ADRIANNA URBANO	DECRYPT KEEPERS	SCTC 4385
Grade Band: 7^{th} – 10^{th}	**Topics:** Modular Arithmetic Computer Science	**Lesson #:** 4- to 5-Day Unit Plan

BRIEF LESSON DESCRIPTION

Description:
Your role as an Intelligence Agent makes you responsible for solving problems and using logic and reasoning to solve crimes. Your specific task as a cryptographer is to uncover secret messages. Since you are in training, you will be encrypting riddles to prove your cryptography skills and your problem-solving skills. You will also decrypt and solve a riddle from another Intelligent Agent.

Leading Question:
How can we use mathematics to send and receive messages that no one can read except for us and the target audience?

PERFORMANCE EXPECTATIONS

Students Will Be Able To:

- Understand how to perform modular arithmetic
- Understand and utilize the modulo notation
- Encrypt and decrypt messages using the Vigenere Cipher
- Conduct meaningful research
- Connect the concept of modular arithmetic to computer science

Students Will Understand:
Modular arithmetic is based in divisibility. Through this unit, students will use the properties of divisibility to learn the basics of cryptography. The modulo operation (seen as % in computer programming) results in the remainder from division. Through this unit plan, the students will create encrypted messages, learn modular arithmetic to decrypt those messages, and later conduct research to learn why and how cryptography connects to computer science.

Key Definitions & Concepts:

- Division: the inverse operation of multiplication; repeated subtraction
- Modular Arithmetic: a method for finding remainders where all the possible numbers (less than the divisor) are put in a circle, and then by counting around the circle the number of times that the number is being divided, where the remainder is the final number landed on; often called “clock math” or “circle math”
- Remainder: the amount that is “left-over” after dividing one number by another

SPECIFIC LEARNING OUTCOMES

Standards:

CC.2.2.HS.C.3: Write functions or sequences that model relationships between two quantities.

- This standard connects to the unit plan because the students will be using modular arithmetic to connect one statement to another that have different representations but are the equivalent.

CC.2.2.HS.C.4: Interpret the effects transformations have on functions and find the inverses of functions.

- This standard connects to the unit plan because the students will be using modular arithmetic to decrypt messages (one function) and to encrypt messages (inverse function).

BACKGROUND INFORMATION

Prior Knowledge:

- Difference between integers and natural numbers
- Whole number division (long division process with a whole number remainder)

Mathematical Practices:	**Disciplinary Core Ideas:**	**Crosscutting Concepts:**
• Construct viable arguments and critique the reasoning of others • Reason abstractly and quantitatively • Look for make use of structure	• Mathematical relationships among numbers can be represented, compared and communicated • Mathematical relations and functions can be modeled through multiple representations and analyzed to raise and answer questions	• Observe and make use of patterns • Identify and utilize structure and function

Possible Preconceptions/Misconceptions:

Many students will complete the division process properly, but disregard having a whole number remainder. Since the point of this unit is to learn via inquiry and discovery, then expect students to struggle to understand why they need non-negative, whole number remainders. This is a key concept that they should fully understand after the encryption introduction and lesson.

LESSON PLAN → 5E (+) MODEL

Engage:

Engage the students with an anchoring event: a video clip from *A Beautiful Mind*. This clip shows the actor going through his mind to figure out what a board filled with numbers means. The purpose of clip is to engage students into a discussion of "what is cryptography?" and "how can cryptography be used?" The following is the link to the YouTube clip: A Beautiful Mind (https://www.youtube.com/watch?v=Vzpu-P2eRuI).

The students will then be engaged in a whole class discussion about how that video clip connects with the unit plan's goals and objectives. Teachers will use student responses to lead into the RAFT of the unit: the students' role as an Intelligence Agent going through the final step of basic training.

