext into 2×1 vectors and multiply them on the left by A^{-1} to obtain the original plaintext.

Given $A = \begin{bmatrix}1 & 3\\2 & 5\end{bmatrix}$ as above, with $\det(A) = -1 = 25 \pmod{26}$, then we have

$$A^{-1} = 25^{-1}\begin{bmatrix}5 & -3\\-2 & 1\end{bmatrix} = \begin{bmatrix}21 & 3\\2 & 25\end{bmatrix} \text{ or equivalently } \begin{bmatrix}-5 & 3\\2 & -1\end{bmatrix} \pmod{26}$$

Remarks: Since many numbers are equivalent modulo 26, there are lots of possible representations for this matrix. Above I've given the two representations that allow for the easiest computations.

So the ciphertext WOHZBY is converted back into the vectors $\begin{bmatrix}23\\15\end{bmatrix}$, $\begin{bmatrix}8\\0\end{bmatrix}$ and $\begin{bmatrix}2\\25\end{bmatrix}$.

Multiplying each vector on the left by A^{-1}, we get

$$\begin{bmatrix}21 & 3\\2 & 25\end{bmatrix}\begin{bmatrix}23\\15\end{bmatrix} = \begin{bmatrix}8\\5\end{bmatrix},\ \begin{bmatrix}21 & 3\\2 & 25\end{bmatrix}\begin{bmatrix}8\\0\end{bmatrix} = \begin{bmatrix}12\\16\end{bmatrix} \text{ and } \begin{bmatrix}21 & 3\\2 & 25\end{bmatrix} = \begin{bmatrix}2\\25\end{bmatrix} = \begin{bmatrix}13\\5\end{bmatrix} \pmod{26}$$

Converting this back to letters gives us HELPME, which is our original plaintext (without spacing).

Though the Hill cipher is generally more resilient to some cryptographic attacks than most older systems (most notably frequency analysis), it is far from perfect for a number of reasons. Just for fun, we'll show you one particular weakness: how to use the knowledge of a suitably long plaintext message and its encrypted ciphertext to completely crack the system (called a known-plaintext attack).

Suppose a Hill-2 cipher encrypts a message into ciphertext IVAZKGYUOPYHBK. Now suppose further that we know the original message starts with the word ACES. Then I have enough information to not only decode the whole message but decode any message sent using that encryption. Let's examine how.

Translating everything into residues modulo 26, and the encryption matrix being used is called E, then we know that multiplying E by the pair of vectors corresponding to AC and ES, we get the vectors corresponding to IV and AZ. More precisely,

$$E\begin{bmatrix}1 & 5\\ 3 & 19\end{bmatrix} = \begin{bmatrix}9 & 1\\ 22 & 0\end{bmatrix} \text{ or equivalently, } E^{-1}\begin{bmatrix}9 & 1\\ 22 & 0\end{bmatrix} = \begin{bmatrix}1 & 5\\ 3 & 19\end{bmatrix}$$

We'll focus on solving E^{-1} directly since this will allow us to immediately decode any encrypted message that comes our way by multiplying it on the left by E^{-1}. We could also solve for E and then take its inverse, but this time, I'll just take the quickest path to being able to decrypt the message that we intercepted.

So assuming $E^{-1} = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$, then we get $\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}9 & 1\\ 22 & 0\end{bmatrix} = \begin{bmatrix}1 & 5\\ 3 & 19\end{bmatrix}$

Performing the matrix multiplication gives us: $\begin{bmatrix}9a+22b & a\\ 9c+22d & c\end{bmatrix} = \begin{bmatrix}1 & 5\\ 3 & 19\end{bmatrix}$

We can see this as two systems of equations to get values for a, b, c and d as follows:

$$\text{Row 1: } \begin{cases} 9a+22b &= 1 \pmod{26} \\ a &= 5 \pmod{26} \end{cases} \qquad \text{and Row 2: } \begin{cases} 9c+22d &= 3 \pmod{26} \\ c &= 19 \pmod{26} \end{cases}$$

In this case, we already have values for a and c, so we can substitute them in to solve for b and d.

