Lecture #3 Midterm – Let's Talk About Matrices & Cryptography
03.29.23

REMINDERS!

1) ALWAYS FOLLOW MY CLASSROOM PROCEDURES.

2) ACTIVITIES ARE ALWAYS UPDATED IN GOOGLE CLASSROOM, & MYOPENMATH

3) ALWAYS SUBMIT YOUR WORK ON TIME. NO MORE SUBMISSSION OF LATE WORK.

4) THE WEEKLY HOMEWORK IS ALWAYS DUE EVERY SATURDAY at 10:00 AM

5) CHECK THE UPDATES ON GOOGLE CLASSROOM AND DO YOUR MISSING ASSIGNMENTS as the GRADES are always UPDATED.

Note: **Activities that you failed to submit on-time will automatically disappear on the system.**

MyOpenMath

1) Bellwork 3 (Midterm) – Knowledge Retention is Essential 03.29.23

2) Activity #3 (Midterm) –Matrices, Cryptography, Probability, & More 03.29.23
(Due Date: April 4, 2023, 11:59 PM)

3) Weekly Homework # 3 (Midterm) – Recalling Knowledge is a MUST 03.29-04.06.23 ***(Due Date: April 4, 2023, 10:00 AM)***

Google Classroom

1) Lectures for Today 03.29.23

QUICK REVIEW (COMBINATORICS , MATRICES & EVERYTHING)

QUESTION #1

Add: $\begin{bmatrix} -8 & 4 & -7 \\ -3 & 7 & 5 \\ 3 & -8 & 5 \end{bmatrix} + \begin{bmatrix} -4 & -7 & -1 \\ 5 & -3 & 5 \\ -1 & -7 & -2 \end{bmatrix}$

$$\begin{bmatrix} \square & \square & \square \\ \square & \square & \square \\ \square & \square & \square \end{bmatrix}$$

QUESTION #2

Let $A = \begin{bmatrix} 2 & 1 \\ 1 & 3 \\ 0 & -4 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 3 & -1 \\ -7 & 4 \end{bmatrix}$.

Then

$A - B =$

$$\begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$$

QUESTION #3

Given the following matrices.

$$[E] = \begin{bmatrix} 1 & 6 & -1 \\ -10 & -5 & 7 \\ -4 & 9 & -7 \end{bmatrix} \text{ and } [F] = \begin{bmatrix} -3 & -8 & 6 \\ -5 & 3 & -4 \\ 1 & 4 & 5 \end{bmatrix}$$

Find $[E] \cdot [F]^T = \begin{bmatrix} \square & \square & \square \\ \square & \square & \square \\ \square & \square & \square \end{bmatrix}$

QUESTION 4

You are making your schedule for next semester. You have 8 choices for your math class, 10 choices for your English class, 15 choices for your communications class, and 7 choices for your elective. How many different schedules are possible?

QUESTION 5

Nine bands are to perform at a weekend festival. How many different ways are there to schedule their appearances?

QUESTION 6

If you randomly select a letter from the phrase "Robert likes to eat tacos at Chipotle," what is the probability that you select a vowel? (Your answer must be in the form of a reduced fraction.)

QUESTION 7

A die is rolled twice.

What is the probability the first roll is a 5?

What is the probability the next roll is an even?

What is the probability of showing a 5 on the first roll and an even number on the second roll?

Note: Permutations of *n* items taken *r* at a time.

P (n, r) represents the number of permutations of *n* items *r* at a time.

$$P(n,r) = \frac{n!}{(n-r)!} = {}_{n}P_{r}$$

QUESTION 8) P (8, 3)

Combination: Selection of members of the set where the order is disregarded. ***The order does not MATTER!***

C (n, r) represents the number of permutations of *n* items *r* at a time.

$$C(n,r) = \frac{n!}{(n-r)!r!} = {}_{n}C_{r}$$

QUESTION 9) C (12, 3)

QUESTION #10

Giving a test to a group of students, the grades and gender are summarized below

	A	B	C	Total
Male	17	2	15	34
Female	13	6	19	38
Total	30	8	34	72

If one student is chosen at random,

Find the probability that the student got a 'A' GIVEN they are female.

