ACSL

2010 - 2011 **American Computer Science League** **Contest #4**

Senior Division

Matrix Encryption

PROBLEM: One method of code encryption uses matrix multiplication. The letters of the alphabet are assigned the numbers 1 – 26 in order and a space is given a value of 27. Although at first glance this might seem a simple code to break, the beauty of the system is that once matrix multiplication is performed, it is very difficult to determine the encoding matrix. The encoding matrix is usually only known by the sender and the reciever. For this program a 2x2 encoding matrix will be used. The method to use is as follows:

1. Convert the message into a series of 2x1 matrices: Given the code MATH ROCKS. The matrices formed will be as follows: $\begin{vmatrix}13\\1\end{vmatrix}\begin{vmatrix}20\\8\end{vmatrix}\begin{vmatrix}27\\18\end{vmatrix}\begin{vmatrix}15\\3\end{vmatrix}\begin{vmatrix}11\\19\end{vmatrix}$. If the code has an odd number of characters, the last character is assumed to be a space (27).

2. Mutiply each matrix by the encoding matrix. For this example the encoding matrix is 0111 and is read in across the rows as follows: $\begin{vmatrix}0 & 1\\1 & 1\end{vmatrix}$

$\begin{vmatrix}0 & 1\\1 & 1\end{vmatrix} * \begin{vmatrix}13\\1\end{vmatrix} = \begin{vmatrix}0*13+1*1\\1*13+1*1\end{vmatrix} = \begin{vmatrix}1\\14\end{vmatrix}$. This procedure is repeated for each 2x1 matrix. To produce:

$$\begin{vmatrix}1\\14\end{vmatrix}\begin{vmatrix}8\\28\end{vmatrix}\begin{vmatrix}18\\45\end{vmatrix}\begin{vmatrix}3\\18\end{vmatrix}\begin{vmatrix}19\\30\end{vmatrix}$$

This converts to ANHARRCRSC.

3. The above string is sent as the message. To decode the message you need to find the inverse matrix of the encoding matrix using the following rule:

$$M = \begin{vmatrix}a & b\\c & d\end{vmatrix} \text{ then } M^{-1}\text{, the inverse, is } \frac{1}{ad-bc} * \begin{vmatrix}d & -b\\-c & a\end{vmatrix}.$$

4. Multiply each 2x1 matrix from Step 2 by the inverse matrix: $\begin{vmatrix}-1 & 1\\1 & 0\end{vmatrix} * \begin{vmatrix}1\\14\end{vmatrix} = \begin{vmatrix}13\\1\end{vmatrix}$. This is the same as the first matrix formed in step one and translates back to MA. This procedure is repeated for each

encoded matrix. Note that in the second set of matricies $\begin{vmatrix} 8 \\ 28 \end{vmatrix}$ The 28 would be converted to a 1 by the receiver and would produce the TH of the original message.

INPUT: There will be 5 lines of input. Each line will contain a one character string (E or D) telling to encode or decode a string. This will be followed by the string to be encoded or decoded. This will be followed by 4 integers that form the encoding matrix. The integers are to be read in across the rows.

OUTPUT: For each input line, print the encoded or decoded message. If the matrix contains a value greater than 27, then use the MOD 27 of that value.

SAMPLE INPUT	SAMPLE OUTPUT
1. E, MATH ROCKS, 0, 1, 1, 1	1. ANHARRCRSC
2. D, ANHARRCRSC, 0, 1, 1, 1	2. MATH ROCKS