Matrices: A Secret Weapon

Algebra 5/Trig

May 4, 2010

In this worksheet we will learn how to use matrix multiplication in cryptography. Our key matrix will be the matrix:

$$A = \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & 4 \end{bmatrix}.$$

Enter this matrix into your calculator. We will also need to know that A is invertible, or the method will not work. To do so, use your calculator to compute the determinant of A.

1 Uncoded Row Matrices

To begin encoding a message, we must form uncoded row matrices. Since we are using a 3 by 3 matrix, we will form uncoded 1 by 3 row matrices.

To do this, we assign each letter of the alphabet a number. The most simple way of doing so is to assign each letter the number of its position in the alphabet, with the number zero standing for a blank space. This is displayed at the top of page 784. This can be made more complicated for an additional level of security, but we will not do so here.

Read Example 6 on page 784 to see how to form uncoded row matrices.

Use the method of Example 6 to write uncoded row matrices for the following messages:

1. THIS MAN CANNOT BE TRUSTED

2. SHOOT AT ONCE

3. MEET ME AT THE KREMLIN

4. THIS PHONE IS NOT SECURE

2 Encoding a Message

We will now use the matrix A to encode a message. To do this, we multiply the uncoded row matrix on the right by the matrix A. Read Example 7 on page 785 to see how this is done.

Using the uncoded row matrices you computed above along with the matrix A, encode the following messages:

1. THIS MAN CANNOT BE TRUSTED

2. SHOOT AT ONCE

3. MEET ME AT THE KREMLIN

4. THIS PHONE IS NOT SECURE

3 Decoding Messages

If we do not know the key A, we cannot decode messages. Thankfully, we know the key! To decode a message, first multiply the row matrices on the right by A^{-1}. Then translate the resulting row matrices into letters. Read Example 8 on page 786 to see how this is done.

Decode the following messages:

1. 31 -56 179 17 -17 75 7 -12 18 10 -15 93 30 -37 106 -16 15 74 7 -15 47

2. -6 5 128 5 -14 30 21 -41 100 35 -54 102 6 -11 140 1 -16 72

3. 32 -45 109 17 -25 52 25 -44 62 17 -28 84

4. 32 -45 109 12 -30 75 -14 9 67 1 -20 113 11 -22 22