At the end of the lesson, students will be able to:
1) solve cryptography and encryption problems

Source: *https://byjus.com/jee/matrices/*

MATRICES

A rectangular array of m × n numbers ***(real or complex)*** in the form of ***m* horizontal lines** (***called rows***) and *n* ***vertical lines (called columns),*** is called a matrix of order m by n, written as m × n matrix. Such an array is enclosed by [ ] or ( ).

Introduction to Matrices

An m × n matrix is usually written as:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots\cdots & a_{mn} \end{bmatrix}$$

In brief, the above matrix is represented by A = $[a_{ij}]_{mxn}$. The number a_{11}, a_{12}, ... etc., are known as the elements of the matrix A, where a_{ij} belongs to the ith row and j^{th} column and is called the $(i, j)^{th}$ element of the matrix A = $[a_{ij}]$.

Source: https://byjus.com/jee/matrix-operations/

Operations on Matrices

Addition, subtraction and multiplication are the basic operations on the matrix. To add or subtract matrices, these must be of identical order and for multiplication, the number of columns in the first matrix equals the number of rows in the second matrix.

- Addition of Matrices
- Subtraction of Matrices
- Scalar Multiplication of Matrices

- Multiplication of Matrices

Addition of Matrices

If $A[a_{ij}]_{mxn}$ and $B[b_{ij}]_{mxn}$ are two matrices of the same order, then their sum A + B is a matrix, and each element of that matrix is the sum of the corresponding elements. i.e. $A + B = [a_{ij} + b_{ij}]_{mxn}$

Consider the two matrices A & B of order 2 x 2. Then the sum is given by:

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$

Properties of Matrix Addition:

If a, B and C are matrices of same order, then

(a) **Commutative Law:** A + B = B + A

(b) **Associative Law:** (A + B) + C = A + (B + C)

(c) **Identity of the Matrix:** A + O = O + A = A, where O is zero matrix which is additive identity of the matrix,

(d) **Additive Inverse:** A + (-A) = 0 = (-A) + A, where (-A) is obtained by changing the sign of every element of A which is additive inverse of the matrix,

(e) A+B=A+CB+A=C+A} ⇒B=C

$$\left.\begin{aligned} A+B&=A+C \\ B+A&=C+A \end{aligned}\right\} \Rightarrow B=C$$

(f) tr (A ± B) = tr(A) ± tr(B)

(g) If A + B = 0 = B + A, then B is called additive inverse of A and also A is called the additive inverse of A.

Subtraction of Matrices

If A and B are two matrices of the same order, then we define

A−B=A+(−B).

Consider the two matrices A & B of order 2 x 2. Then the difference is given by:

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ c_1 - c_2 & d_1 - d_2 \end{bmatrix}$$

We can subtract the matrices by subtracting each element of one matrix from the corresponding element of the second matrix. i.e. A – B = $[a_{ij} - b_{ij}]_{mxn}$

Video: https://www.youtube.com/watch?v=2spTnAiQg4M

Multiplication of Matrices

If A and B be any two matrices, then their product AB will be defined only when the number of columns in A is equal to the number of rows in B.

If

$A = [a_{ij}]_{m \times n}$. *and* $B = [b_{ij}]_{n \times p}$ *then their product* $AB = C = [c_{ij}]_{m \times p}$ will be a matrix of order m×p where

$$(AB)_{ij} = C_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}$$

Properties of matrix multiplication

(a) Matrix multiplication is not commutative in general, i.e. in general

$AB \neq BA.$

(b) Matrix multiplication is associative, i.e. (AB)C = A(BC).