So $9(5)+22b = 1 \pmod{26} \implies 22b = 1-45 \pmod{26} \implies 22b = 8 \pmod{26}$

Interestingly, there is no unique solution for b (we can't simply isolate the variable b since 22 is not invertible modulo 26). But with a bit of work, we can determine $b = 11$ **or** $24 \pmod{26}$.

Similarly, we can see by inspection that c equals 19, and determine that $d = 3$ **or** $13 \pmod{26}$. So we get four possible decryption matrices

$$D_1 = \begin{bmatrix}5 & 11\\ 19 & 3\end{bmatrix} \quad D_2 = \begin{bmatrix}5 & 24\\ 19 & 3\end{bmatrix} \quad D_3 = \begin{bmatrix}5 & 11\\ 19 & 16\end{bmatrix} \quad D_4 = \begin{bmatrix}5 & 24\\ 19 & 16\end{bmatrix}$$

$\text{Det}(D_1) = 5(3) - 11(19) = 14 \pmod{26}$

$\text{Det}(D_2) = 5(3) - 24(19) = 1 \pmod{26}$

$\text{Det}(D_3) = 5(16) - 11(19) = 1 \pmod{26}$

$\text{Det}(D_4) = 5(16) - 24(19) = 14 \pmod{26}$

Only D_2 and D_3 are invertible since their determinants are invertible. So one of those must be our decryption matrix. We still however don't know, so we'll try them both on our ciphertext. We transform our ciphertext IVAZKGYUOPYHBK into a matrix of numbers and multiply it on the left by D_2 and D_3 to see what we get in each case.

$$\text{IV AZ KG YU OP YH BK} \Longrightarrow C = \begin{bmatrix} 9 & 1 & 11 & 25 & 15 & 25 & 2 \\ 22 & 0 & 7 & 21 & 16 & 8 & 11 \end{bmatrix}$$

$$D_2C = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix} \begin{bmatrix} 9 & 1 & 11 & 25 & 15 & 25 & 2 \\ 22 & 0 & 7 & 21 & 16 & 8 & 11 \end{bmatrix} = \begin{bmatrix} 1 & 5 & 15 & 5 & 17 & 5 & 14 \\ 3 & 19 & 22 & 18 & 21 & 5 & 19 \end{bmatrix}$$

$\Longrightarrow$ ACESOVERQUEENS

$$D_3C = \begin{bmatrix} 5 & 11 \\ 19 & 16 \end{bmatrix} \begin{bmatrix} 9 & 1 & 11 & 25 & 15 & 25 & 2 \\ 22 & 0 & 7 & 21 & 16 & 8 & 11 \end{bmatrix} = \begin{bmatrix} 1 & 5 & 2 & 18 & 17 & 5 & 1 \\ 3 & 19 & 9 & 5 & 21 & 5 & 6 \end{bmatrix}$$

$\Longrightarrow$ACESBIREQUEEAF

Only the first message makes sense so $D_2 = E^{-1}$ is the correct decryption matrix and the original message sent was "Aces Over Queens". Moreover we can also now decrypt any further messages sent using the same encryption matrix by simply multiplying the ciphertext by D_2.

Once we have E^{-1} we can easily find E by taking its inverse as $(E^{-1})^{-1} = E$.

$$\text{Thus } E = (5(3) - 24(19))^{-1} \begin{bmatrix} 3 & -24 \\ -19 & 5 \end{bmatrix} = (1)^{-1} \begin{bmatrix} 3 & -24 \\ -19 & 5 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \pmod{26}$$

So we can now send encoded messages of using the same Hill-2 cipher. Now if it only took us the knowledge of four characters of plaintext and their ciphertext in order to crack the cryptosystem, it is not that secure. In fact, to crack a Hill cipher with encryption matrix $n \times n$ will require the knowledge of just n^2 characters in a plaintext message with corresponding ciphertext.

Fortunately, we've come a long way since then. Though that is not to say the Hill cipher has no value. Matrix multiplication itself may not be secure, but if used in combination with other non-linear operations, it can help to increase security by providing diffusion.