**TEAM PROJECT REPORT**

**Applying Cybersecurity in High School Mathematics Classrooms**

**Submitted To**

**The 2018 RET Site**

**For**

**“Engineering Design Challenges and Research Experiences for Secondary**

**and Community College Teachers”**

**Sponsored By**

**The National Science Foundation**

**Grant ID No.: EEC-1710826**

**College of Engineering and Applied Science**

**University of Cincinnati, Cincinnati, Ohio**

**Prepared By**

**Participant 1: Adam Mesewicz, AP Statistics, 11th Grade, Holmes High School, Covington, KY**

**Participant 2: Kelly Hiersche, Algebra II, 10th/11th Grade, Middlesboro High School, Middlesboro, KY**

**Approved By**

****

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Dr. John Franco**

**Electrical Engineering and Computer Science**

**University of Cincinnati**

**Reporting Period: June 11 - July 27, 2018**

**PROJECT REPORT**

**Teaching Algebra II Content Through Cybersecurity Methods**

**Submitted To**

**The 2018 RET Site**

**For**

**“Engineering Design Challenges and Research Experiences for Secondary**

**and Community College Teachers”**

**Sponsored By**

**The National Science Foundation**

**Grant ID No.: EEC-1710826**

**College of Engineering and Applied Science**

**University of Cincinnati, Cincinnati, Ohio**

**Prepared By**

**Participant 1: Kelly Hiersche, Algebra II, 10th/11th Grade, Middlesboro High School, Middlesboro, KY**

**Approved By**

****

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Dr. John Franco**

**Electrical Engineering and Computer Science**

**University of Cincinnati**

**Abstract**

An important aspect of secondary education is motivating students to learn and teaching concepts which are applicable to the real world. This can be difficult in higher level math classes, such as Algebra II. This paper presents a unit that connects the mathematics used in modern cryptographic methods to the content covered in the Common Core Algebra II standards. Cryptography is a viable real world connection; the importance and applicability of data security for individuals, industry, and national security in the modern world cannot be overstated. The basics of public key, private key, and hash algorithm cryptography are reviewed to create a basic knowledge of cryptography. Then a unit is presented which teaches exponent rules, logarithms, inverse functions, and function composition through those cryptographic schemes. This unit also provides a challenge for students to create their own cryptographic schemes, using their Algebra II function knowledge.

*Key Words* – Cryptography, Encryption, Decryption, Algebra II, Cybersecurity, Private Key, Public Key, Hash Algorithms

1. **INTRODUCTION**

Algebra II is criticized by students and parents, alike, for not relating to real world concepts and not benefiting a majority of students, after they graduate high school. Despite covering core mathematical concepts, it can be difficult to show the relatability of the functions covered in Algebra II standards. Previously, the Kentucky Algebra II End of Course, cumulative exam looked like a typical math test, comprised of multiple choice questions, where students solved equations and math function problems. A field test given at the end of the 2017-2018 school year highlighted a shift in the focus of mathematical testing, with an exam comprised of modeling and word problems. ("End-of-Course - Kentucky Department of Education" 2018) This is a positive shift in the way mathematics is tested in Kentucky, and it signals a need for a change in the way curriculum is presented. The culmination of these two factors inspired the research presented in this paper: a unit on inverse functions, developed from cybersecurity and data encryption concepts.

Cybersecurity is a growing field, in manpower and in importance. Secure transmission of data over the internet is vital for individual and national security. By 2022 the International Data Group (IDG) approximate there will be six billion internet users worldwide. (Steven 2018) Along with this increase in internet users, the damages caused by cybercrime are expected to reach $6 trillion annually by 2021, an increase from the $3 trillion in damages in 2015. This would represent “the greatest transfer of economic wealth in history” (Steven, 2018) as cybercrime would become “more profitable than the global trade of all illegal drugs combined” (Steven, 2018). With this expected increase in cybercrime, there needs to be a parallel increase in cyber defense professionals. Current projections by IDG show there will be 3.5 million unfilled cybersecurity jobs by 2021. There is a national call for more experts in the field of cybersecurity.

Whether students have a prior interest in pursuing cybersecurity as a career, data security is still important for most students. High school students, whose attention is often monopolized by their social media applications, understand the necessity of keeping personal information private and controlled. Any user of Snapchat understands the importance of keeping messages private, a cornerstone in the development of this app. 23% of Snapchat users are between the ages of 13 and 17 ("U.S. Snapchat users demographics 2016 | Statista" 2016), the same ages as most high school students. The relatability of cybersecurity to high school students positions it as an effective topic to relate Algebra II to the real world, but the content must match up as well. Conceptually, encryption and decryption match up with Algebra II content of functions and their inverses. This is the inspiration for the unit developed through this research.

The unit presented in this paper (Appendix IV) ties modern cryptographic methods, the Rivest-Shamir-Adleman (RSA) and the Diffie-Hellman to the Algebra II content, such as exponent rules, logarithms, function composition, and function inverses, while allowing students to create their own encryption method, with they will use to send messages and try to intercept other students’ messages in a computerized game. This paper presents the research done to make the mathematical connections and provides a set of proofs and functions to show what are the successful and unsuccessful methods for applying functions and their inverses to a double encryption scheme. This paper is most valuable to mathematics teachers looking for real world applications, in this case cryptography, to Algebra II. This paper is also useful to educators generally interested in pedagogy approaches that that allow students to problem solve and think in ways that apply their knowledge, instead of rogue memorization of concepts and rules. Finally, this paper is interesting for individuals concerned with some of the mathematics behind modern cryptographic schemes.

1. **LITERATURE REIVEW**
   1. **Goals of cryptography**

The need and application of cryptography has evolved over the last century. Historically, cryptography was used for securing military secrets and battle plans sent during times of war. In the 1900s, cryptography emerged as vital resource for commercial industries, as businesses developed a need to secure their information from competitors. (Baker, 2017) In today’s world, cryptography is important for the average person trying to buy Christmas presents on Amazon. Individuals, governments, and companies, alike, need reliable methods of keep their information private. With the development and increased popularity of the internet, methods of securing information sent around the world instantaneously are vital. Computers with the ability to both encrypt and decrypt information have presented new possibilities and challenges in the field of cryptography.

Cryptography’s basic service is to securely send private information between participants over a channel which is vulnerable to infiltrators. This is done when the sender encrypts plaintext, using a secret value or function known as a key or cipher, transmits the ciphertext, and the receiver decrypts the ciphertext to obtain the plaintext. To ensure confidentiality, the encryption key must be computationally difficult to reverse, to prevent infiltrators from deriving the plaintext when viewing the ciphertext. Along with encryption of the information, cryptography must also allow for integrity and authentication checks. Integrity checks are used to ensure that the encrypted message is not changed as it travels between parties. Authentication checks are used to validate the origin of the encrypted message. (Kaufman et al., 2011) The combination of confidentiality, integrity and authentication ensure the safe travel of information over the internet.

The fundamental tenet of cryptography is, “If lots of smart people have failed to solve a problem, then it probably won’t be solved (soon)” (Kaufman et al., 2011), meaning that the cipher used to encrypt must be computationally difficult to crack. The fundamental tenet of cryptographic attacks may be to develop a method sufficiently faster, for obtaining the plaintext from ciphertext, than brute force. Brute force attacks consist of trying all possible plaintext, input variants, until an input is found that gives an output matching the ciphertext. Modern supercomputers can check approximately blocks per second. The Advanced Encryption Standard has a length of 128 bits, so there are or different keys. To try each of these keys in the AES would take approximately seconds, or 3 billion years. (Baker, 2017) This is why hackers must find a faster method of breaking encryption than purely brute force attacks.

**2.2 Types of Cryptographic Functions**

Cryptographic functions must serve the purpose of encryption, authentication, and integrity checks. Encryption refers to the transformation of plaintext to ciphertext, which cannot be interpreted by an outsider either observing data you are transferring over an insecure network or observing an information stored on an insecure media. Authentication is comparable to two spies, who do not know each other’s identity, have a password which they can use to recognize each other. Strong authentication is a term used when someone can prove they have knowledge of a secret, without revealing the secret itself. Integrity checks are used to ensuring that a message has not been corrupted or changed while it travels between the sender and receiver. Integrity checks work as checksums. A simple checksum, which is not cryptographically secure, breaks up a message into fixed blocks of binary and adds all the 1’s and 0’s. That sum would be sent along with the message, and the receiver would take the message they receive and add up the binary, and if the sum they calculate matches the sum sent, then it would ensure the integrity of the message. (Kaufman et al., 2011)

There are three categories of cryptographic functions: public key functions, secret key functions and hash functions. These methods are applied to scenarios in which information is being sent over an insecure channel or stored on an insecure media. Without one of these encryption methods, data is vulnerable to attackers. Encryption via secret key requires a singular key. Public key encryption requires the use of two keys, a public and a private key. Hash functions do not require a key and are one-way functions. Each of these methods have specific applications and key differences, discussed below. (Kaufman et al., 2011)

Secret key cryptography is the most intuitive of the three cryptographic functions. Secret key requires a shared secret between the two parties. Essentially, the sender uses the secret key to encrypt the message, and then the receiver uses the same key to decrypt the message. One challenge in this method, is finding an effective way to share the secret key between the two parties. One way to create a shared secret is through the Diffie-Hellman Exchange (which is discussed in a later section). Secret keys are successful in accomplished the classic goal of cryptography, which is transmitting information over an insecure channel, as described above. A secret key can also be used by a single individual to store information on an insecure media. If a person develops a key to encrypt their information before it is stored, then that information is secure and only accessible to the creator, as long as the key is remembered. (Kaufman et al., 2011)

