Definition 1.8.1 (Application of Matrices in Cryptography)

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.

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

Problem 1.8.2

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

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

$$AT \quad TA \quad CK \quad -N \quad OW$$

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.

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

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

$$\begin{bmatrix} 1 \\ 20 \end{bmatrix}; \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} \qquad (5)$$

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 (5) by matrix A, in turn, gives the desired coded message:

$$\begin{bmatrix} 41 \\ 66 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \end{bmatrix} \begin{bmatrix} 25 \\ 36 \end{bmatrix} \begin{bmatrix} 55 \\ 69 \end{bmatrix} \begin{bmatrix} 61 \\ 84 \end{bmatrix}$$

Problem 1.8.3

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

$$\begin{bmatrix} 21 \\ 26 \end{bmatrix} \begin{bmatrix} 37 \\ 53 \end{bmatrix} \begin{bmatrix} 45 \\ 54 \end{bmatrix} \begin{bmatrix} 74 \\ 101 \end{bmatrix} \begin{bmatrix} 53 \\ 69 \end{bmatrix} \tag{6}$$

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 (6) 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:

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

And the message reads: **KEEP IT UP**.

Problem 1.8.4

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

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

$$ATT \quad ACK \quad -NO \quad W--$$

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

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

So far we have,

$$\begin{bmatrix}1\\20\\20\end{bmatrix}\begin{bmatrix}1\\3\\11\end{bmatrix}\begin{bmatrix}27\\14\\15\end{bmatrix}\begin{bmatrix}23\\27\\27\end{bmatrix} \tag{7}$$

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 (7) by the matrix B, we get the desired coded message as follows:

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

Problem 1.8.5

Decode the following message

$$\begin{bmatrix} 11 \\ 20 \\ 43 \end{bmatrix} \begin{bmatrix} 25 \\ 10 \\ 41 \end{bmatrix} \begin{bmatrix} 22 \\ 14 \\ 41 \end{bmatrix} \tag{8}$$

that was encoded using matrix

$$B = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}.$$

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

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

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 (8) 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

$$\begin{bmatrix} H \\ O \\ L \end{bmatrix} \quad \begin{bmatrix} D \\ - \\ F \end{bmatrix} \quad \begin{bmatrix} I \\ R \\ E \end{bmatrix}$$

The message reads: **HOLD FIRE**.