7.5: Application of Matrices in Cryptography

Learning Objectives

In this section, we will learn to find the inverse of a matrix, if it exists. Later, we will use matrix inverses to solve linear systems. In this section you will learn to

1. encode a message using matrix multiplication.
2. decode a coded message using the matrix inverse and matrix multiplication

Encryption dates back approximately 4000 years. Historical accounts indicate that the Chinese, Egyptians, Indian, and Greek encrypted messages in some way for various purposes. One famous encryption scheme is called the Caesar cipher, also called a substitution cipher, used by Julius Caesar, involved shifting letters in the alphabet, such as replacing A by C, B by D, C by E, etc, to encode a message. Substitution ciphers are too simple in design to be considered secure today.

In the middle ages, European nations began to use encryption. A variety of encryption methods were used in the US from the Revolutionary War, through the Civil War, and on into to modern times.

Applications of mathematical theory and methods to encryption became widespread in military usage in the 20^{th} century. The military would encode messages before sending and the recipient would decode the message, in order to send information about military operations in a manner that kept the information safe if the message was intercepted. In World War II, encryption played an important role, as both Allied and Axis powers sent encrypted messages and devoted significant resources to strengthening their own encryption while also trying to break the opposition's encryption.

In this section we will examine a method of encryption that uses matrix multiplication and matrix inverses. This method, known as the Hill Algorithm, was created by Lester Hill, a mathematics professor who taught at several US colleges and also was involved with military encryption. The Hill algorithm marks the introduction of modern mathematical theory and methods to the field of cryptography.

These days, the Hill Algorithm is not considered a secure encryption method; it is relatively easy to break with modern technology. However, in 1929 when it was developed, modern computing technology did not exist. This method, which we can handle easily with today's technology, was too cumbersome to use with hand calculations. Hill devised a mechanical encryption machine to help with the mathematics; his machine relied on gears and levers, but never gained widespread use. Hill's method was considered sophisticated and powerful in its time and is one of many methods influencing techniques in use today. Other encryption methods at that time also utilized special coding machines. Alan Turing, a computer scientist pioneer in the field of artificial intelligence, invented a machine that was able to decrypt messages encrypted by the German Enigma machine, helping to turn the tide of World War II.

With the advent of the computer age and internet communication, the use of encryption has become widespread in communication and in keeping private data secure; it is no longer limited to military uses. Modern encryption methods are more complicated, often combining several steps or methods to encrypt data to keep it more secure and harder to break. Some modern methods make use of matrices as part of the encryption and decryption process; other fields of mathematics such as number theory play a large role in modern cryptography.

To use matrices in encoding and decoding secret messages, our procedure is as follows.

We first convert the secret message into a string of numbers by arbitrarily assigning a number to each letter of the message. Next we convert this string of numbers into a new set of numbers by multiplying the string by a square matrix of our choice that has an inverse. This new set of numbers represents the coded message.

To decode the message, we take the string of coded numbers and multiply it by the inverse of the matrix to get the original string of numbers. Finally, by associating the numbers with their corresponding letters, we obtain the original message.

In this section, we will use the correspondence shown below where letters A to Z correspond to the numbers 1 to 26, a space is represented by the number 27, and punctuation is ignored.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 7.5.1

Use matrix $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ to encode the message: ATTACK NOW!

Solution

We divide the letters of the message into groups of two.

$$\text{AT} \quad \text{TA} \quad \text{CK} \quad \text{-N} \quad \text{OW}$$

We assign the numbers to these letters from the above table, and convert each pair of numbers into 2×1 matrices. In the case where a single letter is left over on the end, a space is added to make it into a pair.

$$\begin{bmatrix} \text{A} \\ \text{T} \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \quad \begin{bmatrix} \text{T} \\ \text{A} \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix} \quad \begin{bmatrix} \text{C} \\ \text{K} \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} - \\ \text{N} \end{bmatrix} = \begin{bmatrix} 27 \\ 14 \end{bmatrix} \quad \begin{bmatrix} \text{O} \\ \text{W} \end{bmatrix} = \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

So at this stage, our message expressed as 2×1 matrices is as follows.

$$\begin{bmatrix} 1 \\ 20 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} \quad \textbf{(I)}$$

Now to encode, we multiply, on the left, each matrix of our message by the matrix A. For example, the product of A with our first matrix is: $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 41 \\ 61 \end{bmatrix}$

And the product of A with our second matrix is: $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 23 \end{bmatrix}$

Multiplying each matrix in $\textbf{(I)}$ by matrix A, in turn, gives the desired coded message:

$$\begin{bmatrix} 41 \\ 61 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \end{bmatrix} \begin{bmatrix} 25 \\ 36 \end{bmatrix} \begin{bmatrix} 55 \\ 69 \end{bmatrix} \begin{bmatrix} 61 \\ 84 \end{bmatrix}$$

Example 7.5.2

Decode the following message that was encoded using matrix $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$.

$$\begin{bmatrix} 21 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 53 \end{bmatrix} \begin{bmatrix} 45 \\ 54 \end{bmatrix} \begin{bmatrix} 74 \\ 101 \end{bmatrix} \begin{bmatrix} 53 \\ 69 \end{bmatrix} \quad \textbf{(II)}$$

Solution

Since this message was encoded by multiplying by the matrix A in Example 7.5.1, we decode this message by first multiplying each matrix, on the left, by the inverse of matrix A given below.

$$A^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$$

For example: $\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 26 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix}$

By multiplying each of the matrices in $\textbf{(II)}$ by the matrix A^{-1}, we get the following.

$$\begin{bmatrix}11\\5\end{bmatrix}\begin{bmatrix}5\\16\end{bmatrix}\begin{bmatrix}27\\9\end{bmatrix}\begin{bmatrix}20\\27\end{bmatrix}\begin{bmatrix}21\\16\end{bmatrix}$$

Finally, by associating the numbers with their corresponding letters, we obtain:

$$\begin{bmatrix}\mathrm{K}\\\mathrm{E}\end{bmatrix}\begin{bmatrix}\mathrm{E}\\\mathrm{P}\end{bmatrix}\begin{bmatrix}-\\\mathrm{I}\end{bmatrix}\begin{bmatrix}\mathrm{T}\\-\end{bmatrix}\begin{bmatrix}\mathrm{U}\\\mathrm{P}\end{bmatrix}$$

And the message reads: KEEP IT UP.