(c) Matrix multiplication is distributive over matrix addition, i.e. A.(B + C) = A.B + A.C and (A + B)C = AC + BC.

(d) If A is an m × n matrix, then

$I_m A = A = A I_n.$

(e) The product of two matrices can be a null matrix while neither of them is null, i.e. if AB = 0, it is not necessary that either A = 0 or B = 0.

(f) If A is an m × n matrix and O is a null matrix then

$A_{m \times n}. O_{n \times p} = O_{m \times p}.$

i.e. the product of the matrix with a null matrix is always a null matrix.

(g) If AB = 0 (It does not mean that A = 0 or B = 0, again the product of two non-zero matrices may be a zero matrix).

(h) If AB = AC , B ≠ C (Cancellation Law is not applicable).

(i) tr(AB) = tr(BA)

(j) There exist a multiplicative identity for every square matrix such AI = IA = A

Key Idea. ***Multiplying matrices is only possible if, the column of the first matrix is equal to the row of the second matrix.***

For example:

A) 2 x 3 matrix and 3 x 2 matrix; you can multiply the matrix because the first matrix has 3 columns and the second matrix has 3 rows, so they are both 3 and multiplying the matrices will be possible.

B) 4 x 2 matrix and 4 x 2 matrix; you cannot multiply the matrix because the first matrix has 2 columns and the second matrix has 4 rows, so they are not equal and multiplying the matrices will not be possible.

EXAMPLE 1

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix} = \begin{bmatrix} (1)(7)+(2)(8)+(3)(9) \\ (4)(7)+(5)(8)+(6)(9) \end{bmatrix} = \begin{bmatrix} 7+16+27 \\ 28+40+54 \end{bmatrix} = \begin{bmatrix} 50 \\ 122 \end{bmatrix}$$

2 x 3 **3 x 1** **2 x 1** **2 x 1** **2 x 1**

columns on 1st = rows on 2nd

The number of rows in the 1st matrix and the number of columns in the 2nd matrix, make the dimensions of the final matrix

EXAMPLE 2

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{bmatrix} = \begin{bmatrix} 58 & \\ & \end{bmatrix} \qquad 1\times7 + 2\times9 + 3\times11 = 58$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{bmatrix} = \begin{bmatrix} 58 & 64 \\ & \end{bmatrix} \qquad 1\times8 + 2\times10 + 3\times12 = 64$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{bmatrix} = \begin{bmatrix} 58 & 64 \\ 139 & \end{bmatrix} \qquad 4\times7 + 5\times9 + 6\times11 = 139$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 & 8 \\ 9 & 10 \\ 11 & 12 \end{bmatrix} = \begin{bmatrix} 58 & 64 \\ 139 & 154 \end{bmatrix} \qquad 4\times8 + 5\times10 + 6\times12 = 154$$

Here are some of the points to be noted about matrix multiplication, as stated above.

1. **In order to multiply two matrices, the number of columns in the first matrix should be equal to the number of rows in the second matrix. Otherwise matrix multiplication cannot be done.**
2. **The resultant of multiplication of m*n matrix with n*p matrix will be a m*p matrix.**
3. **Matrix multiplication is not cumulative. It means, Matrix A x B ≠ Matrix B x A.**

EXAMPLE 3

Illustration 1:

If $A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & -2 & 1 \\ -1 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & -2 \\ 2 & 1 \\ 4 & -2 \end{bmatrix}$

find AB and BA if possible.

Illustration 1:

Solution:

Using matrix multiplication. Here, A is a 3 × 3 matrix and B is a 3 × 2 matrix, therefore, A and B are conformable for the product AB and it is of the order 3 × 2 such that

(First row of A) (First column of B)

$$= [2\,1\,3] \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} = 2 \times 1 + 1 \times 2 + 3 \times 4 = 16$$

.