Secret key cryptography can be used for authentication. This happens when one party needs to verify the identity of the receiver of their messages. To do this, the sender would use the previously established secret key with their intended receiver. The sender can choose a number and encrypt it using the secret key (possibly by adding the secret to the chosen number) and send the encrypted number to the receiver. If the receiver is the same person who the sender had previously established contact with, then the receiver can decrypt using the secret key, and send the original number back. If the sender gets back the number they originally chose, then they must be communicating with their intended sender. This could be initiated by either party to verify identities. (Kaufman et al., 2011)

Secret key cryptography can provide a more secure checksum method than was described at the beginning of this section. To protect against malicious changes to messages, a secret checksum algorithm is required, and the secret would need to be known by both parties for a successful check. Often, there is a common known algorithm, and a secret key. These two are used to create a Message Authentication Code (MAC), which is sent with the message. The receiver can then use the public function and secret key to create a MAC code and match it with the code sent along with the message. Private keys can be used successfully to encrypt a message, ensuring confidentiality, authentication, and integrity. (Kaufman et al., 2011)

Public Key cryptography differs from secret key because public key requires two separate keys. Secret key cryptography is also called symmetric cryptography because both the sender and receiver use the same key, whereas in public key cryptography, is called asymmetric cryptography, because the sender and receiver decrypt with different keys. In public key cryptography each party has their own public key, available to the general public, and their own private key, which is not to be shared with anyone. In this case, encryption and decryption are each mathematical functions, which are inverses of one another (Here, it begins to become clear how cryptography could be applied to Algebra II). The public key of the receiver is used by the sender to encrypt the information, while the private key of the receiver is used by the receiver to decrypt the information. This method can effectively send secure information over an insecure channel, or be used to secure information stored on an insecure media. (Kaufman et al., 2011)

Secret key cryptography does have a processing speed advantage over public key cryptography, but there are some weaknesses in the secret key checksums, which are addressed by in public key cryptography through the use of digital signatures. In secret key checksums, more than one person knows how to generate a MAC code, because the secret key is shared, Therefore, any person which is capable of verifying a MAC code, could also generate a MAC code. In public key cryptography, digital signatures are used instead of MAC codes. Digital signatures, like MAC codes are numbers associated with messages, but a digital signature can only be created by someone who knows the private key. The public key can be used to verify the signature, but not to create it. This allows digital signatures serve the dual purpose of data integrity and authentication. (Kaufman et al., 2011)

The final class of cryptography utilizes hash algorithms, also known as message digests or one-way transformations for the purpose of verifying message integrity. Hash algorithms can be used to compress a message of an arbitrary length to a smaller, specific size. The hash functions used for this compression are not secret or private, but hash functions are one-direction, so they cannot be undone by someone observing the transmission to get from the hash value to the original message. The process of applying hashing function begins by taking a message of an arbitrary length and breaking it into segments of a fixed length. The shared secret is added to the first segment of the message and hashed, to create a hash value. That hash value is added to the next segment of the message, and hashed to create a new hash value. This process continues until there is a singular hash value which can be sent along with the message. When the receiver gets the message and the hash value, the receiver can put the message through the same hash algorithm, to insure the integrity of the message; if the receiver calculates the same hash value as they received, the message has not been altered between the time the sender sent it and the receiver received it.

There are three essential properties of a hash function.

1. For a message, *m*, the hash of *m, h(m)* must be relatively easy to compute, without taking a lot of processing time.
2. There is no method for determining *m* from *h(m),* other than utilizing brute force methods.
3. It must be computationally infeasible for two inputs values to hash to the same value

One example of a hash function could be square an input, add a large constant, and take the middle digit as the hash value. This example is easy to compute (requirement one), difficult to reverse (requirement two) but does necessarily create a unique hash that could not be recreated with a different input, but it works well to give a general idea of how a hash function would be applied. Hashing is often applied to password checking, so that the password itself does not need to be stored, just its hash value, and when a password is typed in, its hash is taken and compared the stored hash value, if it matches, the user may proceed. These hash algorithms can be used to create a MAC code, similar to secret key cryptography or to create message fingerprints. These are the most common applications of hash functions. (Kaufman et al., 2011)

A combination of asymmetric, symmetric, and hash algorithm cryptography can also be used to encrypt information. Typically, symmetric systems compute faster than asymmetric systems, because they generally use key lengths which are shorter, but asymmetric key systems can enhance the security of communication. To exploit of each these systems advantages public key cryptography can be used to establish a shared, secret key, which can then be used to encrypt the remainder of communication. Hash algorithms can then serve the sole purpose of message integrity. (Damico, 2009) Processing speed, ease of computation, message security, and likelihood of infiltrator access must all be considered when designing a cryptographic protocol for communication.

**2.3 Examples of Math used in Encryption**

To effectively relate the mathematics content in Algebra II to the core concepts of cryptography requires a knowledge of the current applications of math, both historically and in modern cryptography. Classical cryptography, like that used of the Ancient Greeks and Romans, often incorporated a shift cypher, where each letter in the alphabet was shifted by a certain number, to create ciphertext, and then decrypted by reversing the shift. (Damico, 2009) In this case of symmetric cryptography, the shared key would be the number used to shift the original plaintext. This encryption, *E(m)* could be represented mathematically with a simple addition function of a constant, *c*, and the decryption function *D(s)* by a simple subtraction function, where the message sent is represented by the letter *m*.

|  |  |
| --- | --- |
|  | (1) |
|  | (2) |

The use of shift ciphers can be seen from the B.C. era with the Caesar Cipher, to World War II which the application of the Enigma Machine. (Damico, 2009)

While classical cryptography can be characterized by shift ciphers, many modern day public key cryptographic schemes are characterized by their incorporation of modular arithmetic, prime numbers and exponent properties. After discussing these three mathematical concepts, they will be applied to two asymmetric cryptographic methods: The Diffie-Hellman Exchange and the RSA. The Diffie-Hellman Exchange can be used for establishing a shared secret. RSA is an authentication method, for verifying a sender or receiver.

Most of the popular public-key, asymmetric cryptographic systems are based on prime numbers. A number can be classified as prime, if and only if, that number has exactly two divisors, one and itself. The mathematical proof will not be discussed here, but there are an infinite number of prime numbers. (Ferguson and Schneier 2003) This is beneficial for cryptography, because it theoretically gives infinite encryption possibilities (computational time and power may limit these possibilities). Public key cryptography typically uses prime number that are 2000-4000 bits long. A number which is 2000 bits long would fall between and . To determine these prime numbers, the basic method requires the user to pick a number and check if that number is prime. All known methods of determining whether a number is prime, through checking all possibly factors of that number, are computationally infeasible. There are feasible ways to test if a number is prime, but these methods are probabilistic, meaning they have a chance of giving a nonprime number. This chance is arbitrarily small, so these methods are typically applied.

There are strong prime numbers in cryptography, which are defined differently than the strong prime numbers present in number theory. In number theory, a prime number is strong if it is closer in value to the closet prime number which comes after it on a number line (next biggest prime number), than it is to the closest prime number preceding it. Mathematically, a strong prime number, , where n is the index, is greater than the mean of the of the next smallest and next largest prime numbers (equation 3),

|  |  |
| --- | --- |
|  | (3) |

In cryptography, strong primes must satisfy four conditions ("Are 'Strong' Primes Needed for RSA" 2001):

* must be sufficiently large; it must be infeasible for a cryptanalyst to factor the product of with other large prime numbers
* must have large factors. For an integer and a large prime number ,
* needs to have large prime factors. For an integer and a large prime number ,
* must have large prime factors. For an integer and a large prime number ,

In cryptography, strong prime number are essential for the creation of generators, used in cryptographic methods such as RSA. A generator is a number created through the multiplication of two prime numbers. For example, the two prime number 13 and 29 give the generator 377. It is computationally infeasible to factor the number 377 by any method other than trying all possible factors, which takes a long time. In cryptography, as stated above, numbers used are much, much larger than 13, 29, and 377, making brute force an infeasible method as well. (Crow, 2002) RSA is a public key cryptographic method where the public key contains a public modulus, and an encryptor, . The public modulus is the product of two cryptographically strong primes, and . The private key contains the public modulus and a number, , so that . RSA is a method that uses this public key and private key to authenticate the sender of the message. The sender creates a value, , to send along with the message using their private key and their encrypted message, . The receiver then uses the sender’s public key to decrypt the message. It is only possible for the receiver to decrypt the authentication number sent and create the encrypted message, if the sender used their private key to create that authentication number, because of the mathematical relationship between and . (Kaufman, 2011)

Prime number are important in cryptography because of their application when taking the modulus of a number. Modular arithmetic, or clock arithmetic, has an operation called the modulus, which is used to find the remainder when one number is divided by another. In cryptographic methods, a number is computed modulo a strong prime. When a number is divided by a prime number, *p*, the only possible remainders are the numbers 0, 1, …, *p*-1. (Ferguson and Schneier 2003) The number which is the divisor is called the modulus. Modular arithmetic allows computers to work with smaller numbers once the modular operation has been done. For example, 25 modulo 7, would be taking the number 25 and dividing by the modulus 7, to find the remainder. The only possible remainders would be numbers less than 7. In this case, 25 modulo 7 gives 4, a number much smaller than 25. This difference in size is exaggerated in cryptography when working with even larger numbers. Additionally, there is no method for reversing the application of a modulus, meaning it does not have an inverse function. This means, given the number 4, it is computationally infeasible to work backwards and determine that the original number was 25, even if the modulus 7 is a publically known number. The number 32 when divided by 7 also gives a remainder of 4, so how would an eavesdropper know which number was originally intended, 25 or 32. This becomes even more difficult when the number you are taking the modulus of has been raised to a power (for further information, research the discrete logarithm problem). The computational infeasibility of undoing the modulus operation makes this a strong method for encrypting data, which will be more fully expressed in the Diffie-Hellman Exchange.

