VAN VICKLE

8/4/2016

RISING 6TH - 8TH GRADE

Encryption
Rationale

Concept: Patterns Inform Prediction

The learning concept is a subset of the pattern recognition subset.
---Gilberto de Paiva

The foundation of this unit of instruction is the underlying assumption that pattern recognition is a fundamental component of cognitive and intellectual development and is necessary for abstract mathematical reasoning. Most sentient beings use patterns to make cognitive maps of the world around them, recognize individuals of the same or differing species and communicate emotively through sound, body posture and gesture (Mattson, 2014). Pattern recognition is used for the most fundamental tasks of discerning danger and identifying necessary resources. Of all creatures, human beings are the most sophisticated species at pattern recognition. So fundamental to human development is pattern recognition and prediction that we are immersed it from the moment we are born.

When we are infants, our brains are pattern-making machines. As we experiment with visual and motor skills, our movements become less reflexive and more intentional. In the nativist theory of language development, Noam Chomsky argues that human beings are pre-programmed to learn language by observing universal patterns in speech, classifying them and making generalizations. Expanding on this research is the suggestion that an infant's affective experiences display inherent patterns that heavily influence the child affecting both language development and cognitive abilities. As cognitive abilities develop sophistication, we become capable of advanced abstract reasoning.

As human beings, we observe and document patterns in every aspect of our world. Patterns abound in nature and science; the spirals in a sunflower seed, the spread of disease and the cycles of weather to name a few. History creates generational cyclical patterns that we chronicle and sometimes attempt to influence. In addition, we create patterns in our music, art and literature. It is this enduring and overarching nature of patterns and prediction that supply the foundation for this unit on encryption.

Content

Functions are the backbone of a great deal of the high school mathematics curriculum in the United States. *The Place of Functions in the School Mathematics Curriculum*, states, "As the discipline of mathematics has grown, function has become one of the most important and fundamental mathematical concepts as a way to organize and characterize mathematical relationships. A common expectation is that at the end of high school, students will know the function concept in general and be familiar with specific types of functions, including linear,

quadratic, general polynomial, reciprocal, power, step, exponential, logarithmic, trigonometric, and piece-wise functions in different representations (PCMI, 2016). Beginning in eighth grade and extending through the study of Calculus, functions are a major cornerstone of the conceptual understanding that students need to acquire.

Traditional mathematics instruction almost always teaches functions from the viewpoint of one or several of the various classifications of functions listed above. Most commonly students begin with the study of linear functions and add on polynomials and power functions followed by exponential, reciprocal, logarithmic and culminate with trigonometric functions. Somewhere along the way we toss in an exposure to step and piece-wise functions and hope the students understand the general nature of a function. It is possible, however, for students to become caught up in the specifics of the types of functions and miss the essential understanding of what a function is. In creating this unit on encryption, I wanted to approach functions from a new perspective; allowing my students to experience the characteristics of a function by examining methods of encryption that were functions and contrasting encryption methods that were not. This approach gives us a powerful way to examine the characteristics that define functions without studying a specific type of function.

Encryption is a great vehicle for this content as student interest is high. Most middle school children have no desire to formally study mathematical functions but they are fascinated by the mystery of secret codes. Some make up their own secret languages to communicate with their friends and siblings. Others may have taken a beginner's programming course and are interested in the topic of encryption from a technological standpoint. So given this is a summer camp experience, I felt we should explore something that is fun and interesting!

Skill

Pattern recognition is a fundamental skill underpinning critical thinking and forms the bases for all mathematical inductive reasoning. In my years of teaching mathematics, I have found the basic ability to recognize patterns in numbers, shapes and processes is essential to students who are able make the leap into the study of more abstract mathematical concepts. Children, who can readily identify and describe patterns in numbers such as 2, 4, 8, 16, 32, generally grasp the abstract notion of functions and their algebraic representations. Those who struggle with describing these patterns have a harder time with mathematical reasoning. Encryption gives us a way to look at patterns from a new perspective and allows students to explore different types of patterns using well-defined techniques.

Sometimes patterns in numbers, shapes or sequences are so easy to see that most individuals can describe the pattern. For example, most of us could describe the sequence of 2, 4, 6, 8, 10, as counting in 2's, but not all patterns are easily identifiable to all students. In these cases, the process of induction requires we use some strategies to determine if a pattern exists and if so what type of pattern it is.

We might explore mathematical operations of adding, subtracting, multiplying or dividing. Fractions might be involved. Graphing the sequences often elucidates a pattern as does determining first and second differences. As students advance in their study of mathematics, they need to have a robust tool-kit to aid their pattern recognition skill set so they can work with patterns that are not quite so obvious. In this unit of instruction, students will refine their skills of observing and classifying patterns used in simple encryption techniques. They will learn ways of rearranging language patterns using substitution and transposition and combine these with basic geometric patterns used to encrypt messages.

Differentiation for Gifted Learners

It is commonly accepted that differentiation is necessary to adequately serve the gifted child and while gifted children are not a homogenous group, they do have common needs to which our differentiation efforts should attend. Their curriculum should move more quickly than the 'normal' curriculum and should include tasks that are more complex and dig deeper into the essential understandings. Because gifted students have an intrinsic need to be challenged, their curriculum should provide an opportunity for each child to work at the edge of their abilities. Finally, since gifted students are going to be the individuals who generate unique ideas within disciplines, differentiation in the gifted curriculum must provide room for creativity.

Differentiation in Content

The study of functions is normally introduced in 8th grade and is central to the high school math curriculum. By exploring functions from the perspective of encryption, rising 6th, 7th and 8th graders had the opportunity to work with functions before they are typically introduced to the concept mathematically. This acceleration in a novel and complex setting allowed students to build a basic understanding of functions by observing examples of functions and non-examples of functions. Only their foundational level of mathematical thinking and their creativity limited the complexity of the students' thought about functions. Some of the older students were able to articulate that decryption was an inverse function and were able to explain this mathematically with very little prompting. Exposure in this manner will help them to move easily into the formal study of functions well before grade level.

Differentiation in Process

Throughout the unit, students were asked to use critical thinking skills and creativity. As they worked collaboratively to encrypt and decrypt messages they needed to think both "forward" and "backward" to apply the skills of their encryption techniques. Students were also encouraged to examine the complexity of their encryption method and discuss its predicted level of secrecy. Working from multiple perspectives and self-evaluating increased their depth of thinking. In addition, the students used a great deal of creativity as they developed their own encryption technique and tested it in a simulation.

Differentiation in Product

The final product that the students created for the four-day course was a unique encryption tool or technique that they used to communicate with teammates in a game of Risk. In order to devise this encryption technique, the students had to understand substitution and transposition techniques as well as the time-sensitive nature of an encryption tool. Each day the lessons built in complexity and students had the ability to look at the product as they had left it the day before and make

refinements that built in complexity. In this way, they were challenged to be self-evaluative and think deeply about the level of complexity of their encryption technique. Some of the groups were ready to move forward and include much more creative and complex elements in their encryption techniques while others (and not always the younger students as one would suspect) were more comfortable with common techniques. This allowed for a great deal of creativity in a collaborative environment.

Differentiation in the Learning Environment

Much of the work of our week of encryption was done collaboratively. By working together, gifted students often challenge each other in ways that teachers cannot. For example, as the students developed their product, there were times when one of the team members would stop working, satisfied that they had created the final version. Moments later, a second teammate would make a suggestion or ask a question that would cause the entire group to reevaluate their progress. By working collaboratively, the students were encouraged to be as creative as possible and to share ideas in order to work at increasing levels of depth and complexity.

The competitive nature of the product assignment encouraged the students to put a great deal of effort into their work. All three groups expressed a desire to have the "best" encryption tool. In some cases "best" meant most complicated and in others "best" meant most creative. The Risk game simulation brought out the natural competitive nature of the students.