(First row of A) (Second column of B)

$$= [2\ 1\ 3] \begin{bmatrix} -2 \\ 1 \\ -3 \end{bmatrix} = 2 \times (-2) + 1 \times 1 + 3 \times (-3) = -12$$

(Second row of A) (First column of B)

$$= [3\ \ -2\ 1] \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} = 3 \times 1 + (-2) \times 2 + 1 \times 4 = 3$$

Similarly

$$(AB)_{22} = -10, (AB)_{31} = 3\ and\ (AB)_{32} = 0$$

$$\therefore AB = \begin{bmatrix} 16 & -12 \\ 3 & -10 \\ 3 & 0 \end{bmatrix}$$

BA is not possible since the number of columns of B ≠ number of rows of A.

TRANSPOSE OF THE MATRIX

https://byjus.com/maths/transpose-of-a-matrix/

The transpose of a matrix is found by interchanging its rows into columns or columns into rows. The transpose of the matrix is denoted by using the letter "T" in the superscript of the given matrix. For example, if "A" is the given matrix, then the transpose of the matrix is represented by A' or A^T.

The following statement generalizes the matrix transpose:

$$If\ A = [a_{ij}]_{m\times n}, then\ A' = [a_{ij}]_{n\times m}.$$

Thus Transpose of a Matrix is defined as "A Matrix which is formed by turning all the rows of a given matrix into columns and vice-versa."

How to Find the Transpose of a Matrix?

Consider an example, if a matrix is a 2×3 matrix. It means it has 2 rows and 3 columns. While finding the transpose of a matrix, the elements in the first row of the given matrix are written in the first column of the new matrix. Similarly, the elements in the second row of the given matrix are written in the second column of the new matrix. Hence, the order of the new matrix becomes 3×2, as it has 3 rows and 2 columns.

$$A = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}_{2\times 3} \qquad A^T = \begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}_{3\times 2}$$

I DO 1) **Find the transpose of the given matrix**

$$M = \begin{bmatrix} 2 & -9 & 3 \\ 13 & 11 & -17 \\ 3 & 6 & 15 \\ 4 & 13 & 1 \end{bmatrix}$$

Solution- Given a matrix of the order 4×3 will become 3 × 4. The transpose of a matrix is given by interchanging rows and columns.

$$M^T = \begin{bmatrix} 2 & 13 & 3 & 4 \\ -9 & 11 & 6 & 13 \\ 3 & -17 & 15 & 1 \end{bmatrix}$$

YOU DO 1) **Find the transpose of the matrix N**

$$N = \begin{bmatrix} 22 & -21 & -99 \\ 85 & 31 & -2\sqrt{3} \\ 7 & -12 & 57 \end{bmatrix}$$

EXTRA EXAMPLE 1. Find the transpose of Matrix A

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$$

Properties of Transpose of a Matrix

To understand the properties of the matrix transpose, we will take two matrices A and B which have equal order. Some properties of the transpose of a matrix are given below:

(i) Transpose of the Transpose Matrix

If we take the transpose of the transpose matrix, the matrix obtained is equal to the original matrix. Hence, for a matrix A, (A')' = A

What basically happens, is that any element of A, i.e., a_{ij} gets converted to a_{ji} if the transpose of A is taken. So, taking transpose again, it gets converted to a_{ij}, which was the original matrix A.

Example: If

$$N = \begin{bmatrix} 22 & -21 & -99 \\ 85 & 31 & -2\sqrt{3} \\ 7 & -12 & 57 \end{bmatrix},$$

Then

$$N' = \begin{bmatrix} 22 & 85 & 7 \\ -21 & 31 & -12 \\ -99 & -2\sqrt{3} & 57 \end{bmatrix}$$

Now,

$$(N')' = \begin{bmatrix} 22 & -21 & -99 \\ 85 & 31 & -2\sqrt{3} \\ 7 & -12 & 57 \end{bmatrix}$$

$$= N$$

(ii) Addition Property of Transpose

Transpose of an addition of two matrices A and B obtained will be exactly equal to the sum of the transpose of individual matrices A and B.