Now suppose we wanted to use a 3×3 matrix to encode a message, then instead of dividing the letters into groups of two, we would divide them into groups of three.

Example 7.5.3

Using the matrix $B=\begin{bmatrix}1&1&-1\\1&0&1\\2&1&1\end{bmatrix}$, encode the message: ATTACK NOW!

Solution

We divide the letters of the message into groups of three.

ATT ACK -NO W- -

Note that since the single letter "W" was left over on the end, we added two spaces to make it into a triplet.

Now we assign the numbers their corresponding letters from the table, and convert each triplet of numbers into 3×1 matrices. We get

$$\begin{bmatrix}\mathrm{A}\\\mathrm{T}\\\mathrm{T}\end{bmatrix}=\begin{bmatrix}1\\20\\20\end{bmatrix}\begin{bmatrix}\mathrm{A}\\\mathrm{C}\\\mathrm{K}\end{bmatrix}=\begin{bmatrix}1\\3\\11\end{bmatrix}\begin{bmatrix}-\\\mathrm{N}\\\mathrm{O}\end{bmatrix}=\begin{bmatrix}27\\14\\15\end{bmatrix}\begin{bmatrix}\mathrm{W}\\-\\-\end{bmatrix}=\begin{bmatrix}23\\27\\27\end{bmatrix}$$

So far we have,

$$\begin{bmatrix}1\\20\\20\end{bmatrix}\begin{bmatrix}1\\3\\11\end{bmatrix}\begin{bmatrix}27\\14\\15\end{bmatrix}\begin{bmatrix}23\\27\\27\end{bmatrix}\quad\textbf{(III)}$$

We multiply, on the left, each matrix of our message by the matrix B. For example,

$$\begin{bmatrix}1&1&-1\\1&0&1\\2&1&1\end{bmatrix}\begin{bmatrix}1\\20\\20\end{bmatrix}=\begin{bmatrix}1\\21\\42\end{bmatrix}$$

By multiplying each of the matrices in $\textbf{(III)}$ by the matrix B, we get the desired coded message as follows:

$$\begin{bmatrix}1\\21\\42\end{bmatrix}\begin{bmatrix}-7\\12\\16\end{bmatrix}\begin{bmatrix}26\\42\\83\end{bmatrix}\begin{bmatrix}23\\50\\100\end{bmatrix}$$

If we need to decode this message, we simply multiply the coded message by B^{-1}, and associate the numbers with the corresponding letters of the alphabet.

In Example 7.5.4 we will demonstrate how to use matrix B^{-1} to decode an encrypted message.

Example 7.5.4

Decode the following message that was encoded using matrix $B = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$.

$$\begin{bmatrix} 11 \\ 20 \\ 43 \end{bmatrix} \begin{bmatrix} 25 \\ 10 \\ 41 \end{bmatrix} \begin{bmatrix} 22 \\ 14 \\ 41 \end{bmatrix} \quad \textbf{(IV)}$$

Solution

Since this message was encoded by multiplying by the matrix B. We first determine inverse of B.

$$\mathrm{B}^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix}$$

To decode the message, we multiply each matrix, on the left, by B^{-1}. For example,

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & -3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 11 \\ 20 \\ 43 \end{bmatrix} = \begin{bmatrix} 8 \\ 15 \\ 12 \end{bmatrix}$$

Multiplying each of the matrices in $\textbf{(IV)}$ by the matrix B^{-1} gives the following.

$$\begin{bmatrix} 8 \\ 15 \\ 12 \end{bmatrix} \begin{bmatrix} 4 \\ 27 \\ 6 \end{bmatrix} \begin{bmatrix} 9 \\ 18 \\ 5 \end{bmatrix}$$

Finally, by associating the numbers with their corresponding letters, we obtain

$$\begin{bmatrix} \mathrm{H} \\ \mathrm{O} \\ \mathrm{L} \end{bmatrix} \begin{bmatrix} \mathrm{D} \\ - \\ \mathrm{F} \end{bmatrix} \begin{bmatrix} \mathrm{I} \\ \mathrm{R} \\ \mathrm{E} \end{bmatrix} \quad \text{The message reads: HOLD FIRE}$$

The message reads: HOLD FIRE.

We summarize:

TO ENCODE A MESSAGE

1. Divide the letters of the message into groups of two or three.

2. Convert each group into a string of numbers by assigning a number to each letter of the message. Remember to assign letters to blank spaces.

3. Convert each group of numbers into column matrices.

3. Convert these column matrices into a new set of column matrices by multiplying them with a compatible square matrix of your choice that has an inverse. This new set of numbers or matrices represents the coded message.

TO DECODE A MESSAGE

1. Take the string of coded numbers and multiply it by the inverse of the matrix that was used to encode the message.

2. Associate the numbers with their corresponding letters.