Intended Population

Distinguishing Characteristics

The intended population for this unit of instruction is gifted (AIG) middle school students in Durham Public Schools (DPS). While this camp experience would be fun and instructive for most middle school students, by definition, the attendees of SPARK Camp are AIG identified DPS students. The encryption unit was designed to appeal broadly to students of varying genders, ethnic groups and socioeconomic backgrounds. The students that participated in the encryption course were varied in grade level, social maturity, mathematical sophistication and gender, but there was a lack of socioeconomic and ethnic diversity. One explanation might be that minority and lower socioeconomic students are underrepresented in the gifted classroom, however other SPARK camp classes contained a more diverse student population. In order to determine the reasons for this disparity, one would need to look at the student choices for courses and the method for assigning students to courses.

All students, regardless of age and social maturity level were able to focus on the task at hand for extended periods of time, a shared characteristic of gifted learners. Several students displayed typical middle school social behavior, but the majority of the students were socially adept beyond their years. They all enjoyed working collaboratively (with the exception of one extremely shy student) and socializing with each other and the adults at SPARK camp. All of the students grasped the basic concepts of encryption quickly and were eager to move on to more sophisticated techniques. Without exception, they enjoyed creative problem solving activities.

Background

One of the students had previous experience in encryption and quickly recognized the Pigpen Cipher I used on the first day to introduce the unit. Some of the students had taken programming courses and were familiar with binary numbers. Others had little or no experience with the techniques we were practicing in the class. The minimum level of mathematical instruction was completion of 5th grade mathematics and the maximum level was completion of 7+ math. Due to concerns about the rising 6th graders mathematical background, I eliminated the lesson on modulus arithmetic. In retrospect, I would include it. These students are eager for novel mathematical insights despite the level of their previous learning. If the lesson were well scaffolded, they would have been capable of learning modulus arithmetic techniques of encryption.

Needs

Throughout the week, the students clearly communicated their need to be challenged, to be creative and to be social. The first lesson organized in Taba format was intended to give the students exposure to the basic ideas, history and vocabulary of encryption. I found that the SPARK camp students were impatient to begin actually encrypting messages and wanted to rush through this lesson to get to the "fun" stuff. Several complained that this lesson felt too much like school. It was clear to me that asking students to mark the text (a challenging task for most) was a different kind of challenge than allowing them to solve puzzles. It was clear that what excites gifted students is not necessarily a challenge, but rather a novel problem to solve.

Once I introduced the game of Risk and framed the encryption in the realm of game play, the students were excited and the interest level rose considerably. Gifted students enjoy play that requires critical thinking and they were excited by the creativity involved in making their own unique encryption technique. Many gifted students are compelled to be creative and this task allowed them to exercise this drive.

The students' need for social interaction was undeniable. They enjoyed collaborative work both in pairs and in small groups. They spent time on task in these groupings but also invested time in off task socializing. When given breaks, many of the students socialized with adults and with each other in an adult-like manner. Several, however, continued playground socialization as they engaged in elementary school games of chase and gave in to the impulsiveness seen in younger children. At times the more socially mature students showed some resistance at working with the less mature students and gave social corrections to their peers.

Goals

Goal 1 (Content): To understand that a function is a rule that assigns exactly one output for a given input. CCSS (8.F.1)

Students will be able to...

A. Evaluate an encryption technique to determine whether it represents a function.
B. Describe encryption and decryption techniques mathematically.
C. Apply encryption techniques that are functions to encrypt and to decrypt.
D. Apply encryption techniques that are not functions to encrypt and decrypt.
E. Create an original encryption technique and describe the characteristics that classify it as a function or non-function.

Goal 2 (Process): Students will look for and make use of structure.

Students will be able to...

A. Identify and classify patterns represented in diverse encryption techniques.
B. Compare historical requirements of encryption and provide evidence of the impact of technology on the development of increasingly sophisticated encryption techniques.
C. Make inferences about the sophistication of different encryption methods.

Goal 3 (Concept): Students will understand that Patterns inform Prediction

Students will be able to...

A. Make predictions about the intent of a group of people based in the patterns observed in encrypted messages.
B. Evaluate historical methods of encryption based on patterns.
C. Make inferences about game strategy based in patterns observed in encrypted messages.
D. Generate an original method of encryption designed to prevent patterns from being observed and consequently thwarting prediction.

Formative Assessment Day 1

As students are given the opportunity to observe patterns in a message written on strange metallic material. Opportunities for formative assessment are

- What preexisting knowledge do students have of encryption techniques if any?
- What do students understand about letter frequency as a form of pattern recognition?
- How are the group dynamics working (or not) in the prearranged work groups?

As students read articles about encryption and make lists of ideas and issues surrounding encryption; they are asked to group these lists.

- What skills do the students have for marking the text?
- What methods are the students using as they work through the grouping process?
- What difficulties are the students having as they work through the grouping process?
- What similarities and differences exist as each student group makes headings for their lists?

Formative Assessment Day 2

As students make and use the St. Cyr Cipher Strip to encode and decode a message.

- What depth of understanding are students revealing by the questions they are asking as they work on their messages?
- How are students increasing the complexity level by modifying the encryption technique?
- What is the sophistication of the language (vocabulary) that the students are using to discuss the encryption technique as a function or non-function (pro/con sheet)?

As students begin work on their performance task

- How are students using what they understand about functions to modify their encryption technique increasing its level of sophistication?
- How are students self-evaluating their encryption techniques based on what they understand about functions?

- How are students using patterns to inform their choices about encryption techniques?
- What vocabulary is being used that indicates understanding about functions, pattern recognition and encryption techniques?

Formative Assessment Day 3

As students move through the stations using historical encoding techniques

- What questions do they have about the way the encryption devices and techniques work?
- What criteria are they using about how to evaluate the methods of encryption?
- What similarities between encryption techniques are they observing?
- What are the characteristics of the encryption devices that the students are most interested in?

As students write their letters.

- How are students progressing as they work independently?
- What questions do they have about the requirements of their letter?
- How are the students incorporating elements of pattern recognition and functions into their recommendations?

As students work on their performance task.

- What elements of the encryption devices have they isolated and incorporated into their performance task?
- How is their encryption task increasing in sophistication?

Summative Assessment Day 4

As students use their encryption techniques to play the Risk game.

- Are students able to use the encryption technique to send messages?
- Are students able to observe the patterns in the encryption techniques in order to decode messages?
- Are opposing groups able to observe the patterns in each other's code and "break" the code?
- How does the encryption technique measure up against the rubric?

The Performance Task
Topic: Encryption
Van Vickle

G	On the last day of class you will be participating in a role-playing game in which you, along with your allies, will be working to establish world dominance over forty-two territories on six continents. When you play this game, you will be working in teams – some of the teams will be your allies and others will be your opponents. You will need a secure way to communicate with your allies and obscure your messages from your opponents.
R	Your job is that of encryption specialist. You must devise the process or tool through which you will encrypt your messages to your allies. You must try to make your method of encryption secure without making it so complex that your allies have trouble deciphering the messages.
A	Your encryption device will be evaluated by how well it enables you to communicate with your allies and, at the same time, keeps your messages safe from decryption from your opponents. You can assume that the enemy will intercept all of your messages so make sure to consider the standard methods of decryption that may be used to break your code.
S	Keep in mind, this method may or may not use a tool (like the Caesar Cipher) but it will be used in a fast-paced game and as a result should be engineered for such. You should use methods of substitution and transposition, and should also provide for windows of time after which your method expires and necessitates a change to a different encryption rule.
P	You should produce your tool from the materials in the classroom, which include cardstock, paper, markers, brads etc., and provide instructions for using your tool. You may choose not to make a tool, but you must clearly define the instructions for your encryption method. Whether you make a tool or not, you should write the rules of encryption down completely using appropriate vocabulary so that individuals with no experience in encryption could follow them.
S	To determine if you are successful, make sure to use your method of encryption to encode several messages and have your teammates decipher them. This will help you gauge the security of your encryption technique and will also give you feedback on whether it is too complicated for fast-paced game play.

