Matrix Inverses and Cryptography

Finite Math

7 April 2017

Inverse of a 3×3 Matrix

Example

Find the inverse of the matrix

$$M = \begin{bmatrix} 2 & 2 & 0 \\ 1 & 2 & -3 \\ -2 & -3 & -1 \end{bmatrix}.$$

Now You Try It!

Example

Find the inverse of the matrix:

$$E = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.$$

Cryptography

Suppose we represent letters by numbers as follows

Blank	0	I	9	R	18
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26

Cryptography

Suppose we represent letters by numbers as follows

Blank	0	I	9	R	18
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26

Then, for example, the message “SECRET CODE” would correspond to the sequence

Cryptography

Suppose we represent letters by numbers as follows

Blank	0	I	9	R	18
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26

Then, for example, the message “SECRET CODE” would correspond to the sequence

19 5 3 18 5 20 0 3 15 4 5

Cryptography

The goal of Cryptography is to encode messages in a different sequence which can only be translated back to the message using a decoder.

Cryptography

The goal of Cryptography is to encode messages in a different sequence which can only be translated back to the message using a decoder.

Definition (Encoding matrix/Decoding matrix)

Any matrix with positive integer elements whose inverse exists can be used as an encoding matrix. The inverse of an encoding matrix is a decoding matrix.

Cryptography

The goal of Cryptography is to encode messages in a different sequence which can only be translated back to the message using a decoder.

Definition (Encoding matrix/Decoding matrix)

Any matrix with positive integer elements whose inverse exists can be used as an encoding matrix. The inverse of an encoding matrix is a decoding matrix.

To encode a message, we must first decide on a encoding matrix A. If A is a $n \times n$ matrix, then we create another matrix $n \times p$ matrix B by entering the message going down columns and taking as many columns as necessary to fit the whole message. Note that the number of rows of B MUST MATCH the size of A. If there are extra entries in B after fitting the whole message, just fill them with 0's.

Encoding Example

Example

Encode the message "SECRET CODE" using the encoding matrix

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

Decoding Example

Example

A message was encoded with A from the previous example. Decode the sequence

$$29 \;\; 12 \;\; 69 \;\; 28 \;\; 70 \;\; 25 \;\; 111 \;\; 43$$

Now You Try It!

Example

Use the encoding matrix

$$E = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.$$

(a) *Encode the message "MATH IS FUN" using E.*

(b) *Decode the sequence*

39 60 91 65 110 125 6 7 16 44 63 113 37 53 87