Explore:

Students will work in their groups (4 to 5 members per group) to complete a worksheet that explores modular arithmetic and the importance of the remainder in divisibility processes. This guided worksheet includes the following: connecting division to time via "Clock Math" and connecting the "Clock Math" to "Circle Math." The purpose of using "Clock Math" is to provide students with examples of modulus in base 12, but in a manner that is familiar to them (i.e. gauging time). The purpose of using "Circle Math" is to extend their understanding of modulus from base 12 to modulus of any natural number base. However, the students will not be directly told that they are using modular arithmetic. The worksheet also includes a critical thinking question in which students are shown examples of the modulus operator but not told what it is. They must analyze the expressions and the respective answers to produce an explanation of modulus. They will be engaged in group- and whole-class discussions regarding the patterns within the examples, and regarding the connection between the clocks, circles, and the "mystery" (modulo) operator. The students will then be formally introduced to modular arithmetic and given a definition. They will extend the clock and circle examples into formal modulus writing.

Once the students understand modulus, they will explore its connection to cryptography. They will be engaged in group- and whole-class discussions regarding cryptography, the remainders within modulus, and the connection between those topics.

After bridging the examples of modulus to cryptography, the students will explore the *benchmark lesson*: what the Vigenere Cipher is, how to use it, and its connection to modular arithmetic. We will prompt the students to take detailed notes on how to encrypt a message using the Vigenere Cipher. Students will then work in groups to solve a riddle and encrypt its solution using the cipher. This allows them to practice encryption more independently and take charge of their learning.

After encrypting their riddles, the class will lead into the *investigation lesson*: exploring decryption and how to complete its process. The students will not have a guided worksheet for this lesson. Rather, they will work with their groups to explore the proper way to reverse the

steps of encryption and share their ideas with the class. They will then exchange riddles with the other groups, decrypt those messages, and solve the riddles.

Explain:

Throughout the exploration, the students will engage in discussions that inquire their understanding and knowledge of the information at-hand. Thus, teachers will be informally asking students to explain all topics and relevant connections throughout the entirety of this unit.

The guided worksheet contains sections asking students how they arrived at the answer and asking if they notice any patterns between the problems.

The written assignment is designed to be one of the students' formal explanations of the unit plan. This letter will contain the following information: the encrypted riddle they sent, the decryption of the riddle they received, a description of the encryption and decryption process and their rationale (pertaining to how and why they learned how to decrypt).

The final project presentation is designed, in part, so that the students communicate the above information to the class along with their answers to the research topics.

Elaborate:

Concluding the exploration, the students will extend their understanding of modulus and cryptography by conducting research to answer the following: (1) where else cryptography is used and how, (2) what are other cipher methods and give an example, and (3) are there flaws in cryptography. The purpose of having the students answer these questions through research is to give them opportunity to make their presentations unique to their interests within the scope of this unit plan. This portion is the conclusion of the *investigation lesson* and the last section of the summative assessment.

Evaluate:

This unit plan is designed with having both informal and formal evaluations throughout its entirety. The informal evaluations will occur on all four or five days and in multiple outlets. Predominantly, the students will be asked leading and open-ended questions throughout the exploration of the unit. This will allow teachers to gauge surface-level student understanding. The guided worksheets provide the students with an outline of steps to understanding modulus and encryption. By surveying the students during completion of these worksheets, teachers will be able to hear any misconceptions or misunderstandings, and address such immediately. Also, teachers will be able to gauge the percentage of students grasping the content by listening to their conversations and explanations within the groups.

The formal evaluation within this unit plan occurs on the final day, and it includes the formal letter and presentation. Throughout the unit plan, the students will have had ample time to grapple with cryptography, ask questions, answer discussion topics and extend their understanding through research. The purpose of the letter is to have students formally explain

what they learned, how cryptography works, and why encryption and decryption act as an inverse function of the other (through modular arithmetic). The purpose of the presentation is to have the students communicate the purposes of the letter and their research to their peers. Each presentation is expected to be between 15 and 20 minutes long per group. Since there are 4 to 5 members per group, each student is expected to between a four (4) to five (5) minute part within their group's total presentation.

Enrichment:

The following websites provide teachers with the ability to differentiate this unit plan:

- Link: Practical Cryptography (http://practicalcryptography.com/)
    - The above website is mainly an informative source. It provides written explanations and examples of cryptography, including topics that are not covered in this unit. This source can be helpful in extending this lesson to higher grades.
- Link: Crypto Club (https://cryptoclub.org/)
    - The above website is mainly an interactive source. It allows for users to work through cryptography examples using different ciphers, to work through challenge questions, and to experience fun with cryptography. This is a great source to extend this unit into having a technology section.

