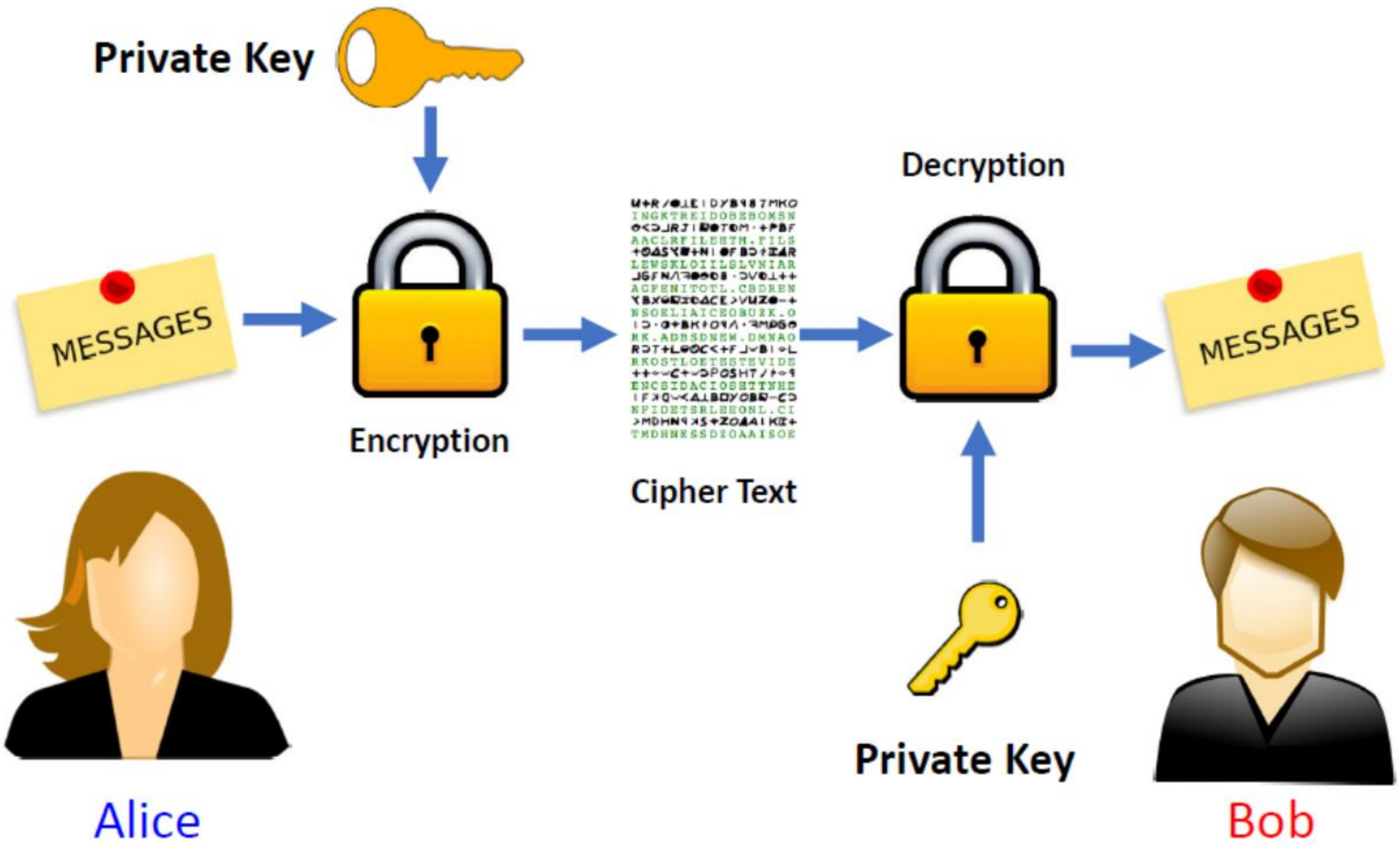
Cryptography

- A **cryptogram** is a message written according to a secret code (the Greek word *kryptos* means “hidden”).
- This section describes a method of using matrix multiplication to **encode** and **decode** messages.

Symmetric Cryptography



Cryptography (cont.)

- Begin by assigning a number to each letter in the alphabet (with 0 assigned to a blank space), as follows.

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

- Then the message is converted to numbers and partitioned into **uncoded row matrices**, each having *n* entries.

Forming Uncoded Row Matrices

Write the uncoded row matrices of size 1×3 for the message MEET ME MONDAY.

SOLUTION Partitioning the message (including blank spaces, but ignoring punctuation) into groups of three produces the following uncoded row matrices.

$$[13 \quad 5 \quad 5] \; [20 \quad 0 \quad 13] \; [5 \quad 0 \quad 13] \; [15 \quad 14 \quad 4] \; [1 \quad 25 \quad 0]$$

13	5	5	20	0	13	5	0	13	15	14	4	1	25	0
M	*E*	*E*	*T*	_	*M*	*E*	_	*M*	*O*	*N*	*D*	*A*	*Y*	_

Note that a blank space is used to fill out the last uncoded row matrix.