Encryption Performance Task Rubric
Van Vickle

	Score / Weight	Expert (4)	Practitioner (3)	Apprentice (2)	Novice (1)	Weight X Score
Encryption Tool allows for clear communication between command center and the front line.	30%	Team members are consistently able to use the tool fluidly for encryption and decryption and are including changes is the tool due to time expiration.	Team members are generally able to use the tool fluidly to encrypt and decrypt messages with minor difficulties and misunderstandings.	Team members occasionally use the tool to encrypt and decrypt. Significant numbers of misunderstandings or decryption failures exist.	Team members are rarely able to use the tool to encrypt and decrypt. Major misunderstandings of decryption failures occur.	
Encryption tool utilizes either a substitution cipher or a transposition cipher or both.	20%	Tool methods demonstrate a thorough and complete understanding of the techniques of substitution and/or transposition.	Tool methodology demonstrates a substantial understanding of the techniques of substitution and/or transposition with minor inaccuracies.	Tool methodology demonstrates a partial or incomplete understanding of the principles of substitution and/or transposition.	Tool methodology contains significant misunderstandings of the principles of substitution and/or transposition.	
Tool or Rule is clearly defined and instructions are clear so that someone unfamiliar could use it.	20%	Instructions for exceptionally clear and easy to follow so that an individual that did not develop your cipher could use them. Appropriate vocabulary is used	Instructions for use are generally clear and require only small inferences for use by an individual that did not develop the method. Inaccuracies do not substantially affect the use of the tool. Appropriate vocabulary shows some lack of sophistication	Instructions for use lack clarity and are difficult to follow for an individual that did not develop the tool. Lack of appropriate vocabulary is evident.	Instructions for use are unclear and prevent an individual that did not develop the tool to use it. Vocabulary is missing or inappropriately used.	
Method of encoding obfuscates patterns sufficiently so that without the tool it is not easily broken.	20%	Encrypted messages are highly effective at obfuscation and are very difficult to break using standard methods.	Encrypted messages are generally effective at obfuscation but are given time are breakable using standard methods.	Encrypted messages are somewhat effective at obfuscation but are easily breakable using standard methods.	Encrypted messages are ineffective at obfuscation and simple inspection allows for code breaking.	
Your tool identifies a time and upon expiration allows for a shift to a similar method of encryption.	10%	Time period shifts are present and highly effect and fluid in the encryption/decryption process.	Time period shifts are present and generally effective and fluid in the encryption/decryption process.	Time period shifts are present but are somewhat effective and fluid in the encryption/decryption process.	Time period shifts are missing or are ineffective or lack fluidity in the encryption/decryption process.	

Student Work Samples
The Letter

On the third day of the camp, students examined several examples of historical encryption techniques. They were assuming the role of advisor to the "general" and were asked to recommend an encryption technique for use in upcoming battle communications. The letters on the following pages are a sample of the letters produced. In many cases, the students were able to identify the Vigenere Square as the most sophisticated encryption method but they did not articulate the fact that its sophistication relied on the lack of letter and word frequency identification.

I believe that the reason the students did not mention this was not because they didn't understand the pattern recognition concepts, but rather a lack of specificity in my instructions for requirements for the letter. In retrospect, I would have an adult volunteer from SPARK camp come into the room dressed in 'military regalia' and describe the requirements of the assignment. I would also emphasize this in the prewriting assignment as we list pros and cons of each encryption technique.

Dear Army General,

Starting in the near future I think that our Army should use Skytale Code to communicate on and off the battlefield. Once you know how to encode and decode messages it is very simple to communicate. If a spy or another army some how manage to get ahold of the encoded message, it would just look like a bunch of gibberish. You would have to have the correct sized Rod to figure out what the message says. Even if the message got into the wrong hands and they happened to know Skytale (highly unlikely!) they wouldn't know which size rod to use!

From,

Addie

Letter frequency?

Dear Ferenc,

they are [illegible] decade, and because It is also

Pattern Recognition
Contrasting Differing methods

Dear Mr. general sir:

I thinketh that should changeth our codes to the vigenere square. It is quick and easy to encode and decode, so even the moste uneducated of our troops will be able to use it. It requires a code word, and if often we switcheth it, our enemies will never crack it. with this code, will we beateth our enemies and take over the world?. I thinketh so!

From:

future-Supreme-lord-and-ruler-and-king-and-president, henry shearer

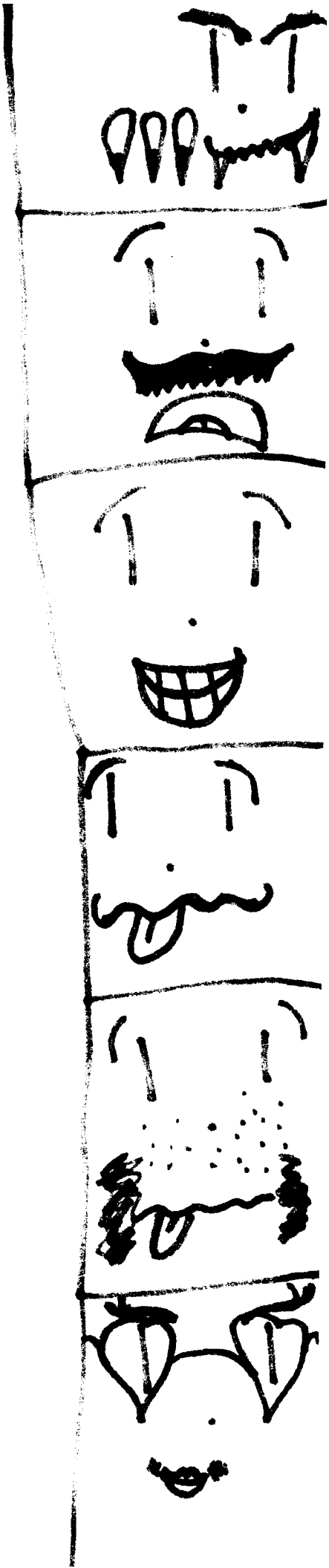
Dear Anonymous General whose name I can't say for safety reasons,

I think you should use the Vigenere square to encrypt messages for allied armys. It is secure unless the enemy finds out the key and would take only a short time for the allied general to decode, but years for the enemys. As long as the friendly armys are the only ones who know the key word, it will be too late to decode intercepted messages by the time they are received and acted upon by the receiver. I hope you will listen to my advice.

Sincerely,
Unseen Anonymous Soldier

Dear General,

I heard you are looking for a code you can use. I suggest the jefferson wheel code. With the wheel it is easy, but without it, hard. Its also kinda fun.



Student Work Samples
Encryption Techniques Performance Task

The following artifacts are reproductions of the students original products used to encrypt messages during the Risk game. The actual encryption techniques were inadvertently destroyed. A varying level of sophistication and creativity is evident in the techniques that the students used. In two of the encryption techniques the students considered word and letter frequency analysis and all three of them included elements of substitution, transposition. In addition, each of the products includes elements suggesting the students understand that patterning becomes more intuitively difficult as numbers or symbols are used instead of letters. Unfortunately, the Red Team did not consider binary code as an easily recognizable pattern of numbers!

The Green Team Encryption Technique

Groups of four letters are written. Only one letter in each group is included in the encrypted message thereby eliminating letter and word frequency. The first letter of the first group is a part of the message, the second letter of the second group is a part of the message, the third letter of the third group is a part of the message and the fourth letter of the fourth group is a part of the message. The pattern then repeats.

For example, to encode ATTACK AT DAWN one would write

AHEV ST**T**KDV MA**T**C HGG**A** **C**PZE H**K**DP MN**A**E ERU**T** **D**BWQ F**A**IK GX**W**N XVI**N**

According to the students, the strength of this encoding technique is that it is simple to remember, uses no written device or key that could be physically intercept by an 'enemy' and obfuscates letter and word frequency. In practice, the students found it effective, but wordy. The technique did not account for an available time period. The red team broke it during game play, so even without the benefit of letter and word frequency analysis, patterns were observable to the other teams.