This lesson can be further extended by having students write a computer program (using any language) to encrypt and decrypt text using the Vigenere Cipher. This allows students to think about the processes involved in cryptography and to break down these processes into executable, logical steps.

See all attachments on the following pages

Central Intelligence Agency

Washington, D.C., 20505

Dear Agents in Training,

Welcome to your Cryptography training! As an Intelligence Agent, you must be skilled in sending and receiving secret messages containing classified information. In this training, you must successfully encrypt a message (typically a riddle), disperse your message, and decrypt the message you received. Upon completion of class training, you must write a letter containing the following information:

1. Your encrypted message
    a. The encryption processes
    b. The riddle's solution
2. The encoded message you received
    a. The decryption processes
    b. The riddle's solution

Upon completion of the letter, you must also conduct research and answer three crucial questions:

1. Where else is cryptography used and how? Describe the processes.
2. What are some other cipher methods? Give and detail an example.
3. Are there any flaws to cryptography? Detail these findings.

You will be required to present your findings to representatives from the agency. If all of this is successfully completed, you will then move on to the final step in your spy training. We wish you the best of luck!

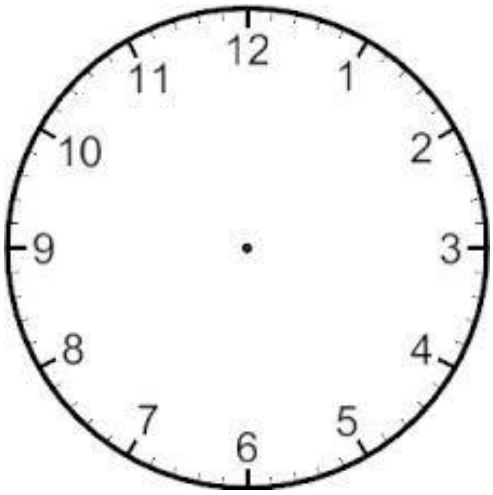
Sincerely,
Chief Special Agent
CIA Training Program Director

Rubric for Content Knowledge and Understanding			
Criteria	**Developing** (does not meet performance standards)	**Proficient** (meets performance standards)	**Advanced** (exceeds performance standards)
Part I: Formal Letter			
Completeness and Accuracy of Required Information : (1) The process taken to decrypt the coded message; (2) The riddle in PlainText; (3) The answer to the riddle; (4) The encrypted answer; (5) The process taken to encrypt the riddle's answer.	One or more pieces of required information are omitted	All required information is included	All required information is included
	Significant information is incorrect, key terms are used inappropriately, and/or important details are missing	Most significant information is correct, although there are some minor errors or missing details	All information is correct and discussed in detail
Part II: Research			
Completeness and Accuracy of Required Information : (1) Where else is cryptography used; (2) What are some other cipher methods; (3) Describe one or two other cipher methods; (4) Are there any flaws to cryptography; (5) How does computer hacking connect with cryptography?	One or more pieces of required information are omitted	All required information is included	All required information is included
	Significant information is incorrect, key terms are used inappropriately, and/or important details are missing	Most significant information is correct, although there are some minor errors or missing details	All information is correct and discussed in detail
Part III: Presentation			
Completeness and Accuracy of Required Information : (1) Detailed explanation of the content within the formal letter; (2) Detailed explanation of the research content	Less that half of the group members do not present a portion of the group's information	Half of the group members do not present a portion of the group's information	All group members present with equal speaking time
	Presentation is shorter than 5 minutes or longer than 25 minutes	Presentation is shorter than 15 minutes or longer than 20 minutes	Presentation is within the 15 to 20 minute time window
	Presenters were not able to accurately answer the posed questions after their given presentation	Presenters provided answers to posed questioning with few incorrect assumptions or few misunderstood concepts after their given presentation	Presenters provided knowledgable and coherent answers to posed questioning after their given presentation

Name: ._____. Date_____.