Cryptography (cont.)

- To **encode** a message, choose an $n \times n$ invertible matrix A and multiply the uncoded row matrices (on the right) by A to obtain **coded row matrices.**

Encoding a Message

Use the matrix

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

to encode the message MEET ME MONDAY.

SOLUTION The coded row matrices are obtained by multiplying each of the uncoded row matrices found in Example 4 by the matrix A, as follows.

$$\begin{array}{ccc} \textit{Uncoded Row Matrix} & \textit{Encoding Matrix } A & \textit{Coded Row Matrix} \end{array}$$

$$[13 \quad 5 \quad 5]\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [13 \quad -26 \quad 21]$$

$$[20 \quad 0 \quad 13]\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [33 \quad -53 \quad -12]$$

$$[5 \quad 0 \quad 13]\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [18 \quad -23 \quad -42]$$

$$[15 \quad 14 \quad 4]\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [5 \quad -20 \quad 56]$$

$$[1 \quad 25 \quad 0]\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [-24 \quad 23 \quad 77]$$

The sequence of coded row matrices is

$$[13 \quad -26 \quad 21][33 \quad -53 \quad -12][18 \quad -23 \quad -42][5 \quad -20 \quad 56][-24 \quad 23 \quad 77].$$

Finally, removing the brackets produces the cryptogram below.

$$13 \;\; -26 \;\; 21 \;\; 33 \;\; -53 \;\; -12 \;\; 18 \;\; -23 \;\; -42 \;\; 5 \;\; -20 \;\; 56 \;\; -24 \;\; 23 \;\; 77$$

Cryptography (cont.)

- For those who do not know the matrix *A*, decoding the cryptogram found in the previous example is difficult.
- But for an authorized receiver who knows the matrix *A*, decoding is simple.
- The receiver need only multiply the coded row matrices by A^{-1} to retrieve the uncoded row matrices.
- In other words, if

$$X = [x_1 \;\; x_2 \; \cdot \; \cdot \; \cdot \;\; x_n]$$

  is an uncoded $1 \times n$ matrix, then $Y = XA$ is the corresponding encoded matrix.
- The receiver of the encoded matrix can decode *Y* by multiplying on the right by A^{-1} to obtain

$$YA^{-1} = (XA)A^{-1} = X.$$

Decoding a Message

Use the inverse of the matrix

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

to decode the cryptogram

$$13 \quad -26 \quad 21 \quad 33 \quad -53 \quad -12 \quad 18 \quad -23 \quad -42 \quad 5 \quad -20 \quad 56 \quad -24 \quad 23 \quad 77.$$

SOLUTION Begin by using Gauss-Jordan elimination to find A^{-1}.

$$\begin{array}{ccc} [A \ \vdots \ I] & & [I \ \vdots \ A^{-1}] \\ \left[\begin{array}{rrr|rrr} 1 & -2 & 2 & 1 & 0 & 0 \\ -1 & 1 & 3 & 0 & 1 & 0 \\ 1 & -1 & -4 & 0 & 0 & 1 \end{array}\right] & \rightarrow & \left[\begin{array}{rrr|rrr} 1 & 0 & 0 & -1 & -10 & -8 \\ 0 & 1 & 0 & -1 & -6 & -5 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{array}\right] \end{array}$$

Now, to decode the message, partition the message into groups of three to form the coded row matrices

$$[13 \quad -26 \quad 21][33 \quad -53 \quad -12][18 \quad -23 \quad -42][5 \quad -20 \quad 56][-24 \quad 23 \quad 77].$$

Decoding a Message (cont.)

To obtain the decoded row matrices, multiply each coded row matrix by A^{-1} (on the right).

Coded Row Matrix	*Decoding Matrix A^{-1}*	*Decoded Row Matrix*

$$\begin{bmatrix} 13 & -26 & 21 \end{bmatrix} \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 13 & 5 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 33 & -53 & -12 \end{bmatrix} \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 20 & 0 & 13 \end{bmatrix}$$

$$\begin{bmatrix} 18 & -23 & -42 \end{bmatrix} \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 13 \end{bmatrix}$$

$$\begin{bmatrix} 5 & -20 & 56 \end{bmatrix} \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 15 & 14 & 4 \end{bmatrix}$$

$$\begin{bmatrix} -24 & 23 & 77 \end{bmatrix} \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 25 & 0 \end{bmatrix}$$

The sequence of decoded row matrices is

$$\begin{bmatrix} 13 & 5 & 5 \end{bmatrix} \begin{bmatrix} 20 & 0 & 13 \end{bmatrix} \begin{bmatrix} 5 & 0 & 13 \end{bmatrix} \begin{bmatrix} 15 & 14 & 4 \end{bmatrix} \begin{bmatrix} 1 & 25 & 0 \end{bmatrix}$$

and the message is

13	5	5	20	0	13	5	0	13	15	14	4	1	25	0.
M	*E*	*E*	*T*	__	*M*	*E*	__	*M*	*O*	*N*	*D*	*A*	*Y*	__