This means,

$$(A+B)' = A' + B'$$

Example-

$$If\ P = \begin{bmatrix} 2 & -3 & 8 \\ 21 & 6 & -6 \\ 4 & -33 & 19 \end{bmatrix}\ and\ Q = \begin{bmatrix} 1 & -29 & -8 \\ 2 & 0 & 3 \\ 17 & 15 & 4 \end{bmatrix}$$

$$P + Q = \begin{bmatrix} 2+1 & -3-29 & 8-8 \\ 21+2 & 6+0 & -6+3 \\ 4+17 & -33+15 & 19+4 \end{bmatrix} = \begin{bmatrix} 3 & -32 & 0 \\ 23 & 6 & -3 \\ 21 & -18 & 23 \end{bmatrix}$$

$$(P+Q)' = \begin{bmatrix} 3 & 23 & 21 \\ -32 & 6 & -18 \\ 0 & -3 & 23 \end{bmatrix}$$

$$P' + Q' = \begin{bmatrix} 2 & 21 & 4 \\ -3 & 6 & -33 \\ 8 & -6 & 19 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 17 \\ -29 & 0 & 15 \\ -8 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 23 & 21 \\ -32 & 6 & -18 \\ 0 & -3 & 23 \end{bmatrix}$$

$$= (P+Q)'$$

So, we can observe that

$$(P+Q)' = P' + Q'.$$

(iii) Multiplication by Constant

If a matrix is multiplied by a constant and its transpose is taken, then the matrix obtained is equal to the transpose of the original matrix multiplied by that constant. That is,

$$(kA)' = kA'$$

where k is a constant

Example-

$$If\ P = \begin{bmatrix} 2 & 8 & 9 \\ 11 & -15 & -13 \end{bmatrix}_{2\times 3} \ and\ k\ is\ a\ constant,\ then\ (kP)'$$

$$= \begin{bmatrix} 2k & 11k \\ 8k & -15k \\ 9k & -13k \end{bmatrix}_{2\times 3}$$

$$kP' = k\begin{bmatrix} 2 & 11 \\ 8 & -15 \\ 9 & -13 \end{bmatrix}_{2\times 3} = \begin{bmatrix} 2k & 11k \\ 8k & -15k \\ 9k & -13k \end{bmatrix}_{2\times 3} = (kP)'$$

We can observe that

$$(kP)' = kP'.$$

(iv) Multiplication Property of Transpose

Transpose of the product of two matrices is equal to the product of transpose of the two matrices in reverse order. That is

$(AB)' = B'A'$

Example:

$A = \begin{bmatrix} 9 & 8 \\ 2 & -3 \end{bmatrix} and\ B = \begin{bmatrix} 4 & 2 \\ 1 & 0 \end{bmatrix}$

Let us find A×B.

$A \times B = \begin{bmatrix} 44 & 18 \\ 5 & 4 \end{bmatrix} \Rightarrow (AB)' = \begin{bmatrix} 44 & 5 \\ 18 & 4 \end{bmatrix}$

$B'A' = \begin{bmatrix} 4 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 9 & 2 \\ 8 & -3 \end{bmatrix}$

$= \begin{bmatrix} 44 & 5 \\ 18 & 4 \end{bmatrix} = (AB)'$

$\therefore (AB)' = B'A'$

$A'B' = \begin{bmatrix} 9 & 2 \\ 8 & -3 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 40 & 9 \\ 26 & 8 \end{bmatrix}$

We can clearly observe from here that (AB)′≠A′B′.

Those were properties of matrix transpose which are used to prove several theorems related to matrices.