Clock Math

1. Say it is 9:00 AM, what time will it be in:



   a. 20 hours? How did you figure this out?

   b. 55 hours? How did you figure this out?

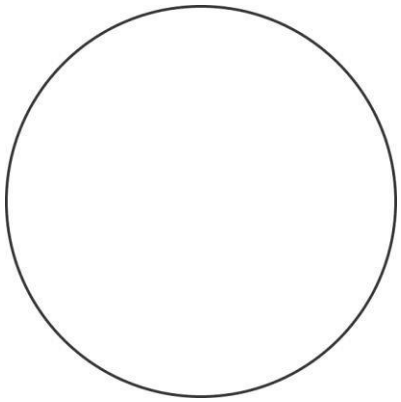
   c. 81 hours? How did you figure this out?

   d. Do you notice any patterns?

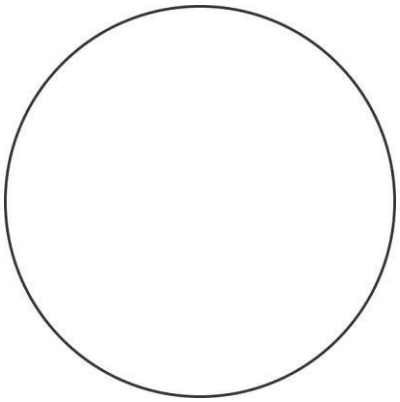
Circle Math

2. Use a circle to figure out (do not use traditional division):

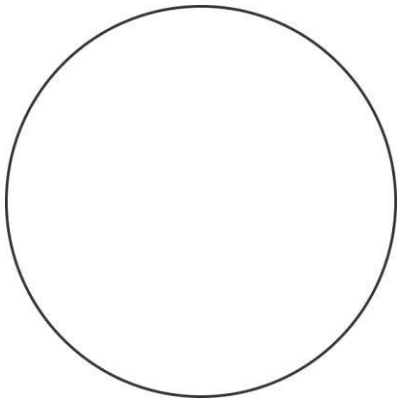
58/9 =



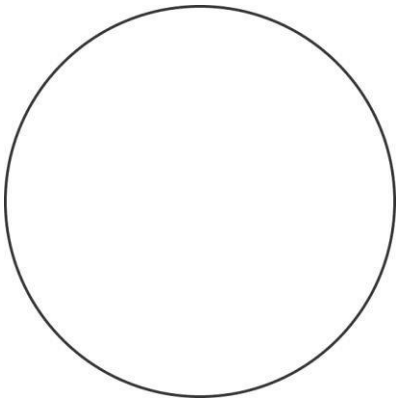
35/4 =



18/10 =



100/19 =



Are there any similarities between this problem and problem #1?

Modular Arithmetic

3. Now consider the “mystery” operation denoted by “mod”:

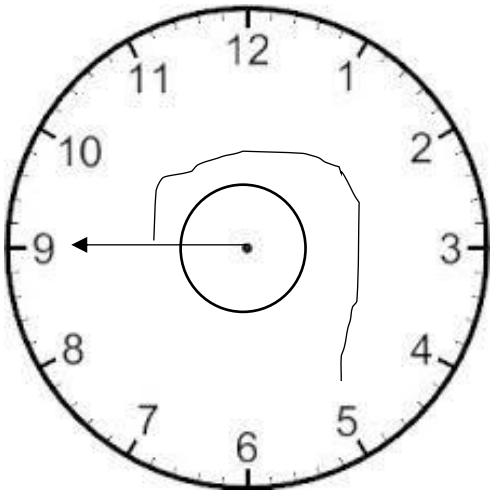
58mod9 = 4
18mod10 = 8
35mod4 = 3
20mod12 = 8

Do you notice any similarities between this operation and what you did in problems #1 and #2?

Hypothesize what the mod operation does:

Name: _____ANSWER_KEY_____ Date: _____

Clock Math



1. Say it is 9:00 AM, what time will it be in:
   b. 20 hours? How did you figure this out?

      5am
      Answers may vary

   c. 55 hours? How did you figure this out?

