CryptoClub Connections to the Common Core State Standards for Mathematics (CCSSM)

Standards for Mathematical Practices

Any rich mathematical application, such as cryptography, provides opportunities for students to develop good mathematical practices. Here are a few of the recommended Mathematical Practices from the CCSSM and how they can be practiced in CryptoClub:

1. Make sense of problems and persevere in solving them.

The problems faced in cryptography are different from what students experience in regular math class. They give students opportunities to explore new techniques and to try out their own ideas. Perseverance is often needed to crack an encrypted message.

2. Reason abstractly and quantitatively.

Arithmetic ciphers are a real-world application of modular arithmetic, which is usually taught at a higher level in an abstract mathematics course. Because students see the value of using modular arithmetic in this concrete setting, they can appreciate the value of abstraction.

3. Construct viable arguments and critique the reasoning of others.

CryptoClub is a safe place for students to solve problems, explain their solutions and compare methods and strategies.

5. Use appropriate tools strategically.

The CryptoClub student is presented with an arsenal of tools, including online applications, for cracking messages and often needs to decide which ones to apply.

Standards for Mathematical Content

Grade 4. Operations and Algebraic Thinking 4.OA

3. Solve multistep word problems posed with whole numbers and having whole-number answers using the four operations, including problems in which remainders must be interpreted. Represent these problems using equations with a letter standing for the unknown quantity. Assess the reasonableness of answers using mental computation and estimation strategies including rounding.

All of the arithmetic ciphers, additive, multiplicative and affine, require an understanding of modular arithmetic. Division with remainder is one of the main tools used to operate in Mod 26 arithmetic. Encrypting and decrypting with these ciphers encourages the use of mental computation, including estimation strategies.

Grade 5. Operations and Algebraic Thinking 5.OA

Write and interpret numerical expressions.

1. Use parentheses, brackets, or braces in numerical expressions, and evaluate expressions with these symbols.

2. Write simple expressions that record calculations with numbers, and interpret numerical expressions without evaluating them.

Students are encouraged to write expressions to show calculations and to use algebraic rules to simplify calculations.

Analyze patterns and relationships.

3. Generate two numerical patterns using two given rules. Identify apparent relationships between corresponding terms. Form ordered pairs consisting of corresponding terms from the two patterns, and graph the ordered pairs on a coordinate plane. For example, given the

rule "Add 3" and the starting number 0, and given the rule "Add 6" and the starting number 0, generate terms in the resulting sequences, and observe that the terms in one sequence are twice the corresponding terms in the other sequence. Explain informally why this is so.

In exploring patterns for multiplicative and affine ciphers, students generate these two different number patterns in mod 26.

Grade 5. Number and Operations in Base Ten **5.NBT**

5. Fluently multiply multi-digit whole numbers using the standard algorithm.

All of the arithmetic ciphers, additive, multiplicative, and affine, require strong arithmetic skills as described here. Multiplicative and affine ciphers involve arithmetic with 3-digit numbers to encrypt and decrypt and to find multiplicative inverses.

Grade 6. Ratios and Proportional Reasoning **6.RP**

Understand ratio concepts and use ratio reasoning to solve problems.

3. Use ratio and rate reasoning to solve real-world and mathematical problems

c. Find a percent of a quantity as a rate per 100.

During activities on frequency of letters, students apply and reinforce their knowledge of ratios and percents, as well as their understanding of proportional reasoning.

Grade 6. The Number System **6.NS**

Compute fluently with multi-digit numbers and find common factors and multiples.

4. Find the greatest common factor of two whole numbers less than or equal to 100 and the least common multiple of two whole numbers less than or equal to 12. Use the distributive property to express a sum of two whole numbers 1–100 with a common factor as a multiple of a sum of two whole numbers with no common factor. For example, express 36 + 8 as 4 (9 + 2).

Finding common factors is a useful way to find the length of the keyword when cracking a Vigenère cipher. Numbers factored in CryptoClub are often larger than 100.

Apply and extend previous understandings of numbers to the system of rational numbers.

5. Understand that positive and negative numbers are used together to describe quantities having opposite directions or values (e.g., temperature above/below zero, elevation above/below sea level, credits/debits, positive/negative electric charge); use positive and negative numbers to represent quantities in real-world contexts, explaining the meaning of 0 in each situation.

6. Understand a rational number as a point on the number line. Extend number line diagrams and coordinate axes familiar from previous grades to represent points on the line and in the plane with negative number coordinates.

a. Recognize opposite signs of numbers as indicating locations on opposite sides of 0 on the number line; recognize that the opposite of the opposite of a number is the number itself, e.g.,

–(–3) = 3, and that 0 is its own opposite.