The Blue Team Encryption Technique

The Blue team modified a St. Cyr Cipher strip to encode their messages. They would encode in numbers, the first number being the offset to use for the remainder of the message. This method observes substitution and transposition techniques as well as a recognizable time period, but did not obscure letter and word frequency. The students concluded that frequent changes in the offset of the code would obscure letter frequency. The competitors did not break it.

For example to encode ATTACK AT DAWN they would write

6,6,25,25,6,8,16,6,25,9,6,2,19

The leading character 6 tells us to assign an offset value of 6 to the A in the alphabet and then decode the remainder of the numbers using the following offset.

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

The Red Team Encryption Technique

The red team chose to use binary symbols for their encryption technique. Their product was a paper tool that they used to encrypt and decrypt. While it observed both transposition and substitution techniques, it did not account for available time period or letter and word frequency pattern recognition. Due to the fact that it used only zeroes and ones, the opposing teams assumed a binary code and broke it quickly.

To Encode ATTACK AT DAWN one would write (choosing from the rightmost two columns):

10110 01111 01111 10110 11000 00110 10110 01111 11001 10110 10010 01001

Original Letter	Position in Alphabet	Binary Conversion	Offset
A	1	00001	F
B	2	00010	G
C	3	00011	H
D	4	00100	I
E	5	00101	J
F	6	00110	K
G	7	00111	L
H	8	01000	M
I	9	01001	N
J	10	01010	O
K	11	01011	P
L	12	01100	Q
M	13	01101	R
N	14	01110	S
O	15	01111	T
P	16	10000	U
Q	17	10001	V
R	18	10010	W
S	19	10011	X
T	20	10100	Y
U	21	10101	Z
V	22	10110	A
W	23	10111	B
X	24	11000	C
Y	25	11001	D
Z	26	11010	E

Spark Camp

Encryption

Day 1

TEACHER NAME			Lesson #
Van Vickle			1
MODEL	**CONTENT AREA**	**GRADE LEVEL**	
Taba Concept Development	Math	5,6,7	

CONCEPTUAL LENS	LESSON TOPIC
Patterns	Encryption

LEARNING OBJECTIVES *(from State/Local Curriculum)*

8.F.1 Understand that a function is a rule that assigns exactly one output for a given input

THE ESSENTIAL UNDERSTANDING *(What is the overarching idea students will understand as a result of this lesson?*	THE ESSENTIAL QUESTION *(What question will be asked to lead students to "uncover" the Essential Understanding)*
Patterns Inform Prediction	How do patterns inform prediction?

CONTENT KNOWLEDGE (What factual information will students learn in this lesson?)	PROCESS SKILLS (What will students be able to do as a result of this lesson?)
• Patterns are used in encryption both in obscuring the message and in decoding the message. • Varying patterns in encryption have been used for centuries. • Encryption is used to obfuscate patterns to those whom we do not want to understand the message. • We build meaning and understanding when we uncover patterns. • Building meaning from seeing patterns allows us to make predictions and therefore take action.	• Analyze encrypted messages to identify patterns (pre lesson activity). • Create encryption functions using patterns to code and decode messages (Post lesson activity).

GUIDING QUESTIONS

What questions will be asked to support instruction?

Include both "lesson plan level" questions as well as questions designed to guide students to the essential understanding

Pre-Lesson Questions:	During Lesson Questions:	Post Lesson Questions:
• What patterns did you notice in the messages on the strange metal? • What strategies did you use to find patterns in an encrypted message? • What are some of the common characteristics the patterns? • What happens once we see a pattern? • What predictions can we make about these messages and their authors?	• What patterns have been used in encryption historically? • What patterns are used in encryption currently? • What issues arise when we create patterns? • What similarities and differences are there in the patterns you have identified? • What similarities exist that cause you to group the patterns in a particular way? • How can we describe our groups of patterns? • Do some groups seem to fit within others? • What differences in interpretation might exist that cause you to want to group them in a different manner?	• How have patterns in encryption patterns changed or stayed the same through history? • What are the patterning characteristics that make an encrypted message easy to crack? • What are the patterning characteristics that make an encrypted message hard to crack? • How does observing patterns in a message inform your ability to predict?

DIFFERENTIATION

(Describe how the planned learning experience has been modified to meet the needs of gifted learners. Note: Modifications may be in one or more of the areas below. Only provide details for the area(s) that have been differentiated for this lesson.

Content	Process	Product	Learning Environment
Functions are 8th grade and high school math content. This lesson allows students to begin thinking about the concept of a function (and using linear functions) before they encounter the abstraction of a linear function.	• Students must use critical thinking to create a cipher that embodies the characteristics they have identified as good encryption. • Students must demonstrate flexibility of thinking to work "forward" and "backward" in coding and decoding. • Students must evaluate the efficacy of certain encryption techniques.	Students "ciphers" will have varying levels of sophistication and will allow more advanced students to work at a higher mathematical level.	Collaborative learning environment encompassing both group work and whole group discussion.

PLANNED LEARNING EXPERIENCES

(What will the teacher input? What will the students be asked to do? For clarity, please provide detailed instructions)

Engage and Connect - *This phase focuses on piquing students' interest and helping them access prior knowledge. This is the introduction to the lesson that motivates or hooks the students.*

As students enter the room they are grouped and given messages written on a strange metallic material. They are asked to decode the message by observing patterns in the messages and then make predictions about how we should respond to the authors of the messages. (20 minutes)

As students finish their group work, we come together as a whole group to answer the questions about the messages and debrief on the process used to identify the patterns in the messages. Together, we identify different strategies that the students used to determine the message that authors left, emphasizing that each strategy involved identifying a particular pattern that was initially hidden but became evident. For example, could they identify the letter A or I as stand-alone letters or pattern associations based on letter frequency? The teacher should allow the students to articulate these patterns using their own observations and words. Conversation in whole group includes the discussion of the pre-lesson questions. (10 minutes)

Explore - *In this phase, the students have experiences with the concepts and ideas of the lesson. Students are encouraged to work together without direct instruction from the teacher. The teacher acts as a facilitator. Students observe, question, and investigate the concepts to develop fundamental awareness of the nature of the materials and ideas.*

LISTING

Students will read articles regarding encryption techniques. As students read, they will be instructed to look for the vocabulary of patterns and write down any words or ideas that they see that relate to patterns. They will be told that we will be using these words in a whole class activity. Note: Students may chose to read these articles aloud to each other or silently to themselves. They should however, make their initial list of words independently. Once they have their individual lists, they will consolidate them as a group and write each unique word on a sticky note. (30 minutes for reading and playing with the cipher techniques and 5 minutes for consolidation and writing on sticky notes.)

Article:
http://www.exploratorium.edu/ronh/secret/secret.html

Students will share lists to the whole group as the teacher makes a comprehensive list on the board. During lesson questions can be used here and in the Grouping and Labeling phase as needed. (5 minutes)

Explain - *Students communicate what they have learned so far and figure out what it means. This phase also provides an opportunity for teachers to directly introduce a concept, process, or skill to guide students toward a deeper understanding.*

GROUPING AND LABELING

1. Students will be given several pieces of different colored card stock and will consolidate their lists based on similarities (with their assigned group of approximately four students) by placing each sticky note on a different color card stock. Groups of students will work together to decide which items in the comprehensive list go together because they are alike in some aspect of the concept of patterns and place those items (sticky notes) on a card stock. Students will be provided with the following rules: At least three different groups (card stock), at least three items (sticky notes) on each card stock, items may not be used twice. The teacher will move throughout the classroom checking in with student groups. The teacher will guide students as necessary with questions but will allow the student groups to come to their own conclusions. As students finish, the teacher will instruct students to label the newly defined groups by writing a title on the card stock. (10-15 minutes)
2. Students will present their groups and explain their reasoning for the groupings and title to the class. The teacher will ask students to describe the similarities and differences among groups. (15 minutes)

Elaborate —*Allow students to use their new knowledge and continue to explore its implications. At this stage students expand on the concepts*

they have learned, make connections to other related concepts, and apply their understandings to the world around them in new ways

SUBSUMING, REGROUPING, RENAMING

1. Student groups will be challenged to regroup items. They will be given new card stock (three new colors) and asked to rearrange their sticky notes on the new colors of card stock. The new groups must be new categories. Rules for regrouping include: items can be used again, categories must be new, and each category needs at least four items. The teacher will remind the students that categories must be based on some aspect of patterns in encryption. (10 minutes)
2. The teacher will facilitate as all groups to share their categories. (10 minutes)

Evaluate: *This phase assesses both learning and teaching and can use a wide variety of informal and formal assessment strategies.*

The teacher will wrap up the lesson by asking the class to explain what they have learned about patterns and the relationship between different patterns and encryption. Post lesson questions will be used in this discussion. (10 minutes)

Students will then be asked (in their groups) to decide upon a message to send back to the authors of the metallic messages. They will create an encoded message using the pattern of encryption they have observed the authors of the message using. (15 minutes).