Students in Algebra II should have knowledge of prime numbers from previous classes, but modular arithmetic is not taught in most public school systems. Fortunately, exponent properties, particularly their application in functions, are important for a variety of standards taught in the Algebra II Common Core curriculum.("High School: Algebra » Introduction | Common Core State Standards Initiative" 2018) As exponents and their properties are utilized in a variety of cryptographic methods, this creates a clear and helpful connection between curriculum and cryptographic concepts. In cryptography, the exponent rule most often applied is the power rule. The power rule for exponents states that if an expression, , with exponent , is raised to a power, , you must multiply the exponent with that power. (Equation 4).

|  |  |
| --- | --- |
|  | (4) |

The commutative property of multiplication (Equation 5) states that two numbers can be multiplied in any order, and the same result will be given.

|  |  |
| --- | --- |
|  | (5) |

Both these properties apply in modular operations as well, and therefore, are essential for a variety of cryptographic methods. (Ferguson and Schneier 2003)

1. **GOALS AND OBJECTIVES**

The goal of this research is to identify mathematical principles in basic cryptography, tie those principles to the Algebra II Common Core Standards, and create a unit to increase student engagement and performance. This unit should provide opportunities for students to relate Algebra II content to the real world, so they can see the applicability of the subject. Students should learn content related to exponential functions, logarithms, functions and their inverses, and function composition in this unit.

1. **RESEARCH STUDY DETIALS** 
   1. **Diffie-Hellman Exchange**

With the goal of creating an Algebra II unit inspired by concepts in Cybersecurity, an understanding of some current cryptographic techniques is necessary. There are two cryptographic techniques in particular, The Diffie-Hellman Exchange and the RSA, which were essential in deciding on the mathematical content that will be covered in this unit. The Diffie-Hellman Exchange is an asymmetric, public key cryptographic method used to create a shared secret between two parties over an insecure channel, using the power rule, modular arithmetic, and prime numbers. The RSA is another asymmetric, public key cryptographic method which allows for authentication of the source of a message. (Kaufman, 2011)

Like all asymmetric cryptographic methods, the Diffie-Hellman Exchange requires both a public and a private key. The public key is comprised of two prime numbers, which are visible to to all parties, including potential attackers. Each party has their own private key, which a number smaller than both numbers in the public key, and does not have to be prime. In the Diffie-Hellman Exchange, both parties take a base number (from the public key), raise it to a power (from their personal, private key), and then take the modulus (number from the public key) of the resulting number. For this example, the two prime numbers will be 23 and 5, though it should be noted in real-life cryptographic algorithms, the numbers used would be much, much larger. The number 5 will be the base number for both Party 1 and Party 2, while 23 will be the modulus. The modulus should always be the larger of the two numbers. Party 1’s private key number will be 4 and Party 2’s private key number will be 3. The first operation done by Party 1 is shown in Equation 6 and the first operation done by Party 2 is shown in equation 7.

|  |  |
| --- | --- |
| *Party 1:* | (6) |
| *Party 2*: | (7) |

Party 1 then sends their resulting number, 4, to party 2 over the insecure channel. Party 2 in turn sends their number, 10, to Party 1. So far, both prime numbers and modular arithmetic have been utilized. Now, the power rule and commutative property of multiplication will be used to create the shared secret. Party 1 takes the number they have received, 10, and raises it to their own private key number, 4 and then takes modulo 23 of the resulting number (Equation 8) 18. Party 2 does the same with the number 4 and their private key number 3 (Equation 9). When this is done, the two parties now share a secret, which is not visible or able to be calculated by unwanted observers.

|  |  |
| --- | --- |
| *Party 1:* | (8) |
| *Party 2:* | (9) |

If these equations are rewritten in their exponential form (equations 10 and 11), we can see how the power rule is applying and allowing both parties are able to generate the same number.

|  |  |
| --- | --- |
| *Party 1:* | (10) |
| *Party 2:* | (11) |

Exponent rules are directly covered in Algebra II and background knowledge of exponents are necessary for a variety of equation graphing standards, making the Diffie-Hellman a real-world application of the content of Algebra II material, which is beneficial for students. Students will see that Alegbra II is applicable to a field which directly impacts not only their daily life, but their parents’ lives, and even national security. (Ferguson and Schneier, 2003)

The Diffie-Hellman Exchange is useful because it establishes a shared secret, which, in combination with a function. can be used to encrypt a message. The inverse of that function is then necessary to decrypt the cipher text and obtain the message. Encrypting and decrypting with functions and their inverses is the next essential cryptographic concept that inspired this Algebra II unit. Functions and their inverses are covered in the Common Core Standards, as well. The proposed unit allows students to create a system that fulfills cryptography’s basic service of encrypting plaintext and subsequently decrypting the ciphertext to return the original plaintext. This will be done purely with functions covered in Algebra II: namely, linear functions power functions, exponential functions, and their inverses, linear inverses, root functions, and logarithmic functions.

* 1. **Development of Function Proofs**

The function chosen to encrypt must allow all possible inputs, and each input must only give one output. This happens to be the mathematical definition of a pure function, which is a core concept for students taking Algebra II. Also, the function used to encrypt must have an inverse which will always return the original input. A function, , with an input of *,* and its inverse, *,* must have a relationship so that returns the value *x*. Otherwise, when applied to cryptography, the receiver could not reliably get the original message. Functions need to be identified that both fulfill the above requirement and are part of Common Core Algebra II curriculum, so proofs were designed. These functions and their inverses are available in Table 1. To increase the security of the method developed in this unit, the sender and receiver would not use the same function. Ideally, for activities in this unit, the sender and receiver would need no prior contact established, so that they could each use any function they desired to send a secure message. A double encryption method was identified as they best method for accomplishing this goal, because each person could inverse their own function, without needed to know the other person’s function. In this method: Party 1 encrypts their message, *,* with function *,* and sends the result to Party 2. Then Party 2 encrypts what they received with function *,* and sends the result to Party 1. Party 1 can then decrypt using the inverse of their function, *,* and send the result to Party 1. Party 2 could then decrypt with their inverse, *.* Once this decryption was done, Party 2 would have the original message sent by Party 1. The two functions must fulfill the equation:

|  |  |
| --- | --- |
|  | (12) |

This introduces the concept of function composition into the unit as well, covered in standard (insert standard number here). Trying a variety of functions combinations in equation 12, it was determined that Party 1 and Party 2 would need some prior knowledge to successfully send a message. Both parties need to decide ahead of time to use either linear functions, power function, or exponential functions. For example, a successful method for allowing Party 1 to use a linear function, while Party 2 used a power function, could not be determined using the true inverse of the functions):

**Proposition 1:** Two parties may not choose from different classes of functions and still successful transmit a function.

**Proof:**

*Party 1:*  *= , , where*

*Party 2:* ,

**Step 1:** Party 1 encrypts message *x* with

**Step 2:** Party 2:

**Step 3:** Party 1 decrypts using

**Step 4:** Party 2 decrypts with

*Message is not successfully received*

As shown above, when the two parties use different function types, the double encryption process does not return the original message, *x*. If the two parties use the same type of function, even without knowledge of the constant chosen by the other party, it is possible to successfully send a message using the double encryption method. For example, both parties can decide to use power functions, with non-zero integer constants *n* and *m*.

**Proposition 2:** Two parties can send a message using double encryption via power functions without sharing the value of their exponent.

**Proof:**

*Party 1:*  *,*

*Party 2:* ,

**Step 1:** Party 1 encrypts message *x* with

**Step 2:** Party 2:

**Step 3:** Party 1 decrypts using

**Step 4:** Party 2 decrypts with

*Message successfully received*

This will work if both parties use any of the functions from this list,: linear function with a slope of one (, multiplicative function (, power function , reciprocal function , or root function , where is any positive integer, as long as they both agree upon a function type. Each party may choose their own value for A as their private key. The function type would need to be either a shared secret between the two parties, possibly established through the Diffie-Hellman Exchange, or the function type would be listed as the public key.

The functions listed above still have some limitations, because they only allow for one constant, *A*, to be used. If this double encryption method was to be used, but a second constant were to be added, such as in the functions: , , or , where *A* and *B* are two positive integers not equal to one, then more information must the shared between the parties. This is proven below in proof three.

**Proposition 3:** The decryption method of applying does not successfully transmit a message if both parties use a function of the form , where B and A are non-zero, positive integers.

**Proof**

*Party 1:* , *:*

*Party 2: ,*

**Step 1:** Party 1 encrypts message *x* with

**Step 2:** Party 2:

**Step 3:** Party 1 decrypts using

*The problem here is that when Party 1 takes the inverse, the B factor should disappear, but it does not. This is only possible if Party 1 has knowledge of what number B was raised to (D). Otherwise:*

**Step 4:** Party 2 decrypts with

*Message not successfully received.*

If Party 1 knows the power chosen by party 2, *D*, then Party 1 can account for this when they create their decryption function. Party 2 must know the value of exponent A to create their inverse function. The proof below shows the appropriate inverse function when the value of *D* is shared either through the Diffie-Hellman or public key.