      4pm
      Answers may vary

   d. 81 hours? How did you figure this out?

      6pm
      Answers may vary

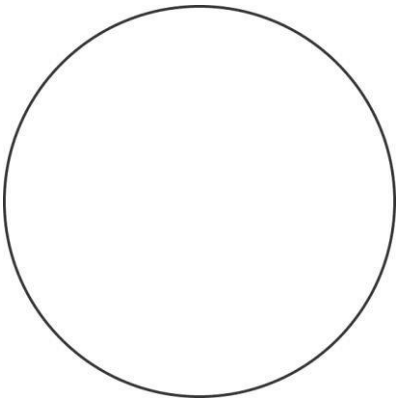
   e. Do you notice any patterns?

      Target answer: Each time we divided by 12 to see how many times the hour hand made a full rotation. Then, the remainder when we divided the time passed by 12 gave us the hour.

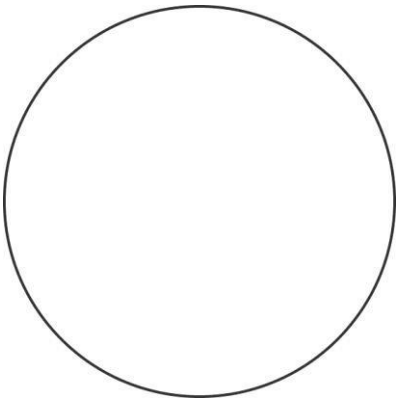
Circle Math

2. Use a circle to figure out (do not use traditional division):
   Like the clock, situate [1, base] around the clock, and make necessary rotations

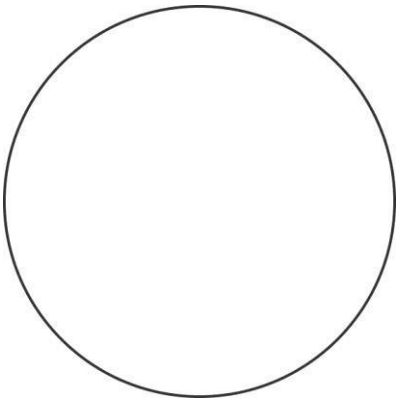
58/9 = 6 R 4



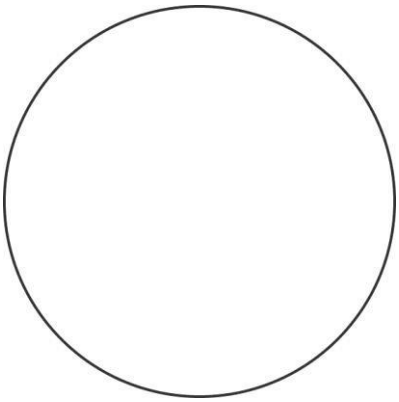
35/4 = 8 R 3



18/10 = 1 R 8



100/19 = 5 R 5



Are there any similarities between this problem and problem #1?

Here, the quotient is the number of rotations around the circle; in the clocks, the quotient was the number of rotations of the hour hand around the clock. In both, we found the remainder by seeing how many units were left over once we divided. The clocks were like this problem but we divided by 12 and had to start at a certain point.

Modular Arithmetic

3. Now consider the “mystery” operation denoted by “mod”:

   58mod9 = 4
   18mod10 = 8
   35mod4 = 3
   20mod12 = 8

   Do you notice any similarities between this operation and what you did in problems #1 and #2?

   58mod9 = 4 and 58/9 = 6 R 4, so they both have a 4 in the answer
   18mod10 = 8 and 18/10 = 1 R 8, so they both have an 8 in the answer
   35mod4 = 3 and 35/4 = 8 R 3, so they both have a 3 in the answer
   20mod12 = 8, which is how many hours we added in the first clock example after one rotation.

   The answer between the clocks, circle and modulus is the remainder after division.

   Hypothesize what the mod operation does:

   It gives us the remainder when the first number is divided by the second.