Once encoded, they share their messages with the whole class and allow us to decipher their encrypted replies. Group discussion during this part of the lesson focuses on whole group recognizing the patterns of encryption used by the group. Post lesson questions will be used in this discussion. (15 minutes).

The remainder of the session will be spent introducing and working on their encryption Performance Task

Encryption Performance Task

G	On the last day of class you will be participating in a role-playing game in which you, along with your allies, will be working to establish world dominance over forty-two territories on six continents. When you play this game, you will be working in teams – some of the teams will be your allies and others will be your opponents. You will need a secure way to communicate with your allies and obscure your messages from your opponents.
R	Your job is that of encryption specialist. You must devise the process or tool through which you will encrypt your messages to your allies. You must try to make your method of encryption secure without making it so complex that your allies have trouble deciphering the messages.
A	Your encryption device will be evaluated by how well it enables you to communicate with your allies and, at the same time, keeps your messages safe from decryption from your opponents. You can assume that the enemy will intercept all of your messages.
S	Keep in mind, this method may or may not use a tool (like the Caesar Cipher or Scytale) but it will be used in a fast-paced game and as a result should be engineered for such.
P	You should either produce your tool from the materials in the classroom, which include cardstock, paper, markers, brads etc., or you should write the rules of encryption down completely so that individuals with no experience in encryption could follow them.
S	To determine if you are successful, make sure to use your method of encryption to encode several messages and have your teammates decipher them. This will help you gauge the security of your encryption technique and will also give you feedback on whether it is too complicated for fast-paced game play.

Spark Camp

Encryption

Day 2

TEACHER NAME		Lesson #
Van Vickle		2
MODEL	**CONTENT AREA**	**GRADE LEVEL**
Creative Problem Solving	Math	5,6,7

CONCEPTUAL LENS	LESSON TOPIC
Patterns Inform Prediction	Encryption

LEARNING OBJECTIVES *(from State/Local Curriculum)*

8.F.1 Understand that a function is a rule that assigns exactly one output for a given input

THE ESSENTIAL UNDERSTANDING *(What is the overarching idea students will understand as a result of this lesson?*	THE ESSENTIAL QUESTION *(What question will be asked to lead students to "uncover" the Essential Understanding)*
Patterns Inform Prediction	How do patterns inform prediction?

CONTENT KNOWLEDGE (What factual information will students learn in this lesson?)	PROCESS SKILLS (What will students be able to do as a result of this lesson?)
• Patterns are used in encryption both in obscuring the message and in decoding the message. • Varying patterns in encryption have been used for centuries. • Encryption is used to obfuscate patterns to those whom we do not want to understand the message. • We build meaning and understanding when we uncover patterns. • Building meaning from seeing patterns allows us to make predictions and therefore take action. • Know a basic definition of a function • Understand and use vocabulary associated with functions and encryption such as plain text, encrypt, cipher, decipher.	• Evaluate methods of encryption • Create encryption functions to code and decode messages. • Advocate for a method of encryption based on its attributes.

GUIDING QUESTIONS

What questions will be asked to support instruction?

Include both "lesson plan level" questions as well as questions designed to guide students to the essential understanding

Pre-Lesson Questions:	During Lesson Questions:	Post Lesson Questions:
• What types of patterns did we see in our messages yesterday? • How did those patterns obfuscate the message? • What characteristics of those patterns made the messages easier or harder to decipher? • What are the challenges we encounter when we create patterns of encryption? • What types of patterns did we see in the movie clips? • How are the challenges of encryption different today than they were historically? • How did the patterns of the enigma machine differ from the patterns on the metallic substance? • Do you believe the patterns from the enigma machine would be difficult to "crack" now? • What challenges might future encryption experts face?	• What patterns of the Caesar Cipher make it desirable/undesirable when we want to hide messages? • What patterns of the Caesar Cipher make it desirable/undesirable when we want to read the hidden messages? • In what way could the Caesar Cipher be considered a function? • In what ways could we expand upon the Caesar Cipher patterning to make it fit the characteristics we have identified as desirable?	• Of the group ciphers methods, what were the patterns that helped you crack the code? • Of the group ciphers, what were the patterns that made it harder to crack the code? • Describe any "aha" moments you might have had when trying to crack the code. • How are the purposes of our decryption efforts today different from our decryption efforts in yesterday's alien adventure? • What were we able to predict when the patterns were exposed in the alien adventure? The codes from our exercise today? The enigma machine? • What personality characteristics do you believe would be good for a code breaker to have?

DIFFERENTIATION

(Describe how the planned learning experience has been modified to meet the needs of gifted learners. Note: Modifications may be in one or more of the areas below. Only provide details for the area(s) that have been differentiated for this lesson.

Content	Process	Product	Learning Environment
Functions are 8th grade and high school math content. This lesson allows students to begin thinking about the concept of a function (and using linear functions) before they encounter the abstraction of a linear function.	• Students must use critical thinking to create a cipher that embodies the characteristics they have identified as good encryption. • Students must demonstrate flexibility of thinking to work "forward" and "backward" in coding and decoding. • Students must evaluate the efficacy of certain encryption techniques.	Students "ciphers" will have varying levels of sophistication and will allow more advanced students to work at a higher mathematical level.	Collaborative learning environment based on problem solving.

PLANNED LEARNING EXPERIENCES

(What will the teacher input? What will the students be asked to do? For clarity, please provide detailed instructions)

Engage and Connect - *This phase focuses on piquing students' interest and helping them access prior knowledge. This is the introduction to the lesson that motivates or hooks the students.*

As students enter the room there is a picture of the enigma machine projected on the board with the questions, "What is this machine? What is its use? What are the different parts? What do they do?" (10 minutes)

https://upload.wikimedia.org/wikipedia/commons/b/bd/Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

Once students are assembled, we watch the trailer to The Imitation Game.

https://www.youtube.com/watch?v=S5CjKEFb-sM

And an excerpt from A Beautiful Mind

https://www.youtube.com/watch?v=ttU2fPxJ5sQ

The teacher facilitates pre lesson questions designed to prompt a discussion of the patterns in encryption as a method of both obfuscating the content of messages and of giving hints to the meaning of the message. We review the patterns we observed in yesterday's activity and the predictions we were able to make as a result of our pattern detection. Pre Lesson Questions are designed to encourage divergent thinking. (Stage 1 CPS) (20 minutes)

Direct instruction on vocabulary and functions is presented here: (10 minutes)

- Plain Text
- Cipher Text
- Cipher (noun and verb)
- Decipher
- Encrypt
- Decrypt
- Code
- Encode
- Algorithm
- Key
- Obfuscate
- Function (the function machine)

Explore - *In this phase, the students have experiences with the concepts and ideas of the lesson. Students are encouraged to work together without direct instruction from the teacher. The teacher acts as a facilitator. Students observe, question, and investigate the concepts to develop fundamental awareness of the nature of the materials and ideas.*