**Proposition 4:** When functions apply two integer constants, the value of one of those constants must be shared with the second party for successful message transmission

**Proof:**

*Party 1:* , *:*

*Party 2: ,*

**Step 1:** Party 1 encrypts message *x* with

**Step 2:** Party 2:

**Step 3:** Party 1 decrypts using

**Step 4:** Party 2 decrypts with

*Message successfully received*

The value of the constant *D* is essential knowledge for Party 1 when developing a proper inverse function, as is the value of exponent A for Party 2. As the complexity of the function chosen for encryption is increased, so must the amount of information shared between the parties. This is not ideal for cryptographic methods meant to be applied outside of the classroom environment. Despite this, it does create an interesting problem for students to solve; they must think outside of their knowledge of inverse functions taught in class to create a specific inverse that will return the original input during function composition. For students to create the appropriate inverse function, as in the case demonstrated above, requires a firm grasp of exponent properties, inverses, function composition, and also a strong number sense. It would also require divergent thinking, as they move beyond the basic methods taught for finding function inverses, and look to solve a more complicated problem. This would be a good extension for high-excelling students.

All of this function testing is necessary so that any teacher implementing this unit understands the possibilities available to the students solving the challenge of using Algebra II functions to create a double encryption cryptographic method. While it will be important for students to develop some, or all, of these proofs on their own, to practice content standards and standards for mathematical practice, most students do not find the development of proofs to be fun or interesting. A fundamental goal of developing this unit to is find a way to make the content interesting and real-world so that students will have increased engagement and performance. Therefore, a computer game was developed, which would allow students to use the functions they provided proofs for to send secret messages to one another.

This game utilizes the proofs developed through this research to allow students to send each other messages that are encrypted and decrypted through a double encryption scheme. Students may connect with anyone who is also running the Java code, and all the information passed in the game goes through a central monitor, which is run by the teacher. All students are broken up into teams. Once a student decides to connect communicate with another student and sends a message, all other students can see the cipher text that passes between to two parties, as if they were a man in the middle, trying to intercept valuable secrets or information. Students gain points whenever a message is successfully transmitted, unless a man-in-the-middle student can intercept and decode their message. If a man-in-the-middle student can determine another team’s encryption method, they can impersonate a member of that team, and they will gain points for ever message they successfully transmit over that team’s channel. The user interface of this game can be seen in Figures 1 and 2 (Appendix III), and the source code for this game is available at https://sites.google.com/site/kellyjhiersche2018/.

1. **RESEARCH RESULTS**

Students will have the opportunity to learn about the basics of cybersecurity, reinforce their prior math content knowledge, learn new content covered in the Common Core Algebra II standards, and refine skills from the Standards for Mathematical Practice. The overall goal of this unit is for students to use functions and their inverses to develop a double-encryption technique for securely sending information. The unit presented is broken up into four activities, the first to introduce students to data security and public key cryptography principles, the second activity introduces the Diffie-Hellman Exchange, the third requires students to create double encryption function proofs, and in the fourth activity students can test their solutions in the Java-code-based computer game.

In the first activity (Appendix V) provides an opportunity to build the students’ interest in the cryptography. This activity is essential for convincing the students to buy into the unit. If they are excited about the idea of encryption, both to send secret messages and to intercept the messages of their friends, then it should make the mathematical content instruction in later activities more exciting and valuable. Students will go through a process that introduces them to public key cryptography through an activity developed by the CS Unplugged organization. This activity requires students to use public and private maps, shown in Figure 3 (Appendix III), and simple mathematical operations (addition) to encrypt information. This activity should be particularly helpful for visual learners or students who struggle with math, because it does not yet introduce any Algebra II content, but does promote critical thinking and problem solving.

In the second activity (Appendix V), students will get introduced to logarithms as an inverse to exponents, as well as reinforce their knowledge of exponent rules. This material will be presented through the cryptographic method of the Diffie-Hellman Exchange. To understand why the Diffie-Hellman is successful at creating a shared secret between two parties, students must understand both the commutative property of multiplication and the power rule. Initially the Diffie-Hellman should be presented in an adjusted form, so that modulus is not used. This allows students to have an opportunity to try and “break” the Diffie-Hellman by finding a way to solve for a missing exponent. Students will have an opportunity to develop methods on their own, but this will also serve as a transition into logarithms. By introducing logarithms in this way, students will see them as instantly applicable and as a solution to a problem they are currently trying to solve. Now, students will hopefully realize that if the Diffie-Hellman Exchange can be cracked by high school math students, it is not very secure. This will allow the introduction of modular arithmetic. Modular arithmetic may not be explicitly covered in the Common Core Algebra II standards, but it will give students another way to think about numbers and their relationships. According to the New Jersey Department of Education, modular arithmetic is helpful for increasing students number sense. ("Standard 6: Number Sense" 2018) Throughout this activity, students will have the opportunity to increase their knowledge of cybersecurity processes used in modern cryptography and increase their math knowledge in a more fulfilling way than typical direct instruction.

In the third activity (Appendix V) students will develop their encryption schemes. The encryption process will require students to develop either sets of functions or generic proofs which will allow them to encrypt, and provide the appropriate inverse functions that will decrypt a message. This will require a lesson by the teacher on the relationship between functions and their inverses, how to determine the inverse of a function, and the relationship between a function and its inverse when you compose these two functions (it is recommended that students have prior knowledge of function composition). When they use this information to begin creating their own encryption schemes, requirements derived from cybersecurity principles must be considered.

To develop a set of criteria and constraints for the challenge, the requirements for a successful hash function were modified to fit this assignment. Students’ encryption schemes must be reliable: All possible inputs must be viable for successful transmission (or students must explicitly state the limitations – which is the possible domain of their functions). Their schemes must be computationally difficult for infiltrators to break through. This should encourage students to use more complex functions, and limit the amount of information they make available in a public key. This would also require students to provide more than one method of encryption, because if they use the same method over and over, it becomes easier for a hacker to determine the strategy being used. This will motivate students to work with as many functions as possible. Clearly, functions and their inverses will be understood by the challenge presented to the students, but to prepare the students for the challenge, both mathematically and in their knowledge of cryptography, there is the opportunity to cover other content standards as well.

1. **CONCLUSIONS**

Conclusions on the value of this unit can only be fully understood after not one, but multiple years of implementation of this unit. Student interest, content retention, and knowledge of cryptography needs to be measured before and after unit implementation. The broad conclusion that can hopefully be drawn from this research is: when students are presented the content of Algebra II in the context of its real world applications, they are more interested in the content, and therefore, have a better understanding for the content and more successfully retain the knowledge. An expected specific conclusion to this unit is that students will perform better on summative exams at the end of this unit, in comparison to prior units taught and in comparison to previous years’ student performance. Also, students will demonstrate they have retained knowledge on inverse functions and logarithms by performing well on End of Course exam questions related to that content. Hopefully, teachers implementing this unit will also observe a qualitative change in student motivation and excitement about the course due to the implementation of this unit.

1. **RECOMMENDATIONS**

Further research should look to develop additional units which provides applications of Algebra II content and give students opportunities to problem solve and critically think while they learn math. As these units are created and subsequently taught, teachers should be sure to measure pre and post-performance of students on math content, knowledge of the real world application, and student reported interest during the unit, using surveys. It may also serve this research well to have a control class, who is taught the material using the traditional approach of direct instruction through notes and worksheets, and then a class who is taught using a CBL/EDP approach, so that student performance can be compared. Further research should also look to apply the overarching concept behind this research: students are more motivated to learn material they feel matters to their lives and the world, in content areas besides mathematics.

1. **CLASSROOM IMPLEMENTATION PLAN**

This unit should be implemented utilizing Challenge Based Learning (CBL) principles. Challenge Based Design begins with the introduction of a big idea. The big idea for this unit is Cybersecurity. The big idea needs to be broad enough for multiple possible challenges, but focused enough for the teacher to guide students in the direction they planned. The big idea should be presented to the students, and then there should be a hook, which elicits intrigue and interest in the topic. For this unit, there are various possible hooks. A video which directly relates to the students, such as a video talking about social media hacks, perhaps Snap Chat, a very popular application among teenagers, would be a good way to pique the interest of high school students.

Once students develop an interest in the big idea, they next need to be given an opportunity to develop a list of questions concerning the overarching topic, called Essential Questions. The goal of CBL is for students to guide the instruction and seek out information on their own. CBL is a good example of student centered learning. From this list, the class can determine one essential question, which connect the big ideas to the content of the subject. A possible essential question for the proposed unit is: “How is mathematics used to keep data secure during transmission?”. With the essential questions determined, the teacher can lead the students to developing a possible challenge which could be completed to answer this question.

The students should approach the challenge through the Engineering Design Process (EDP). The challenge for this proposed unit is: “How many secure methods of encryption can you develop to send a secure message between you and your friends? Constraint: This method must use the properties of functions and their inverses”. The most essential component of the challenge is that there must be multiple solutions for the students to discover; there cannot be one correct or obvious solutions. Now that the challenge is agreed upon within the class, students use the EDP to learn more about the topic, brainstorm possible solutions, create a solution process, test the process, refine their solution, and finally, students must communicate their results either verbally, through text, or using a combination (such as a PowerPoint presentation). The EDP provides enough structure to be applied in a classroom without excessive chaos, but enough flexibility that students are not confined to predetermined steps that will guide them to a singular answer. The combination of the intrigue created by a real world field, cryptography, with the CBL and EDP principles allows for a unit which inspires students to learn, encourages teamwork, and rewards creativity.