QUICK REVIEW
WE DO 1)

Subtract: $\begin{bmatrix} 7 & 1 \\ -5 & -3 \\ -1 & -5 \\ 3 & 6 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ -6 & 2 \\ -4 & -8 \\ -1 & 3 \end{bmatrix}$

$$\begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$$

WE DO 2)

$$[D] = \begin{bmatrix} -3 & -8 & -10 & -5 & 0 \\ 3 & 10 & -4 & 5 & -4 \\ 3 & -3 & 9 & -10 & -1 \\ 0 & -9 & -8 & 1 & 7 \\ 8 & -1 & -6 & -9 & 8 \end{bmatrix}$$

$$[D] + [D]^T = \begin{bmatrix} \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{bmatrix}$$

WE DO 3)

Given the following matrices.

$$[D] = \begin{bmatrix} 3 & 9 \\ -1 & 5 \\ 6 & -5 \end{bmatrix} \quad \text{and} \quad [A] = \begin{bmatrix} -7 & 4 \\ 9 & -5 \end{bmatrix}$$

Find $[D] \cdot [A]^T = \begin{bmatrix} \square & \square \\ \square & \square \\ \square & \square \end{bmatrix}$

WE DO 4)

$$[A] = \begin{bmatrix} 10 & -1 & -10 & 6 \\ -4 & -8 & 2 & -9 \\ 4 & -5 & -3 & 5 \\ 8 & 9 & 7 & -2 \\ -6 & 1 & -7 & 0 \end{bmatrix}$$

The negative of $[A]$ is

$$\begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix}$$

Cryptography

Video: https://www.myopenmath.com/course/testquestion2.php?cid=158915&qsetid=31377&formn=selq&loc=qo0&checked=1

Cryptography and Encryption using Substitution Cipher

Cryptography

When people need to secretly store or communicate messages, they turn to cryptography. Cryptography involves using techniques to obscure a message so outsiders cannot read the message. It is typically split into two steps: encryption, in which the message is obscured, and decryption, in which the original message is recovered from the obscured form.

Substitution Ciphers

One simple encryption method is called a **substitution cipher**.

A simple example of a substitution cipher is called the **Caesar cipher**, sometimes called a **shift cipher**. In this approach, each letter is replaced with a letter some fixed number of positions later in the alphabet.

SAMPLE ENCRYPTION

Example: A Caesar cipher with a shift of 5 right would replace A with F, B with G, C with H, and so on.

A	B	C	D	E	F
A	B	C	D	E	F

Notice here after U is mapped to Z, we map the next letter V to A.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps To	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Use the shift of 5 right to encrypt the following message. "Meet at the bank at eight AM" Write the final code in 4 letter blocks.

RJJY FYYM JGFS PFYJ NLMY FRAA

EXAMPLE DECRYPTION

Decrypt the word RPJHT if it was encrypted using an alphabetic Caesar shift cipher with shift 15 (mapping A to P).

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps To	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

CAUSE

Notice that in both the ciphers above, the extra part of the alphabet wraps around to the beginning. Because of this, a handy version of the shift cipher is a cipher disc, such as the Alberti cipher disk shown here from the 1400s. In a cipher disc, the inner wheel could be turned to change the cipher shift. This same approach is used for "secret decoder rings.

http://en.wikipedia.org/wiki/File:Alberti_cipher_disk.JPG

The security of a cryptographic method is very important to the person relying on their message being kept secret. The security depends on two factors:

1. The security of the method being used
2. The security of the encryption key used

In the case of a shift cipher, the **method** is "a shift cipher is used." The **encryption key** is the specific amount of shift used.

Suppose an army is using a shift cipher to send their messages, and one of their officers is captured by their enemy. It is likely the method and encryption key could become compromised. It is relatively hard to change encryption methods, but relatively easy to change encryption keys.

During World War II, the Germans' Enigma encryption machines were captured, but having details on the encryption method only slightly helped the Allies, since the encryption keys were still unknown and hard to discover. Ultimately, the security of a message cannot rely on the method being kept secret; it needs to rely on the key being kept secret.