- In their groups, students will make a St. Cyr Cipher Strip from card stock/paper and use it to encrypt and decrypt a message to each other. (20 minutes) The template for the cipher strip is here:
-

http://www.cleavebooks.co.uk/trol/trolc04.pdf

- After using the St. Cyr Cipher Strip, the groups will analyze the benefits and shortcomings of the patterns formed by this encryption technique by making a Pro/Con list on a sheet of paper with a line down the middle. (Stage 2 CPS) (10 minutes)

Explain - *Students communicate what they have learned so far and figure out what it means. This phase also provides an opportunity for teachers to directly introduce a concept, process, or skill to guide students toward a deeper understanding.*

- Teacher will facilitate whole group discussion centered on the Pro/Con sheet. Pro/Con list will be written on the board and students will summarize the groups' analysis into one or two bullet points (convergent thinking) that might be requirements for improvement of the Caesar Cipher. (5 minutes)
- During lesson questions will lead students to the understanding that this type of encryption is a simple function that produce encrypted messages that have patterns that are easy to decipher. Students should come to the conclusion that a requirement of the more sophisticated encoding device would be that it would not produce a pattern that is a function. (Stage 3 CPS) (20 minutes)

Elaborate —*Allow students to use their new knowledge and continue to explore its implications. At this stage students expand on the concepts they have learned, make connections to other related concepts, and apply their understandings to the world around them in new ways*

- Teacher will facilitate whole group "brainstorming" for a more secure method of encryption in an effort to encourage divergent thinking. (Stage 4 CPS) (15 minutes)
- The class will have time for student groups to work on their product (convergent thinking) tweaking it so that it is more difficult to crack than the St Cyr Cipher. They should practice using this method encode a message. If time allows they should exchange their message with another group to see of it can be "cracked." Materials such as cardstock, markers, glue etc. should be provided. They should name their encryption method. (This is the evolution of their product) (Stage 5 CPS) (45 minutes)

Evaluate: *This phase assesses both learning and teaching and can use a wide variety of informal and formal assessment strategies.*

- Teacher will facilitate post lesson discussion centered on evaluating the methods proposed and addressing post lesson questions. Discussion will utilize post lesson questions and focus on how we changed the patterns of the Caesar Cipher so that it was more secure and the differences in the patterns formed in yesterday's alien adventure, the Caesar Cipher and the Enigma Machine. (Stage 6 CPS) (10 minutes)

Spark Camp

Encryption

Day 3

TEACHER NAME		Lesson #
Van Vickle		3
MODEL	**CONTENT AREA**	**GRADE LEVEL**
Questioning	Math	5,6,7

CONCEPTUAL LENS	LESSON TOPIC
Patterns Inform Prediction	Encryption

LEARNING OBJECTIVES *(from State/Local Curriculum)*

8.F.1 Understand that a function is a rule that assigns exactly one output for a given input.

THE ESSENTIAL UNDERSTANDING *(What is the overarching idea students will understand as a result of this lesson?*	THE ESSENTIAL QUESTION *(What question will be asked to lead students to "uncover" the Essential Understanding)*
Patterns Inform Prediction	How do Patterns Inform Prediction?

CONTENT KNOWLEDGE (What factual information will students learn in this lesson?)	PROCESS SKILLS (What will students be able to do as a result of this lesson?)
• Encryption has been used for many purposes. • Encryption can be used to obfuscate patterns. • We build meaning when we uncover patterns. • Meaning allows us to make predictions and therefore take action	• Evaluate methods of encryption by analyzing the sophistication of the patterns the method creates. • Advocate for a method of encryption by discussing the patterns the method creates.

GUIDING QUESTIONS

What questions will be asked to support instruction?

Include both "lesson plan level" questions as well as questions designed to guide students to the essential understanding

Pre-Lesson Questions:	During Lesson Questions:	Post Lesson Questions:
• What patterns have we observed in our study of encryption so far? • In what ways can these patterns be grouped? • What are the characteristics of a pattern that is "easy" to crack? • What are the characteristics of a pattern that is "difficult" to crack?	• What patterns do we see if we have a function? • What patterns did you observe about any of the machines that would cause you to believe they represent a function? • How do these patterns affect our ability to make predictions? • When choosing an encoding device, what types of patterns would be desirable? Undesirable? • How do these characteristics fit with your understanding of a function?	• When you write the letter, what information about patterns does your "commander" want to know? • What benefits do these patterns give us in the use of the machine you chose? • What will the patterns do if your enemy should intercept a message? • How did the patterns you observed help you make a prediction and thus choose an encryption tool?

DIFFERENTIATION

(Describe how the planned learning experience has been modified to meet the needs of gifted learners. Note: Modifications may be in one or more of the areas below. Only provide details for the area(s) that have been differentiated for this lesson.

Content	Process	Product	Learning Environment
Functions are 8th grade and high school math content. This lesson	Students must use critical thinking to observe the patterns created by each	Students must produce written work at a developmentally	Collaborative learning environment.

allows students to begin thinking about the concept of a function (and use linear functions) before they encounter the abstraction of a linear function.	cipher wheel and identify and evaluate the patterns that cause a message to be obscure.	appropriate level.	

PLANNED LEARNING EXPERIENCES

(What will the teacher input? What will the students be asked to do? For clarity, please provide detailed instructions)

Engage and Connect - *This phase focuses on piquing students' interest and helping them access prior knowledge. This is the introduction to the lesson that motivates or hooks the students.*

As students enter the room images of many historic encoding machines are flashing on the screen along with background music to the slide show.

Once the class is assembled the teacher shows a picture of the Alberti Cipher Disk and asks, "How could we evaluate this tool for encoding messages and make a decision if we should use it?"

https://en.wikipedia.org/wiki/Alberti_cipher_disk#/media/File:Alberti_cipher_disk.JPG

Students' responses are recorded on the board and Pre-lesson questions guide the discussion.

To wrap up the conversation, we make a list on the board of the patterns that obscure/inform messages. (15 minutes)

Explore - *In this phase, the students have experiences with the concepts and ideas of the lesson. Students are encouraged to work together without direct instruction from the teacher. The teacher acts as a facilitator. Students observe, question, and investigate the concepts to develop fundamental awareness of the nature of the materials and ideas.*

Role Play: Students are divided into 4-5 groups and given the following scenario, "Imagine we are at war and have to send messages great distances on horseback to our troops. We have to cross enemy lines, so we need the messages to be encoded so the enemy cannot read them. We can choose any of the five devices here, but we must make an intelligent decision on which one to select."

Each group begins at one of the stations of encoding Methods: Confederate Army Cipher Disk, Union Army Cipher Disk, Scytale, Jefferson Wheel, Vignere Square, Musical Encryption and Affine Cipher. Each station has the encoding machine and instructions. The groups will have 5-7 minutes to examine the encoding machine and evaluate it for its sophistication of encoding (pattern obfuscation) based on the pre-lesson criteria we established. Students rotate through the seven stations so that each group has the opportunity to observe and manipulate all of the tools. (50 minutes)

Explain - *Students communicate what they have learned so far and figure out what it means. This phase also provides an opportunity for teachers to directly introduce a concept, process, or skill to guide students toward a deeper understanding.*

Giant Post-It notes are placed on the walls-one for each machine. Student groups have 3 minutes at each post-it note to record the patterns they notice with each coding machine. (20 minutes)

Direct instruction on the definition of a function is given (or reviewed from the day before) here. For our purposes, a function is any operation for which there is a unique output given an input. The teacher will draw the "function machine" on the board and we practice "dropping" input values in and getting "output" values and determining if the "machine" is a function. (15 minutes)

Elaborate —*Allow students to use their new knowledge and continue to explore its implications. At this stage students expand on the concepts they have learned, make connections to other related concepts, and apply their understandings to the world around them in new ways*

With the post-it notes filled out, whole group discussion centers on the During Lesson Questions. Connections are made between patterning and functions as the students classify the machines as functions and not functions and evaluate which patterns create more obfuscation. (20 minutes)

Evaluate: *This phase assesses both learning and teaching and can use a wide variety of informal and formal assessment strategies.*

In their role-play persona, students are asked to write a letter of recommendation to their "commander" defending their choice of one of the encoding devices. Before writing the letter, we discuss the post lesson

questions and they are written on the board so students are reminded of the elements they should include in their letter, particularly the discussion of how patterns informed their predictions and ultimately their choice in encryption devices. (15 minutes)

When they complete their letter, they are given time to work on their product, the encoding device that they will use to play the game on day 4. (20 minutes).