1. **ACKNOWLEDGEMENTS**

This research and the resulting paper would not be possible without the support and resources of the National Science Foundation. This research was funded by grant Grant ID# EEC-17110826: “Engineering Design Challenges and Research Experiences for Secondary and Community College Teachers.” Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation. Also instrumental to this research was the guidance and expertise of faculty mentor Dr. John Franco and Graduate Research Assistant Shaunuk Kapoor. The Java code was written in its entirety by Dr. Franco. A special thank you to Adam Mesewicz, an RET participant also working on the Cybersecurity project. Gratitude would also like to be extended to the RET Project Director and Principal Investigator, Dr. Anant R. Kukreti, RET Resource Person and Grant Coordinator, Debbie Liberi, Kristin Barnes, and RET Resource Teacher, Mrs. Pamela Truesdell.

1. **BIBLIOGRAPHY**

Baker, S. (2017). "Dissecting Schnorr’s Digital Signature Scheme". Review of Computational Science and Engineering, 3(1), 52.

Crow, J. (2003). "Prime Numbers in Public Key Cryptography". Sans.org, <https://www.sans.org/reading-room/whitepapers/vpns/prime-numbers-public-key-cryptography-969> (Jul. 23, 2018).

"High School: Algebra » Introduction | Common Core State Standards Initiative." (2018). Corestandards.org, <http://www.corestandards.org/Math/Content/HSA/introduction/> (Jul. 11, 2018).

Damico, T.M. (2009). A Brief History of Cryptography.” *Inquiries Journal/Student Pulse,* 1(11).

"End-of-Course - Kentucky Department of Education." (2018). Education.ky.gov, <https://education.ky.gov/AA/Assessments/Pages/EOC.aspx> (Jul. 13, 2018).

Ferguson, N., and Schneier, B. (2003). Practical cryptography. Wiley, New York, 185-222.

Kaufman, C., Perlman, R., and Speciner, M. (2011). *Network security: private communication in a public world*. Prentice Hall PTR, Upper Saddle River, NJ.

Morgan, Steven. (2018). “Top 5 cyerbescurity facts, figures and statistics for 2018.” Cybersecurity Business Report, in press.

Rivest, R. and Silverman, R. (2001). “Are 'Strong' Primes Needed for RSA.” [Abstract] Cryptology ePrint Archive.

"Standard 6: Number Sense." (2018). State.nj.us, <https://www.state.nj.us/education/archive/frameworks/math/math4.pdf> (Jul. 23, 2018).

"U.S. Snapchat users demographics 2016 | Statista." (2016). Statista, <https://www.statista.com/statistics/326452/snapchat-age-group-usa/> (Jul. 23, 2018).

1. **APPENDIX I: NOMENCLATURE USED**

RSA = Rivest-Shamir-Adleman; used for authentication of data (pg. 7)

Public Key Encryption = asymmetric cryptographic method, each user has two keys, a public key used by others to encrypt information and a private key which can be used to decrypt (pg. 5)

Secret Key Encryption = symmetric cryptographic method, two parties share a secret key used to encrypt and decrypt the information (pg. 4)

Hash Algorithm = one-way function used to compress the size of data (pg. 5)

Authentication = verification that a message came from the intended source or will be received by the intended source (pg. 4)

Data/message Integrity = verification that a message has not been altered as it traveled through an insecure channel between parties (pg. 4)

Function = a mathematical equation in which each input maps to only one output (pg. 9)

Exponentiation = the operation of raising a quantity to a power (pg. 8)

Modular Arithmetic = system of integer arithmetic (pg. 7)

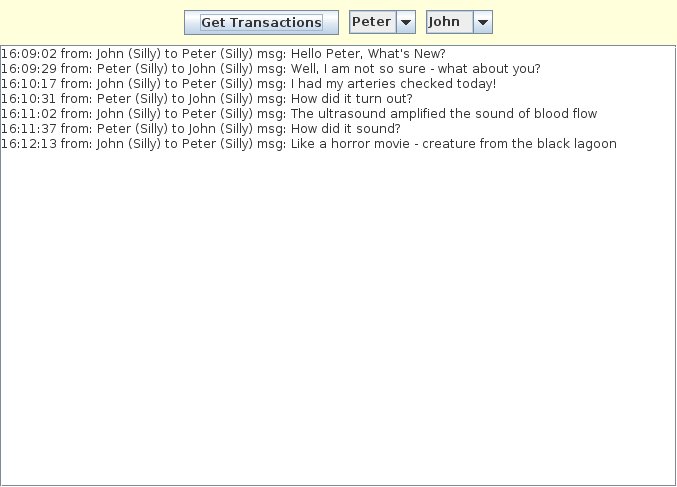
1. **APPENDIX II: RESEARCH SCHEDULE**

|  |  |
| --- | --- |
| **Date** | **Research** |
| 6/18-6/22 | Learned basic cryptographic methods – public key, secret key, hash algorithms |
| 6/25-6/29 | Went through Diffie-Hellman, RSA, and other encryption methods, began developing a scheme for students to encrypt data |
| 7/2-7/6 | Created proofs for functions that could be used in double encryption scheme, began laying out design for the Java Code / created activities to tie specific cryptographic concepts to mathematical content |
| 7/9-7/13 | Continued working on Java code specifications and finalizing content standards which could be covered in the unit |
| 7/16-7/20 | Worked on final research paper and poster for end of summer presentations |

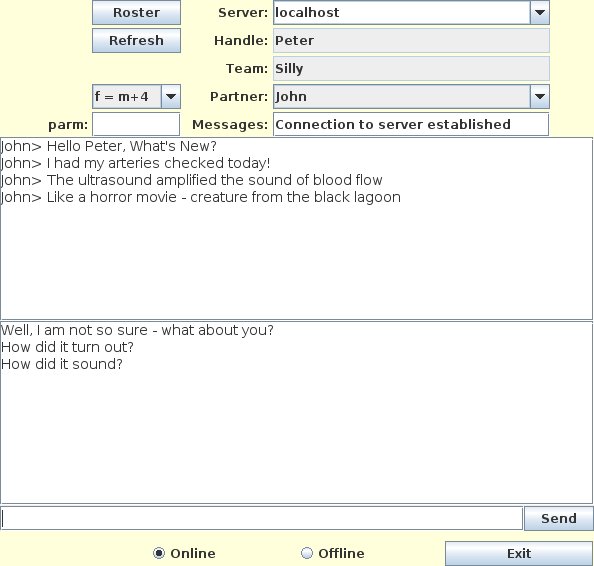
1. **APPENDIX III: TABLES AND FIGURES**

|  |  |  |
| --- | --- | --- |
| **Functions that Satisfy**  when A is an integer greater than zero | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

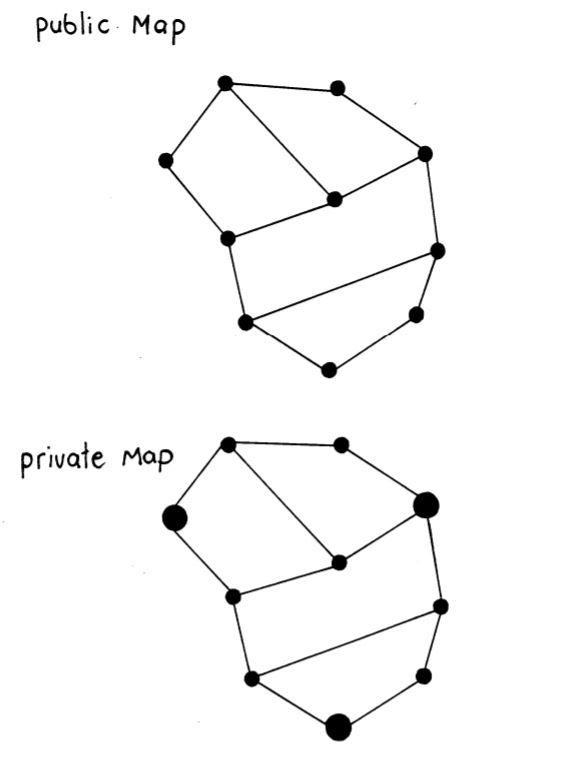
**Table 1:** This table shows the functions and inverses which can be used by students in a double encryption scheme to send messages securely.

****

**Figure 1:** Public information available to all students, which can be used to break encryption schemes.



**Figure 2:** The interface available to each student, where they will choose their function, set parameters, and send messages to one another.



**Figure 3:** These are the public and private maps that will be used in Activity 1 by the students as an introduction into public key cryptography.

1. **APPENDIX IV: UNIT TEMPLATE**

|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info: kellyhiersche@gmail.com** | **Date: 6/26/18** |

|  |
| --- |
| **Unit Number and Title: Unit 1 Cybersecurity and Encryption** |

|  |  |
| --- | --- |
| **Grade Level:** | 10th/11th |

|  |  |
| --- | --- |
| **Subject Area:** | Algebra 2 |

|  |  |
| --- | --- |
| **Total Estimated Duration of Entire Unit:** | 11 Days (50 minute periods) |

**Part 1: Designing the Unit**

|  |
| --- |
| 1. **Unit Academic Standards (**Identify which standards:NGSS, OLS and/or CCSS.Cut and paste from NGSS, OLS and/or CCSS and be sure to include letter and/or number identifiers.**):** |

**N-RNA1-2** Extend the properties of exponents to rational exponents

**F-IFB5** Interpret functions that arise in applications in terms of the context: Relate the domain of a function to its graph and, where applicable, to the quantitative relationship it describes

**F-BFA1b** Write a function that describes a relationship between two quantities: Combine standard function types using arithmetic operations.