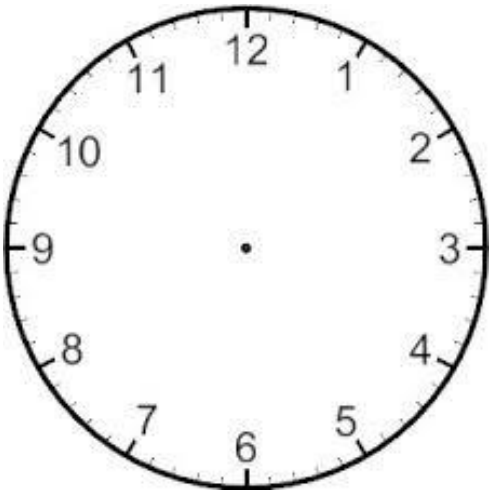
Name: _____ Date: _____

Clock and Circle Math Quiz

1.) Assume that it is 8:00 PM. What time will it be in 37 hours?

a. Use the clock to illustrate your answer

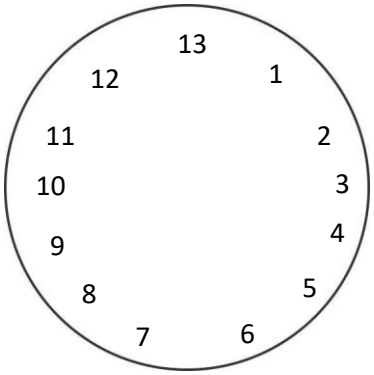
b. Represent your answer mathematically (i.e. write out your steps and solution explanation).



2.) Solve 85/13

a. Use the circle to illustrate your answer

b. Represent your answer mathematically (i.e. write out your steps and solution explanation).

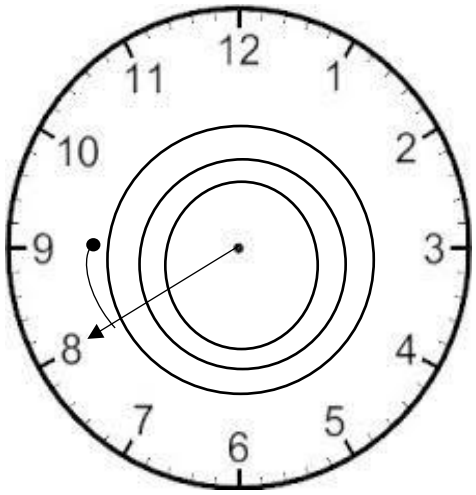


Name: _____ANSWER_KEY_____ Date: _____

Clock and Circle Math Quiz

1.) Assume that it is 8:00 PM. What time will it be in 37 hours?

a. Use the clock to illustrate your answer



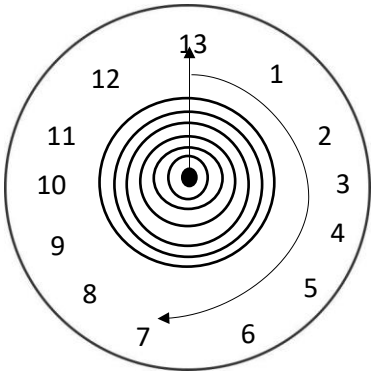
b. Represent your answer mathematically (i.e. write out your steps and solution explanation).

9:00 AM = 8:00 PM + 37 Hours

37 = 12(3) + 1 (where 3 is the number of revolutions and 1 is the remainder).

2.) Solve 85/13

a. Use the circle to illustrate your answer



b. Represent your answer mathematically (i.e. write out your steps and solution explanation).

85 = 13(6) + 7 (where 6 is the number of revolutions and 7 is the remainder).

Name: _____ Date: _____

Cryptography Worksheet

The vigenere cipher is one of many ways to conduct cryptography. Specifically, the Vigenere Cipher is an encryption processed by using interwoven Caesar ciphers. Remember that a cipher is the process of re-designating a number to a letter in the alphabet based on a keyword. In this example, we have the message BEST OF LUCK and our keyword is LIGHT. Using the numerated alphabet (Table 1) and modular arithmetic, we can code this message to be secretive to all other societies.