Confederate Army Cipher Disk

Align the inner wheel letter A (plain text) with an outer wheel (cipher text) letter. To encode your message find the plain text letter on the inner wheel and substitute the outer wheel letter that it is pointing to.

For example, align the inner wheel A with the outer wheel D (the standard Caesar Cipher offset.) Now to encode the words HELLO WORLD, find the letter H on the inner wheel (plain text) and use a K (cipher text). For the letter E, substitute H and so forth. My cipher text for HELLO WORLD would read KHOOR ZRUOG.

Now you try encoding HELLO WORLD using a different alignment of letter A (plain text) with the outer wheel (cipher text) letter.

Jefferson Wheel

Using a single row for the wheel, spell your message. For example I aligned the wheel to spell ATTACKATDAWN. Now I can use any of the rows on the wheel to encode. If I use the one just below the message, my cipher would be "oKHEZW6KWEBI". I could send this message to my allies and they could arrange a row to read "oKHEZW6KWEBI" and then read the line above it – But – they would have to have a Jefferson wheel with the same cylinders on it!

See if you can create a cipher text for OCCUPY THE NORTHERN TERRITORIES.

Union Army Cipher Disk

The Union Army Cipher Disk was used with flag signaling during the American Civil war. The numbers 1 and 8 were associated with different movements of a flag and thus a signalman could stand in the open and move the flag without revealing the message to the enemy. The standard placement indicated the flag signal that was associated with the letter R. For example, if R and 1881 are matched up, the code for UNION ARMY becomes 8111, 8888, 81, 888, 8888, 111, 1881, 181, 8118.

The characters ing, tion and & were often used to abbreviate or in some cases to indicate the end of a word. In the UNION ARMY example, we might insert an & to read UNION&ARMY and encode it as 8111, 8888, 81, 888, 8888, 8181, 111, 1881, 181, 8118.

Scytale (Skit – a- lee)

In the 5th Century BC, Spartan Generals wrapped ribbons of paper around a cylinder of a known diameter and wrote their messages. When the paper was unwound, the writing made no sense, but it could be easily deciphered if rewound. I have encoded a message on this piece of paper. Can you figure out which dowel rod should be used to decipher it?

Use one of the dowel rods to encode "WE SHOULD OCCUPY KAMCHATKA"

Vigenere Square

Blasé De Vigenere invented this square for encoding messages. (Notice the alphabet is offset one position for each column to the right/row down.)

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

The table requires a keyword to encrypt. For example, if we wish to send the message HELLO WORLD using the keyword LAMPSHADE we would find the L in lampshade on the top of the table, and the H for hello world on the side of the table and find that they intersect at an S so the first letter of our encrypted message would be S. To find the second letter we would use the A in lampshade on the top of the table and the E in hello world on the side and find the intersection in the table. We would use the letter E for this position. When completely encrypted, HELLO WORLD would be SEXAGDOUPO. Sometimes it is easier to see if they are written on top of one another. If the key is not long enough, we just repeat it.

L	A	M	P	S	H	A	D	E	L
H	E	L	L	O	W	O	R	L	D
S	E	X	A	G	D	O	U	P	O

Musical Encryption

It is possible to associate letters of the alphabet with musical frequencies. (Have you seen Close Encounters of the Third Kind? G, A, F, F, C ?) In this way, we can sing melodies to each other that have a hidden meaning or maybe send them as pieces of sheet music. Use the piano Keyboard and my letter associations to encode HELLO WORLD and ATTACKATDAWN.

Affine Cipher

A shift cipher, like the Caesar Cipher uses simple addition to move the letters, but an Affine Cipher uses both multiplication and addition to achieve the encoded text. For example I could take the letters of the alphabet and give them a numeric association like this:

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Then, using both multiplication and addition I could take the message HELLO WORLD and change it to 8, 5, 12, 12, 15, 23, 15, 18, 12, 4. Then I would multiply each number by 2 for 16, 10, 24, 24, 30, 46, 30, 36, 24, 8. And finally, I would add six to arrive at 22, 16, 30, 30, 36, 52, 36, 42, 30, 14. We could represent this as an equation that looks like

$$CT = 2PT + 6$$

To decode my message, I would have to undo the arithmetic in the opposite order by first subtracting 6 and then dividing by 2. We can represent this in an equation that looks like

$$PT = \frac{CT - 6}{2}$$

Spark Camp

Encryption

Day 4

TEACHER NAME			Lesson #
Van Vickle			4
MODEL	**CONTENT AREA**	**GRADE LEVEL**	
Simulation	Math	5,6,7	

CONCEPTUAL LENS	LESSON TOPIC
Patterns Inform Prediction	Encryption

LEARNING OBJECTIVES *(from State/Local Curriculum)*

8.F.1 Understand that a function is a rule that assigns exactly one output for a given input

THE ESSENTIAL UNDERSTANDING *(What is the overarching idea students will understand as a result of this lesson?*	**THE ESSENTIAL QUESTION** *(What question will be asked to lead students to "uncover" the Essential Understanding)*
Patterns Inform Prediction	How do patterns inform prediction?
CONTENT KNOWLEDGE (What factual information will students learn in this lesson?)	**PROCESS SKILLS** (What will students be able to do as a result of this lesson?)
• Encryption has been used during wartime to send messages of strategy. • Encryption can be used to obfuscate patterns. • We build meaning when we uncover patterns. • Meaning allows us to make predictions and therefore take/change course of action.	• Evaluate methods of encryption • Create encryption functions to code and decode messages. • Judge the weaknesses in a method of encryption and make modifications to improve it.

GUIDING QUESTIONS

What questions will be asked to support instruction?

Include both "lesson plan level" questions as well as questions designed to guide students to the essential understanding

Pre-Lesson Questions:	During Lesson Questions:	Post Lesson Questions:
• Why do we encode messages, in times of war, in peace-time? • What types of information might be in these encoded messages? • How does the recognition of patterns give us an edge in war, in peace-time? • How are the challenges of encryption different today than they were historically?	• What patterns do you notice in the enemy's messages? • What patterns in your messages are informing your enemy? • What conclusions can you draw from observing these patterns? • How does seeing this pattern inform your game play? • How does seeing this pattern inform your enemy's game play? • What alternative outcomes could come out of these patterns? • How could messages confuse?	• What patterns did you observe in the "enemy's" encoded messages? • How do these patterns hide the meaning of the message? • How do these patterns make the message readable? • What patterns in game play told you the "enemy" had decoded your messages? • What changes in patterns did you make in response to these observations? • What would you change about the patterns in your encoding technique?

DIFFERENTIATION

(Describe how the planned learning experience has been modified to meet the needs of gifted learners. Note: Modifications may be in one or more of the areas below. Only provide details for the area(s) that have been differentiated for this lesson.

Content	Process	Product	Learning Environment
• Functions are 8th grade and high school math content. This lesson allows students to begin thinking about the concept of a function (and using linear functions) before they encounter the abstraction of a linear function.	• Students must use critical thinking to create a cipher that they believe the "enemy" cannot read. • Students must demonstrate flexibility of thinking to work "forward" and "backward" in coding and decoding. • Students must evaluate the efficacy of certain encryption techniques.	• Students encoding methods will have varying levels of sophistication and will allow more advanced students to work at a higher mathematical level. • Students' game play will take on varying levels of sophistication.	• Collaborative learning environment based on problem solving.