Even on the first day of CryptoClub, using the cipher wheel, students are able to see the importance of 0. Later while studying additive ciphers, students use negative numbers to help encrypt and decrypt messages. Using a number wheel model for mod 26 arithmetic reinforces number line concepts from regular arithmetic. Students understand that subtraction 'undoes' addition and that adding the additive inverse of a number is the same as subtracting.

Grade 7. The Number System **7.NS**

Apply and extend previous understandings of operations with fractions to add, subtract, multiply, and divide rational numbers.

1b. Understand p + q as the number located a distance |q| from p, in the positive or negative direction depending on whether q is positive or negative. Show that a number and its opposite have a sum of 0 (are additive inverses). Interpret sums of rational numbers by describing real-world contexts.

Students can see the similarities and differences of additive inverses in regular arithmetic and mod 26 arithmetic.

2a. Understand that multiplication is extended from fractions to rational numbers by requiring that operations continue to satisfy the properties of operations, particularly the distributive property, leading to products such as (–1)(–1) = 1 and the rules for multiplying signed numbers. Interpret products of rational numbers by describing real-world contexts

Using the fact that a negative times a negative is positive can reduce computations mod 26. Students study other properties of operations such as multiplicative inverses mod 26, which reinforces their understanding of multiplicative inverses in regular arithmetic.

Grade 7. Expressions and Equations **7.EE**

Use properties of operations to generate equivalent expressions.

1. Apply properties of operations as strategies to add, subtract, factor, and expand linear expressions with rational coefficients.

Students learn to represent encryption and decryption using algebraic expressions. Facility in handling linear expressions builds an understanding of additive and multiplicative inverses mod 26, which are used to solve linear equations.

Solve real-life and mathematical problems using numerical and algebraic expressions and equations.

3. Solve multi-step real-life and mathematical problems posed with positive and negative rational numbers in any form

Cracking a message encrypted with an affine cipher is a multi-step problem that requires the use of positive and negative numbers.

Grade 7. Statistics and Probability **7.SP**

Use random sampling to draw inferences about a population.

1. Understand that statistics can be used to gain information about a population by examining a sample of the population; generalizations about a population from a sample are valid only if the sample is representative of that population. Understand that random sampling tends to produce representative samples and support valid inferences.

Throughout CryptoClub, students come to understand that different letters appear with different frequencies in the English language. They learn how to use frequency analysis to help crack messages. While learning about substitution ciphers and the Vigenère cipher, students construct their own experiments to determine the frequencies of letters in a message.

Grade 8. Functions **8.F**

1. Understand that a function is a rule that assigns to each input exactly one output.

Substitution ciphers are examples of functions that can be represented in tables or by formulas. The CryptoClub student learns that an encryption scheme, as represented in a cipher table can be decrypted only when the decryption is a function. They learn that

multiplicative encryption has an inverse exactly when the encryption key has a multiplicative inverse. This is an introduction to the concept of bijective functions.

3. *Interpret the equation y = mx + b as defining a linear function, whose graph is a straight line*
4. *Construct a function to model a linear relationship between two quantities. Determine the rate of change and initial value of the function from a description of a relationship or from two (x, y) values*

Students learn that the encryption equation for an affine cipher looks like $Y = mx + b$, where m is the multiplicative key and b is the additive key. They come to see the connection with slope and y-intercept that they learn about in algebra class.

Grade 8.Expressions and Equations **8.EE**

3. *Use numbers expressed in the form of a single digit times an integer power of 10 to estimate very large or very small quantities*

Calculating the number of substitution ciphers is an example of a problem where students can come to terms with very large numbers. They use factorials to generate the answer and then scientific notation to understand that the number is indeed very large, approximately 4×10^{26}.

7. *Solve linear equations in one variable.*
8. *Analyze and solve pairs of simultaneous linear equations.*

One technique for cracking a multiplicative cipher involves solving a linear equation mod 26.

Similar techniques for cracking affine ciphers involve solving pairs of linear equations mod 26.

Mathematics concepts used in ciphers in CryptoClub ciphers:

The following summarizes the mathematics topics found in CryptoClub, listed by cipher.

Caesar cipher:

Functions (encrypting and decrypting), reading tables, understanding 0, problem solving, recognizing patterns in the English language.

Keyword cipher and other substitution ciphers:

Bijective functions, frequency analysis, decimals and percents, counting problems.

Additive cipher:

Addition and subtraction, additive inverse, negative numbers, introduction to modular arithmetic, division with remainder.

Multiplicative and affine ciphers:

Arithmetic patterns in modular arithmetic, reducing numbers mod 26 (division with remainder), bijective functions, finding multiplicative inverses mod 26, solving linear equations mod 26, solving simultaneous linear equations mod 26.

Vigenère cipher:

Frequency analysis, common factors