Steps explained:

- In column 1, we write out the message that we want to encrypt.
- In column 2, we write out the associated number from the table.
- We do this same process with our keyword for columns 3 & 4. Then, the computational steps come into play.
- In column 5, we find the sum of columns 2 & 4.
- In column 6, we take column 5 and compute modulo base 26. What does that mean? Let's look at the first row, column 6. We have 12mod26. Envision division such that 12/26. Without having decimals, how can we represent this answer? Well, how many times does 26 "go into" 12? (0 times) and what is the remainder? (12). That's what the modulo does; it gives us the remainder from division! Now let's look at the third row, column 6. We have 26mod26. Well, what is the remainder of 26/26? (the remainder is 0)! Let's look at the next row, column 6. We have 33mod26. Well, if we're doing 33/26, we get 1 remainder 7. What patterns are we noticing? If the number we computed is less than the base, than the remainder is that number. If the number is equal to the base, then the remainder is 0. If the number is greater than the base, then the remainder is what is left over after subtracting the base from the number (until the result is less than the base). Here, the base is 26 because there are 26 letters in the alphabet! This is the modulo base 26 step that completes column 6 and, essentially, encrypts our original message.
- Column 7 comes from using the numerated alphabet to write out the letters associated with the computed numbers. Hence, column 1 is our original message and column 7 is the encryption of that message!

See Figure 1 for the worked encryption example

Table 1:

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

Figure 1:

B	1	L	11	1 + 11 = 12	12mod26 = 12	M
E	4	I	8	4 + 8 = 12	12mod26 = 13	M
S	18	G	6	18 + 6 = 24	24mod26 = 24	Y
T	19	H	7	19 + 7 = 26	26mod26 = 0	A
O	14	T	19	14 + 19 = 33	33mod26 = 7	H
F	5	L	11	5 + 11 = 16	16mod26 = 16	Q
L	11	I	8	11 + 8 = 19	19mod26 = 19	T
U	20	G	6	20 + 6 = 26	26mod26 = 0	A
C	2	H	7	2 + 7 = 9	9mod26 = 9	J
K	10	T	19	10 + 19 = 29	29mod26 = 3	D
			KEY			
			What we're given			
			Based on the chart			
			What we compute			

Riddles (Some samples from prior students)

Riddle One:

How can you throw a ball as hard as possible,
To only have it come back to you,
Without the ball bouncing off of anything?
Keyword: BRIGHT

Riddle's Solution:_____

Answer: THROW THE BALL STRAIGHT UP

Riddle Two:

Two mothers and two daughters went out to eat.
Everyone ate one burger, but only three burgers were eaten.
How is this possible?
Keyword: THRONE

Riddle's Solution:_____

Answer: ONE MOTHER IS ALSO A DAUGHTER

Riddle Three:

What occurs once in a minute,
Twice in a moment,
But never in a thousand years?
Keyword: TEAM

Riddle's Solution:_____

Answer: THE LETTER M

Riddle Four:

They come out at night without being called.
They are lost in the day without being stolen.
What are they?
Keyword: FORCES

Riddle's Solution: _____

Answer: STARS

Name: _____ Date: _____

Decryption Worksheet

Encoded Message: I T Y Z F C S F P O S

Keyword: BLUE

CODED	NUMERATED ALPHABET	KEYWORD	NUMERATED ALPHABET	COMPUTATION	MOD 26	DECODED
I						
T						
Y						
Z						
F						
C						
S						
F						
P						
O						
S						

Name: _____ Date: _____

Decryption Answer Key

Encoded Message: I T Y Z F C S F P O S

Keyword: BLUE

CODED	NUMERATED ALPHABET	KEYWORD	NUMERATED ALPHABET	COMPUTATION	MOD 26	DECODED
I	8	B	1	7	7	H
T	19	L	11	8	8	I
Y	24	U	20	4	4	E
Z	25	E	4	21	21	V
F	5	B	1	4	4	E
C	2	L	11	-9	17	R
S	18	U	20	-2	24	Y
F	5	E	4	1	1	B
P	15	B	1	14	14	O
O	14	L	11	3	3	D
S	18	U	20	-2	24	Y