PLANNED LEARNING EXPERIENCES

(What will the teacher input? What will the students be asked to do? For clarity, please provide detailed instructions)

Engage and Connect - *This phase focuses on piquing students' interest and helping them access prior knowledge. This is the introduction to the lesson that motivates or hooks the students.*

Preparatory to the simulation:

- In this simulation, students will be using encryption techniques within the context of playing the game Risk (or depending on interest, Star Wars Risk.) In order to participate in the simulation, it is necessary for the students to have some familiarity with the rules of Risk, so for the first 20 minutes of class, students will explore the game board and the MODIFIED rules of the game.
- As students enter the room, the Risk rules are projected on the white board and several tables have risk games opened up.
- Students are directed to tables and asked to work together to learn the rules. Students who have experience playing the game are paired with those who have not to facilitate basic understanding of the game rules. They are encouraged to step through the beginning of a practice game.
- After the students have worked for approximately 20 minutes, whole group instruction focuses on debriefing and making sure students understand the game play.
- Once the students have learned the rules, the layer of encryption is added. The teacher may or may not regroup the students for the simulation.

Setting the Scene for the Simulation

- One Risk board is placed in the center of the room with student groups on four sides. If necessary, a document camera is placed over the Risk game board so that everyone can see the game as it is played.
- Students are told that there are two "teams" trying to take over the world. Together, groups 1 and 3 (sitting opposite the game board) form one "team" and groups 2 and 4 (sitting opposite the board) form the other.
- Individuals within a group may talk with one another, but to communicate with the other group in their team they must send a message. That message must be encrypted because we must assume that it will be intercepted. The teacher computer will be used to display the encrypted messages on a second white board.
- Each "team" is given 10 minutes to collaborate on a name for their side and decide upon an encryption tool that they will use to send messages during the game. They should not discuss game strategy during this meeting.
- Once a name and encryption technique is chosen, they are asked to take up their game playing positions.
- The groups begin the game. Each turn requires that they send a message to their teammates across the board regarding their strategy for their moves. They first take a turn and send a message.
- These messages are "intercepted" by the teacher and displayed in encrypted form on the second white board using the teacher computer.

Explore - *In this phase, the students have experiences with the concepts and ideas of the lesson. Students are encouraged to work together without direct instruction from the teacher. The teacher acts as a facilitator. Students observe, question, and investigate the concepts to develop fundamental awareness of the nature of the materials and ideas.*

- Students take turns playing the Risk game while encrypting and decoding messages. Teacher facilitates, helping groups who get stuck and asking during lesson questions designed to help students push the level of critical thinking in terms of observations of patterns.
- Game play may take on varying levels of complexity. Some teams may simply focus on understanding the messages sent to them from the other group in their team. Other teams may decide to decode the enemy's message. Particularly sophisticated groups may decide to send messages to confuse their enemy.

- Groups may devise roles for the team members, such as decoder, encoder, strategist etc. If these roles limit play by any one individual, the teacher should redirect.
- Depending on how the game progresses, students may be allowed to have team meetings periodically throughout the game (after the game board has been established) to discuss encryption techniques (but not strategy.) (90 minutes)

Explain - *Students communicate what they have learned so far and figure out what it means. This phase also provides an opportunity for teachers to directly introduce a concept, process, or skill to guide students toward a deeper understanding.*

- Once game play is finished, the teams will be asked to meet and answer post lesson questions (during game encoded messages are still on the board for reference.)

- Teacher will facilitate whole group discussion centering on the post lesson questions.

Elaborate —*Allow students to use their new knowledge and continue to explore its implications. At this stage students expand on the concepts they have learned, make connections to other related concepts, and apply their understandings to the world around them in new ways*

- Each group will fill out the following table and share it with the whole class. (15 minutes)

	Our Messages	Enemy Messages
Patterns that made them easy to read		
Patterns that made them harder to read		

Evaluate: *This phase assesses both learning and teaching and can use a wide variety of informal and formal assessment strategies.*

- Working individually, students will write in response to the prompt, "How did you use patterns and prediction to inform changes to your encryption techniques?" "After having played the game, how would you change your encryption techniques and why?" (20 minutes)
- During this phase each group is encouraged to share their encryption device and explain the design decisions they made as the week progressed. (Product)

MODIFIED RISK RULES

PHASE ONE: In this phase, the armies occupying each territory are established. Each player takes a turn rolling one die.

- The player must place the number of armies on the boards as represented on the face of the die. For example, if player 1 rolls a 3, she must place 3 of her armies on the board.
- Each territory should have one occupying army on it before armies can be doubled or tripled on a territory.
- Once a territory is occupied by and army, no other armies can occupy it.
- A maximum of 5 armies can be placed on any one territory
- For a three-player game, each player begins with 30 armies. For four or more players, each player shall begin with 25 armies.

PHASE TWO: The Battle

- The first player will decide where to attack. Only one army may attack at a time and there must be at least two armies on a territory for an offensive attack – this way, if the attacker looses, an occupying army will remain on the territory. To attack, the attacker rolls a die and the defender rolls a die. The highest die wins and the looser removes one army and places it in the box lid.
- If the attacking player wins, he may choose to attack again or rearrange his armies and pass the play on to the next player.
- Once an attacking player looses, she may choose to rearrange her armies or pass play on to the next player.
- When rearranging armies, a player may only move armies to contiguous territories and all territories must be left with at least one occupying army.
- A player may not rearrange his armies at the beginning of his turn (before the attack.)
- Play rotates counter clockwise after the each player has lost an attack and had an opportunity to rearrange his armies.

List of Helpful Resources

Hipshman, R. (1995). Secret language: Cryptography & Secret Codes. Exploratorium. Retrieved from http://www.exploratorium.edu/ronh/secret/secret.html

This is the reading resource given to the students on the first day for their TABA exercise. It introduces many of the encryption concepts such as transposition and substitution ciphers as well as the idea of pattern recognition using letter and word frequency.

Janeczko, P.B. (2004). Top secret: A handbook of codes, ciphers, and secret writing. York, PA: Candlewick Press.

This book is a general resource for basic encryption techniques (not computer encryption techniques) and information on the history of encryption. It is age appropriate for middle school students and contains a list of additional resources on page 129.

Lecture Notes, Cryptography and Modular Codes. Retrieved from http://www.willamette.edu/~emcnicho/courses/Contemporary/Handouts/Cryptography.htm

This is a resource that explains how to use linear functions to encode and decode. It uses function notation and inverse function notation to describe the process of encoding and decoding. Used as a resource for the activities I planned for the students, it would be appropriate for an older student as a primary resource.

Tapson, F. (2003). Cryptology: Simple cipher messages. Retrieved from http://www.cleavebooks.co.uk/trol/trolc04.pdf

This resource has templates for the St. Cyr Strip and several other Cipher wheels.

Trailer for the Imitation Game. (2014). Retrieved from https://www.youtube.com/watch?v=S5CjKEFb-sM

Used to pique interest in the enigma machine and begin a discussion of more complex methods of encryption.

Modular arithmetic: Cryptographer's Mathematics. Retrieved from http://www2.sunysuffolk.edu/fultonj/MA22/Modular%20Arithmetic%20&%20Cryptography.pdf

A good resource for modular arithmetic encryption techniques.

Bibliography

de Paiva, G. (2011). Proposal of pattern recognition as a necessary and sufficient principle to cognitive science. Retrieved from https://arxiv.org/pdf/1106.0171.pdf

Nativist theory: Chomsky and language learning. Retrieved from https://www2.vobs.at/ludescher/Ludescher/LAcquisition/Nativist/nativist%20theory.htm

Greenspan, S., & Shanker, S. (2007). The developmental pathways leading to pattern recognition, joint attention, language and cognition. *New ideas in psychology* 25(2), 128-142.

The place of functions in the high school mathematics curriculum (2016). Park City Mathematics Institute; Princeton, NJ: Retrieved from http://mathforum.org/pcmi/curriculum11.25.09.pdf

Mattson, M.P. (2014). Superior pattern processing is the essence of the evolved human brain. *Frontiers in Neuroscience,* 8: 265.

Modular arithmetic: Cryptographer's Mathematics. Retrieved from http://www2.sunysuffolk.edu/fultonj/MA22/Modular%20Arithmetic%20&%20Cryptography.pdf