Encryption Security

The security of any encryption method should depend only on the encryption key being difficult to discover. It is not safe to rely on the encryption method (algorithm) being kept secret.

Brute Force Attack

A brute force attack is a method for breaking encryption by trying all possible encryption keys.

Suppose you intercept a message, and you know the sender is using a Caesar cipher, but do not know the shift being used. The message begins **EQZP**. How hard would it be to decrypt this message?

Since there are only 25 possible shifts, we would only have to try 25 different possibilities to see which one produces results that make sense. While that would be tedious, one person could easily do this by hand in a few minutes. A modern computer could try all possibilities in under a second.

Shift	Message	Shift	Message	Shift	Message	Shift	Message
1	DPYO	7	XJSI	13	RDMC	19	LXGW
2	COXN	8	WIRH	14	QCLB	20	KWFV
3	BNWM	9	VHQG	15	PBKA	21	JVEU
4	AMVL	10	UGPF	16	OAJZ	22	IUDT
5	ZLUK	11	TFOE	17	NZIY	23	HTCS
6	YKTJ	12	**SEND**	18	MYHX	24	GSBR
						25	FRAQ

To make a brute force attack harder, we could make a more complex substitution cipher by using something other than a shift of the alphabet. By choosing a random mapping, we could get a more secure cipher, with the tradeoff that the encryption key is harder to describe; the key would now be the entire mapping, rather than just the shift amount.

While there were only 25 possible shift cipher keys (35 if we had included numbers), there are about 10^{40} possible substitution ciphers. That's much more than a trillion trillions. It would be essentially impossible, even with supercomputers, to try every possible combination. Having a huge number of possible encryption keys is one important part of key security. There are 35 choices for what A maps to, then 34 choices for what B maps to, and so on, so the total number of possibilities is $35 \cdot 34 \cdot 33 \cdot \cdots \cdot 2 \cdot 1 = 35!$.

Unfortunately, this cipher is still not secure, because of a technique called frequency analysis, discovered by Arab mathematician Al-Kindi in the 9th century.

http://en.wikipedia.org/wiki/File:English_letter_frequency_(frequency).svg

WE DO 1) Write the shift of 7 right to encrypt the following message. "Hack the system at one PM". Write the final code in 5 letter blocks.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps to																										

WE DO 2) Decrypt the word NSCMBODO if it was encrypted using an alphabetic Caesar shift with shift 10 (mapping A to K)

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Maps to																										

EXTRA EXAMPLE 1

This question will guide you through the process of encrypting the sentence

the student stared at the quick airplane

with the encoding matrix

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

Step 1

Replace each letter in the sentence with the corresponding number: a = 1, b = 2, etc. Use 0 for blank spaces. Enter your answer as a comma-separated list of numbers:

Step 2

Arrange your list of numbers into the following matrix, proceeding from left to right. If you have empty spots at the end of the matrix, fill them with zeroes.

$$\begin{bmatrix} \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \end{bmatrix}$$

Step 3

Multiply the matrix you created in step 2 with the encoding matrix:

$$\begin{bmatrix} \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \end{bmatrix}$$

EXTRA EXAMPLE 2

This question will guide you through the process of encrypting the sentence

the fish raced the smelly airplane

with the encoding matrix

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 0 \\ -2 & 1 & 0 & 0 & -6 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Step 1

Replace each letter in the sentence with the corresponding number: a = 1, b = 2, etc. Use 0 for blank spaces. Enter your answer as a comma-separated list of numbers:

Step 2

Arrange your list of numbers into the following matrix, proceeding from left to right. If you have empty spots at the end of the matrix, fill them with zeroes.

$$\begin{bmatrix} \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{bmatrix}$$

Step 3

Multiply the matrix you created in step 2 with the encoding matrix:

$$\begin{bmatrix} \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{bmatrix}$$

Thank you for listening and paying attention!
Do the assigned activities!