**F-BF3-4a** Build new functions from existing functions

**F-LEA4** Construct and compare linear, quadratic, and exponential models and solve problems: For exponential models, express as a logarithm the solution to *abct*= *d* where *a*, *c*, and *d* are numbers and the base *b* is 2, 10, or *e*; evaluate the logarithm using technology.

**A-REIA2** Solve simple rational and radical equations in one variable, and give examples showing how extraneous solutions may arise

|  |
| --- |
| 1. **Unit Summary** |

*The Big Idea (including global relevance):*

Encrypting Information to protect data

Societal Impact – All people send important information over the internet, including students and their parents. This unit will enlighten students into how data is encrypted, how to keep their information safe, and they will develop a way to safely encrypt data.

*The (anticipated) Essential Questions: List 3 or more questions your students are likely to generate on their own. (Highlight in yellow the one selected to define the Challenge):*

1. How can we reliably and effectively encrypt information?
2. How is data encrypted to protect our information?
3. How can math be used to secure information sent online?
4. How can cybersecurity and math be combined to reliably transmit information over the internet?
5. How can we secure secret information using encryption methods?

|  |
| --- |
| 1. **Unit Context** |

Justification for Selection of Content– Check all that apply:

■ Students previously scored poorly on standardized tests, end-of term test or any other test given in the school or district on this content.

■ Misconceptions regarding this content are prevalent.

■ Content is suited well for teaching via CBL and EDP pedagogies.

☐ The selected content follows the pacing guide for when this content is scheduled to be taught during the school year. (Unit 1 covers atomic structure because it is taught in October when I should be conducting my first unit.)

☐ Other reason(s) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Hook: (Describe in a few sentences how you will use a “hook” to introduce the Big Idea in a compelling way that draws students into the topic.)

Students will be shown two videos from news sources that explain recent successes in hacking people’s Snap Chat accounts. Students will then participate in an activity where they use a simple system to encrypt a message, and then find out how to break this encryption. Once they figure out how to break and fix it, they will look for ways to make this method more secure. (This is a visual, pattern based method with only simple addition).

The Challenge and Constraints:

☐ Product **or** ■ Process (Check one)

|  |  |
| --- | --- |
| Description of Challenge (Either Product or Process is clearly explained below): | List the Constraints Applied |
| Snap Chat has hired your firm to develop a secure method of encrypting data being sent over the internet using mathematical functions. | System cannot be easily “hackable”  Must be reliable for all inputs – or you must state what inputs are not viable  Must use at least 1 function we have covered this year  Must use double encryption  Cannot use the exact same encryption system as another group |

Teacher’s Anticipated Guiding Questions (that apply to the Challenge and may change with student input.):

**How is data currently encrypted? What is the goal of cryptography?**

**Is math used to encrypt data – in what ways? Is different data encrypted in different ways?**

**How does coding play a role in encryption? What makes something a “good” encryptor?**

**How many methods are there for data encryption?**

|  |
| --- |
| **4. EDP: Use the diagram below to help you complete this section.** |

****

How will students test or implement the solution? What is the evidence that the solution worked? Describe how the iterative process from the EDP applies to your Challenge.

**To test the solutions, Dr. Franco and I are developing an Applet in java with a GUI that will allow students to input their encryption and decryption functions, to see if they successfully can pass the message between two parties. We will use characteristics of secure encryption to judge their solutions. We will consider factors:**

1. **Each input must only have one possible output**
2. **Low computational power – quick to compute**
3. **Code cannot be broken without trying all possible function encryptions (high level brute force)**
4. **A small change in the input must substantially change the output**
5. **Two messages cannot have the same output**

**This challenge becomes iterative because you can go from Double Encryption to multiple encryption by making small changes to your functions, like incorporating coefficients or additional terms. Also, it can become iterative by making the initial function key secret, so they need to add a second type of encryption to make their key private instead of public. It can be iterative by requiring students to increase security by requiring an authentication process, as well.**

How will students present or defend the solution? Describe if any formal training or resource guides will be provided to the students for best practices (e.g., poster, flyer, video, advertisement, etc.) used to present work.

**Students will present their method of encryption to the class in a 5-minute pitch. They may accompany this pitch with either a poster, a powerpoint, or by using the Whiteboard to explain their process.**

What academic content is being taught through this Challenge?

**Inverse functions, exponent rules, rational functions, exponential functions, and logarithms will be the focus on the content in this Challenge, but students will need a firm grasp on what a function is and inputs and outputs to successful engineer a method to address the challenge.**

Assessment and EDP:

Using the diagram above, identify any places in the EDP where assessments should take place, as it applies to your Challenge. Describe below what kinds of assessment are most appropriate.

|  |  |
| --- | --- |
| What EDP Processes are ideal for conducting an Assessment? (List ones that apply.) | List the type of Assessment (Rubric, Diagram, Checklist, Model, Q/A etc.) Check box to indicate whether it is formative or summative. |
| Identify and Define\_\_\_\_\_\_  Gather Information\_\_\_\_\_\_\_\_\_  \_\_Select Solutions\_\_\_\_\_\_  \_Refine\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_Communication Solution\_\_ | KWL\_\_\_­­\_\_\_\_\_\_\_\_\_\_\_\_\_ ■ formative ☐ summative  Q/A as students research encryption methods■ formative ☐ summative  Checklist for attempted encryption functions ■ formative ☐ summative  Diagram show improvement from last solution■ formative ☐ summative  Students will present their encryption method to teacher for approval ☐ formative ■ summative |

Check below which characteristic(s) of this Challenge will be incorporated in its implementation using EDP. (Check all that apply.)

■ Has clear constraints that limit the solutions

■ Will produce than one possible solution that works

■ Includes the ability to refine or optimize solutions

■ Assesses science or math content

■ Includes Math applications

☐ Involves use of graphs

☐ Requires analysis of data

■ Includes student led communication of findings

|  |
| --- |
| **5. ACS (Real world applications; career connections; societal impact):** |

Place an X on the continuum to indicate where this Challenge belongs in the context of real world applications:

|  |  |  |
| --- | --- | --- |
| **Abstract or Loosely Applies to the Real World** | **|--------------------------------------|-------------------------X-------------|** | **Strongly Applies to the Real World** |

Provide a brief rationale for where you placed the X**:­­­­­­­­­­­­­­**

What activities in this Unit apply to real world context?

Place an X on the continuum to indicate where this Challenge belongs in the context of societal impact:

|  |  |  |
| --- | --- | --- |
| **Shows Little or No Societal Impact** | **|-------------------------------------|------------------------------X---------|** | **Strongly Shows Societal Impact** |

Provide a brief rationale for where you placed the X**:**

What activities in this Unit apply to societal impact? ­­

Careers: What careers will you introduce (and how) to the students that are related to the Challenge? (Examples: career research assignment, guest speakers, fieldtrips, Skype with a professional, etc.)

**Computer Science careers specifically Cryptographer, Cryptanalyst, Computer Engineer, Encryption specialist. – have not decided exactly how to introduce these – don’t know if guest speakers are available.**

|  |
| --- |
| **6. Misconceptions:** |

**I expect misconceptions in the differences between inverse function and function multiplication and function composition, because they are similar in process and both valid approaches to creating an encryption system. I also think there may be misconceptions between inverse operations and inverse functions.**

|  |
| --- |
| **7. Unit Lessons and Activities:** (Provide a tentative timeline with a breakdown for Lessons 1 and 2. Provide the Lesson #’s and Activity #’s for when the Challenge Based Learning (CBL) and Engineering Design Process (EDP) are embedded in the unit.) |

**Unit 1: Cybersecurity and Data Encryption – Design as many methods as possible to mathematically encrypt a message**

**Lesson 1: Understanding Encryption Keys & Breaking Them**

*Lesson 1 will focus on the basics of encrypting information. Students will learn about public keys and privates keys. Students will use the Diffie-Hellman to be introduced to the concept of Logarithms as the inverse of exponential functions. Additionally, student will utilize exponent rules to create a secret key between to people.*

Activity 1: Introducing the Big Idea, the hook, Generating Essential Questions, Presentation of Challenge, Generation of Guiding Questions, gathering information (2 days)

Activity 2: Exponent rules and introduction of logs via Diffie-Hellman (3 days)

**Lesson 2: Encryption with Algebra 2**

*Lesson 2 will focus on the development and utilization of students’ knowledge of inverse functions to send encryption messages. Students will learn about double encryption with asymmetric keys*

Activity 1: Encrypting with Inverse Functions, Gathering information, select solutions, communicate solutions, refine (4 days)

Activity 2: Make and Break the Encryptions: Implement solutions, evaluate solutions, refine (2 days)

