4.5 The Inverse of a Square Matrix

Thursday, October 5, 2017 8:48 AM

Goals (1) Find the Inverse of a Square Matrix

(2) Applications in Cryptography.

Identity Matrices.

1 ⟶ Multiplicative Identity

What matrices play the role of 1 in multiplication?

$$\begin{pmatrix} 4 & 8 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 8 \\ 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 4 & 8 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 8 \\ 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is called the 2-by-2 identity matrix.

$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{I_3}$; $\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{I_4}$; . . .

The inverse of a matrix A, denoted by A^{-1}, is a matrix such that

$$A \cdot A^{-1} = I \quad \text{and} \quad A^{-1} \cdot A = I.$$

Formula to find the inverse of a 2-by-2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The inverse of A is given by the formula:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

provided that $ad - bc \neq 0$

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

E.g. $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$

Find A^{-1} using the formula.

$$A^{-1} = \frac{1}{2 \cdot 2 - 3 \cdot 1} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$$

$$A^{-1} = \frac{1}{1} \cdot \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$$

Check:

$$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Process to find the inverse of a 3-by-3 matrix.

E.g. Find the inverse of the matrix

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

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 3 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 1 & 0 \\ -2 & -2 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R_2 \leftarrow -2R_1 + R_2}$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 3 & 1 & 0 & 0 \\ 0 & 3 & -4 & -2 & 1 & 0 \\ -2 & -2 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R_3 \leftarrow 2R_1 + R_3}$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 3 & 1 & 0 & 0 \\ 0 & 3 & -4 & -2 & 1 & 0 \\ 0 & -4 & 7 & 2 & 0 & 1 \end{array}\right) \xrightarrow{R_2 \leftarrow \frac{1}{3} R_2}$$

$$\left(\begin{array}{ccc|ccc} 1 & -1 & 3 & 1 & 0 & 0 \\ 0 & 1 & -\frac{4}{3} & -\frac{2}{3} & \frac{1}{3} & 0 \\ 0 & -4 & 7 & 2 & 0 & 1 \end{array}\right) \xrightarrow{R_1 \leftarrow R_2 + R_1}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & \frac{5}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 1 & -\frac{4}{3} & -\frac{2}{3} & \frac{1}{3} & 0 \\ 0 & -4 & 7 & 2 & 0 & 1 \end{array}\right) \xrightarrow{R_3 \leftarrow 4R_2 + R_3}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & \frac{5}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 1 & -\frac{4}{3} & -\frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 0 & \frac{5}{3} & -\frac{2}{3} & \frac{4}{3} & 1 \end{array}\right) \xrightarrow{R_3 \leftrightarrow \frac{3}{5} R_3}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & \frac{5}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 1 & -\frac{4}{3} & -\frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{2}{5} & \frac{4}{5} & \frac{3}{5} \end{array}\right)$$

the inverse matrix

$$\xrightarrow[R_1 \leftrightarrow -\frac{5}{3} R_3 + R_1]{R_2 \leftrightarrow \frac{4}{3} R_3 + R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & -1 \\ 0 & 1 & 0 & -\frac{6}{5} & \frac{7}{5} & \frac{4}{5} \\ 0 & 0 & 1 & -\frac{2}{5} & \frac{4}{5} & \frac{3}{5} \end{array}\right)$$

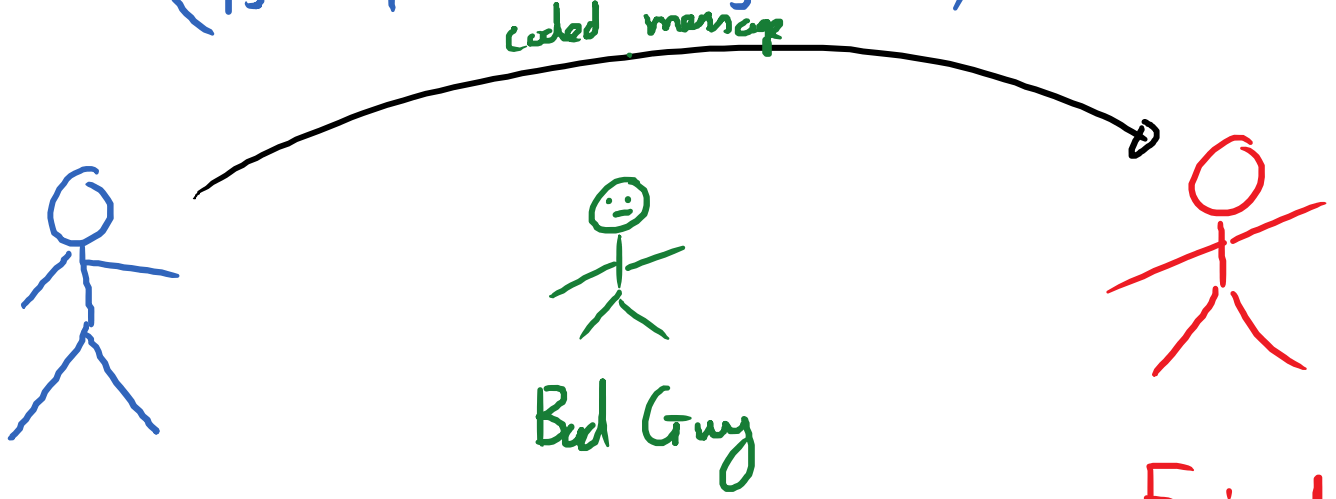
Application in Cryptography

"GOOD MORNING"

Blank	A	B	C
0	1	2	3

7 15 15 4 0 13 15 18 14 9 14 7

$$A = \begin{pmatrix} 7 & 15 & 0 & 15 & 14 & 14 \\ 15 & 4 & 13 & 18 & 9 & 7 \end{pmatrix}$$



You

$$B = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \rightarrow \text{Key}$$

Friend

$$BA = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 7 & 15 & 0 & 15 & 14 & 14 \\ 15 & 4 & 13 & 18 & 9 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 89 & 50 & 65 & 120 & 73 & 63 \\ 67 & 31 & 52 & 87 & 50 & 42 \end{pmatrix} \rightarrow \text{coded message}$$

C

$$B \cdot A = C$$

$$B^{-1} \cdot B \cdot A = B^{-1} \cdot C$$

$$A = B^{-1} \cdot C$$