CBL: Lesson 1 Activity 1, Lesson 2 Activity 2

EDP: Lesson 1 Activity 1, Lesson 1 Activity 2, Lesson 2 Activity 1, Lesson 2 Activity 2,

|  |
| --- |
| **8. Keywords:** |

Exponent, Radical, Rational, Function, Inverse Functions, Cryptography, Encrypt, Decrypt, Security

|  |
| --- |
| **9. Additional Resources:** |

N/A

|  |
| --- |
| **10. Pre-Unit and Post-Unit Assessment Instruments:** |

None needed

|  |  |
| --- | --- |
| **11. Poster** | **12. Video (Link here.)** |

**If you are a science teacher, check the boxes below that apply:**

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☐ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☐ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☐ Analyzing and interpreting data | ☐ Systems and system models |
| ☐ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☐ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☐ Obtaining, evaluating, and communicating information |  |

**If you are a science teacher, check the boxes below that apply:**

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☐ Demonstrating Science Knowledge **(D)** |
| ☐ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

**If you are a math teacher, check the boxes below that apply:**

| **Ohio’s Learning Standards for Math (OLS) or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ■ Make sense of problems and persevere in solving them | ☐ Useappropriate tools strategically |
| ☐ Reason abstractly and quantitatively | ☐ Attendto precision |
| ■ Construct viable arguments and critique the reasoning of others | ☐ Look for and make use of structure |
| ■ Model with mathematics | ■ Look for and express regularity in repeated reasoning |

1. **APPENDIX V: ACTIVITY TEMPLATES**

|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info: kellyhiersche@gmail.com** | **Date: 07/02/2018** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Understanding Encryption Keys & Breaking them** | **Unit #: 1** | **Lesson #: 1** | **Activity #: 1** |
| **Activity Title: Encryption with Public Key** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **5 days** |
| **Estimated Activity Duration:** | **2 days (50 minute periods)** |

|  |  |
| --- | --- |
| **Setting:** | **Classroom** |

|  |
| --- |
| **Activity Objectives:** |

I can…

1. Develop essential questions about Cybersecurity and Encryption
2. Present at least one way math is used in modern encryption
3. Pass secret information using a public key

|  |
| --- |
| **Activity Guiding Questions:** |

* What are methods of information encryption?
* What are public and private keys?
* How do you share a public key?

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☐ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☐ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☐ Analyzing and interpreting data | ☐ Systems and system models |
| ☐ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☐ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☐ Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☐ Demonstrating Science Knowledge **(D)** |
| ☐ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒ Make sense of problems and persevere in solving them | ☐ Useappropriate tools strategically |
| ☒ Reason abstractly and quantitatively | ☐ Attendto precision |
| ☐ Construct viable arguments and critique the reasoning of others | ☒ Look for and make use of structure |
| ☒ Model with mathematics | ☐ Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):** |

**F-BFA1b**

|  |
| --- |
| **Materials**: (Link Handouts, Power Points, Resources, Websites, Supplies) |

**Powerpoint (**1.1.1.a)

**Video on social media hacking** (still looking for a good video or going to create my own compilation – will input once I have it) 1.1.1.b

[**Printed/laminated copies of public and private map**](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf) **(pg 194)** 1.1.1.c

**Calculators** (not necessary but will increase the speed of the activity)

|  |
| --- |
| **Teacher Advance Preparation:** |

Read the [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf) explaining how the public key encryption works to ensure you understand the method of encryption, how to break it, and how to create guiding questions to bring your students through the activity

|  |
| --- |
| **Activity Procedures:** |

(Procedure can be better understood by viewing the [Powerpoint](https://docs.google.com/presentation/d/1PFSJLHMLpvj9VAB9eCYzF34C6HHqY5XorI_HDjtB6mI/edit?usp=sharing) that goes with this activity)

1. The students need to take a pretest the day before, should only take 15 minutes
   1. This pretest will have a few questions on their knowledge of encryption as well as test their knowledge on inverse functions (logarithms focus) and exponent rules
2. Big Idea: Data Encryption – Will be introduced on the first slide of the powerpoint
3. Hook: Video on social media hacking (tailor to your group of students- I recommend snapchat)
   1. Start a whole class discussion
      1. Ask questions like “Has anyone ever had their social media hacked? Do your photos really disappear after 10 seconds? Can anyone “steal” the information you send?”
   2. Show the video (on powerpoint) \*check ahead of time that Youtube is not blocked on your schools internet
4. Essential Question: Ask students to develop questions surrounding the idea of: “What do you want to know about data encryption?”

\*\*Students will have a sheet where they write their questions – questions they get from their partner and the chosen essential question at the end. This can be done in a notebook as well if it is a graded notebook

* 1. Take 3 minutes to write at least 3 questions about the big idea
  2. Take 3 minutes to share your ideas with a partner and together pick at least 2 questions to share with the group
  3. Criteria/Constraints:
     1. Questions cannot be yes/no or one word answers
     2. Questions cannot be easily Googleable
  4. Have the students share out the questions they decided and fill them in to the empty slide on the powerpoint
     1. (Done whole group) Look for questions that essentially ask the thing until you narrow down to one essential question

1. Do an simple encryption example, outlined in the [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf): Public Key Encryption from Computer Science Unplugged
   1. You will need supplies for this! (printed public and private keys, if laminated, need expo markers kids can write with)
   2. Class should be broken up into groups of 2. Each person with their own public and private map. Everyone sends a message and everyone decodes a message.
2. Class discussion – How did this encryption method work? How could it be broken? How could it be made more secure?
   1. Students should have opportunity to brainstorm possible challenges. This can happen either whole group or in the way essential questions were brainstormed **END OF DAY 1**
3. **START DAY 2** The next day the Challenge will be announced to the classes: Come up with as many viable ways as possible to mathematically encrypt a message between you and your team.
4. Develop guiding questions:
   1. Use same brainstorming technique for guiding questions as we used above for picking the essential questions – with altered times if needed
5. Provide students with a research template for them to start answering some of the questions developed
   1. Each student will have to address at least 2 questions - This can be done by provided a list of websites you recommend students use to gather information
   2. Try to lead students to research things like public vs. private keys, symmetric and asymmetric keys, hash functions, diffie hellman exchange, double encryption
   3. For smaller classes, it may work better to research these questions as a group on the smartboard – student lead google searchs – put 1 trusted student in charge of googleing – give other students the ability to go off and search other things as they think of it, while the main search is run in front of the class
6. Bring all research together whole group – work on answering the question – how is math used now to encrypt information / what are methods of encrypting / what makes an encryption successful
   1. each group must share 2 things they have learned
7. Question to contemplate whole class: Can any of the math we have learned be a viable method of encrypting? **END OF DAY 2**

**\*\*If extra time at end of day 1 or 2 students can try to develop their own public and private key that would work from the exercise completed on day 1**

**Formative Assessments:** Link the items in the Activities that will be used as formative assessments.

1. Brainstorming of essential question worksheet
2. Research template to start answering their guiding questions

**Summative Assessments:** These are optional; there may be summative assessments at the end of a set of Activities or only at the end of the entire Unit.

N/A

|  |
| --- |
| **Differentiation:** Describe how you modified parts of the Lesson to support the needs of different learners.  Refer to Activity Template for details. |

Accommodations:

* Simpler patterned encryption maps (available on page 193 of [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf))
* Adjusted amount of brainstorming time – require 2 questions per person instead of 3
* Give list of websites to use for researching

Extensions:

* If extra time at end of day 1 or 2 students can try to develop their own public and private key that would work from the exercise completed on day 1
* Try and write a procedure for breaking this encryption

|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info:** [**kellyhiersche@gmail.com**](mailto:kellyhiersche@gmail.com) | **Date: 7/2/18** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Understanding Encryption Keys & Breaking them** | **Unit #: 1** | **Lesson #: 1** | **Activity #: 2** |
| **Activity Title: Encrypting with Private Key** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **5 days** |
| **Estimated Activity Duration:** | **3 days (50 minute periods)** |

|  |  |
| --- | --- |
| **Setting:** | **Classroom** |

|  |
| --- |
| **Activity Objectives:** |

1. Students will be able to state the inverse function of exponents – logarithms
2. Students will be able to use logarithms to find the exponential term
3. Students will explain the difference between logs and roots
4. Students will describe and give an example for how private keys are needed for encryption
5. Students will be able to use exponent rules for encrypting information
6. Students will use the basics of modular arithmetic to encrypt information

|  |
| --- |
| **Activity Guiding Questions:** |

1. What is the Diffie-Hellman exchange?
2. How are exponent rules used to encrypt information?
3. How are logs and roots different?
4. Does math create a secure way to encrypt information?
5. How does modern computational power affect the effectiveness of encryption techniques?

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☐ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☐ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☐ Analyzing and interpreting data | ☐ Systems and system models |
| ☐ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☐ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☐ Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☐ Demonstrating Science Knowledge **(D)** |
| ☐ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☐ Make sense of problems and persevere in solving them | ☐ Useappropriate tools strategically |
| ☒ Reason abstractly and quantitatively | ☐ Attendto precision |
| ☐ Construct viable arguments and critique the reasoning of others | ☒ Look for and make use of structure |
| ☒ Model with mathematics | ☒ Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):** |

**F-LEA4** Construct and compare linear, quadratic, and exponential models and solve problems: For exponential models, express as a logarithm the solution to *abct*= *d* where *a*, *c*, and *d* are numbers and the base *b* is 2, 10, or *e*; evaluate the logarithm using technology.

**N-RNA1-2** Extend the properties of exponents to rational exponents

|  |
| --- |
| **Materials**: (Link Handouts, Power Points, Resources, Websites, Supplies) |

Powerpoint explaining the Diffie-Hellman

Worksheet – practice log as inverse of exponents / practice using exponent rules (to be made)

Worksheet – using modular arithmetic & exponent rules to complete Diffie-Hellman

|  |
| --- |
| **Teacher Advance Preparation:** |

Read [this](http://www.cimt.org.uk/resources/topics/art003.pdf) article on Cryptography and mathematics that provides in-depth foundational knowledge.

|  |
| --- |
| **Activity Procedures:** |

**Day 1**

1. Review exponent rules (students should already know product rule, quotient rule, power rule, expanded power rule)
2. Go through Powerpoint which leads students to see how you can use the log if you don’t know what power a number was raised too.
3. Give worksheet where they can practice taking the log to find the missing exponent
4. END CLASS – with a discussion
   1. Ask your students: now that we have seen how logs work – “would you be able to break this encryption method?” “If students with high school math knowledge can break an encryption – is that encryption secure?” Using this knowledge, can we start developing criteria for what would constitute a secure encryption method?
   2. makes

**Day 2**

1. Use Powerpoint to cover Diffie-Hellman with modular arithmetic example
   1. Be sure to discuss why it is difficult to undo modular arithmetic – no set inverse function
   2. Start talking about using inverses to crack codes
2. Students complete worksheet in teams with modular arithmetic to create a shared key
3. END CLASS – discuss why it is difficult to break the Diffie-Hellman when you include modular arithmetic / discuss whether it is better to have a secret key or public key? (difference between activity 1 and 2)

**Formative Assessments:** Link the items in the Activities that will be used as formative assessments.

Worksheet - Diffie-Hellman Exchange by taking the log

Worksheet – Diffie-Hellman with modular arithmetic

**Summative Assessments:** These are optional; there may be summative assessments at the end of a set of Activities or only at the end of the entire Unit.

N/A

|  |
| --- |
| **Differentiation:** Describe how you modified parts of the Lesson to support the needs of different learners.  Refer to Activity Template for details. |

Accommodations

* Include extra examples / more steps in worksheet
* Have worksheet only deal with mod12 so students can use clock model to find the remainder (or have blank clocks w/ right # of blanks for students to fill in to practice modular arithmetic

Extension

* Come up with two possible inputs that would both satisfy the Diffie-Hellman modular example from the powerpoint
* Explain why modular arithmetic is good for created a shared key

|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info: kellyhiersche@gmail.com** | **Date: 07/03/2018** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Encryption with Algebra 2** | **Unit #: 1** | **Lesson #: 2** | **Activity #: 3** |
| **Activity Title: Encrypting with Inverse Functions** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **6 Days** |
| **Estimated Activity Duration:** | **4 Days (50 minute periods)** |

|  |  |
| --- | --- |
| **Setting:** | **Classroom** |

|  |
| --- |
| **Activity Objectives:** |

I can…

1. Recognize and find inverse functions for linear, exponential, power, log, quadratic, and rational functions
2. Develop methods of encrypting messages using functions and their inverses

|  |
| --- |
| **Activity Guiding Questions:** |

1. How can high school math students reliably encrypt information with their current knowledge?
2. What is double encryption?
3. What are the inverses of the functions we have learned about this year?

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☐ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☐ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☐ Analyzing and interpreting data | ☐ Systems and system models |
| ☐ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☐ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☐ Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☐ Demonstrating Science Knowledge **(D)** |
| ☐ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒ Make sense of problems and persevere in solving them | ☐ Useappropriate tools strategically |
| ☒ Reason abstractly and quantitatively | ☐ Attendto precision |
| ☐ Construct viable arguments and critique the reasoning of others | ☐ Look for and make use of structure |
| ☒ Model with mathematics | ☒ Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):** |

**F-IFB5** Interpret functions that arise in applications in terms of the context: Relate the domain of a function to its graph and, where applicable, to the quantitative relationship it describes

**F-BFA1b** Write a function that describes a relationship between two quantities: Combine standard function types using arithmetic operations.

**F-BF3-4a** Build new functions from existing functions

|  |
| --- |
| **Materials**: (Link Handouts, Power Points, Resources, Websites, Supplies) |

Powerpoint explaining double encryption with simple example

Notes sheet on inverse operations and functions

Worksheet on inverse functions and operations

Directions page with challenge (constraints/criteria included)

Cardstock for students to present their encryption methods

Rubric for grading sales pitch

|  |
| --- |
| **Teacher Advance Preparation:** |

Read through all materials and check answer key to worksheet

|  |
| --- |
| **Activity Procedures:** |

1. Using direct instruction, present a simple double encryption of a message using addition for encryption and subtraction for decryption (example in [powerpoint](https://docs.google.com/presentation/d/14GAVk7lC8xunWGk_sc5XJi5flFDU4vtxExYoUOcc3zM/edit?usp=sharing))
2. Use this to transition your direct instruction lesson into an exploration of inverse operations and then inverse functions (Does not include full instruction on teaching inverse functions and operations)
3. Implement a lesson on inverse functions
   1. The lesson should give students an opportunity to discover inverse functions on their own, as they have already learned about inverse operations, but should include a time of note giving and clarification – so you are certain all students can identify which functions are inverses
4. Have students complete a worksheet finding inverse functions
5. Have students break up into their teams and spend 2 class periods creating their encryption systems and presenting them to the teacher who will check them to see if they meet the criteria

**Formative Assessments:** Link the items in the Activities that will be used as formative assessments.

Inverse function worksheet

**Summative Assessments:** These are optional; there may be summative assessments at the end of a set of Activities or only at the end of the entire Unit.

Sales pitch to teacher on their chosen encryption methods (may happen more than once if a critique is given during their explanation that they have to go back and fix)

|  |
| --- |
| **Differentiation:** Describe how you modified parts of the Lesson to support the needs of different learners.  Refer to Activity Template for details. |

Accommodations:

1. Provide a template/organizer that mirrors the example so that there is a clear example to work off of
2. Allow the choice of an oral pitch or a written pitch to explain encryption system

Extension

1. Must show how the best way to break each of your encryptions
2. Find a function that needs at least two decryption steps

|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info: kellyhiersche@gmail.com** | **Date: 07/03/2018** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Encryption with Algebra 2** | **Unit #: 1** | **Lesson #: 2** | **Activity #: 4** |
| **Activity Title: Make and Break the Encryptions** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **6 days** |
| **Estimated Activity Duration:** | **2 days (50 minute periods)** |

|  |  |
| --- | --- |
| **Setting:** | **Middlesboro High School (my classroom)** |

|  |
| --- |
| **Activity Objectives:** |

I can …

1. Use inverse functions and function composition to double encrypt and decrypt messages
2. Break double encryptions using knowledge of inverse functions

|  |
| --- |
| **Activity Guiding Questions:** |

1. How are encryptions broken using inverse function and function composition?
2. What is a man in the middle – how does he operate?

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| ☐ Asking questions (for science) and defining problems (for engineering) | ☐ Patterns |
| ☐ Developing and using models | ☐ Cause and effect |
| ☐ Planning and carrying out investigations | ☐ Scale, proportion, and quantity |
| ☐ Analyzing and interpreting data | ☐ Systems and system models |
| ☐ Using mathematics and computational thinking | ☐ Energy and matter: Flows, cycles, and conservation |
| ☐ Constructing explanations (for science) and designing solutions (for engineering) | ☐ Structure and function. |
| ☐ Engaging in argument from evidence | ☐ Stability and change. |
| ☐ Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| ☐ Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| ☐ Demonstrating Science Knowledge **(D)** |
| ☐ Interpreting and Communicating Science Concepts **(C)** |
| ☐ Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☐ Make sense of problems and persevere in solving them | ☐ Useappropriate tools strategically |
| ☐ Reason abstractly and quantitatively | ☒ Attendto precision |
| ☐ Construct viable arguments and critique the reasoning of others | ☒ Look for and make use of structure |
| ☒ Model with mathematics | ☒ Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):** |

**F-LEA4** Construct and compare linear, quadratic, and exponential models and solve problems: For exponential models, express as a logarithm the solution to *abct*= *d* where *a*, *c*, and *d* are numbers and the base *b* is 2, 10, or *e*; evaluate the logarithm using technology.

**F-IFB5** Interpret functions that arise in applications in terms of the context: Relate the domain of a function to its graph and, where applicable, to the quantitative relationship it describes

|  |
| --- |
| **Materials**: (Link Handouts, Power Points, Resources, Websites, Supplies) |

Worksheet to track all messages sent and received

Worksheet to track any broken encryptions

Flashdrives with Java code to allow game to be player

|  |
| --- |
| **Teacher Advance Preparation:** |

Make sure the java runs on all computers

Edit individual codes to reflect progress of each group/team

|  |
| --- |
| **Activity Procedures:** |

1. Explain the rules (provided with source code on Wiki)
2. Give teams 5 minutes to plan a strategy of playing
3. Let students play game, teacher can monitor by watching the server code

**Formative Assessments:** Link the items in the Activities that will be used as formative assessments.

Results of the game count as a quiz grade – graded on curve: 1st team gets 100, 2nd 95, and on and on (feel free to change grading schedule as you want)

**Summative Assessments:** These are optional; there may be summative assessments at the end of a set of Activities or only at the end of the entire Unit.

N/A

|  |
| --- |
| **Differentiation:** Describe how you modified parts of the Lesson to support the needs of different learners.  Refer to Activity Template for details. |

Accommodations:

1. Changed point amounts / time to play depending on individual student accommodations

Extensions

1. Try to gain all your points by breaking other peoples’ codes