**TEAM PROJECT REPORT Securing Cyberspace Submitted To**

**The RET Site**

**For**

**RET Site on “Challenge­Based Learning and Engineering Design Process Enhanced**

**Research Experiences for Middle and High School In­Service Teachers”**

**Sponsored By**

**The National Science Foundation**

**Grant ID No.: EEC­1404766**

**College of Engineering and Applied Sciences**

**University of Cincinnati, Cincinnati, OH**

**Prepared By**

**Participant #1: Benjamin Dougherty, Purcell Marian High School, Cincinnati, Ohio**

**Participant #2: Amanda Sopko, Indian Hill Middle School, Cincinnati, Ohio**

**Approved By:**

**Dr. John Franco**

**Electrical Engineering and Computing Systems Department College of Engineering and Applied Sciences University of Cincinnati**

**Reporting Period: June 15 ­ July 30, 2015**

**ABSTRACT**

Cryptography utilizes a variety of principles from mathematics to ensure that transmitted messages remain confidential, are unmodified in transit by third parties, and arrive at the intended destination with complete confidence that the sender is who it claims to be. The purpose of this research is to determine the best pedagogical methods for introducing secondary students to cryptography in particular and, more generally, key elements of cybersecurity, how cryptography is used to secure cyberspace, and the mathematics that supports modern cryptographic systems. The hypothesis of this research is that early exposure to well­formed and engaging activities will increase the number of students entering higher

education programs in cryptography and cybersecurity and later, the workforce as cybersecurity professionals. The importance of this research cannot be overstated as increasing the size of

the qualified and competent cybersecurity workforce has become a national priority. To increase student interest in this field, teachers will implement mathematics­based units that use games and activities to engage students. Teachers will collect data on student interest in cybersecurity and understanding of cryptological and mathematical concepts and skills before and after the units. Students will use the Engineering Design Process to iteratively refine secure

cryptographic protocols for sending messages that are encrypted, unmodified in transit, and authenticated.

**KEY TERMS: cryptography, cybersecurity, teaching and learning, pedagogy, mathematics**

**Table of Contents**

**Abstract………………………………………………………………..……………………………...……**

**1**

**Table of**

**Contents…………………………………...………………………………………..…….…….2**

**Introduction……………………………………………………………………………..………………...**

**3**

**Literature**

**Review…………………………………………………………………………….……...……4**

**Goals and**

**Objectives………………………………………………………………………………....…8**

**Research Study**

**Details………………………………………………………………………………....8**

**Research**

**Results………………………………………………………………………………………..10**

**Research**

**Conclusions………………………………………………………………………………....10**

**Recommendations for Further**

**Study………………………………………………………………..11**

**Classroom Implementation**

**Plan……………………………………………………………………..12**

**Acknowledgements………………………………………………………………………………….....2**

**0**

**Bibliography……………………………………………………………………………………………..2**

**0**

**Appendix**

**I………………………………………………………………………………………………..22**

**Appendix**

**II……………………………………………………………………………………………....29**

**Appendix**

**III……………………………………………………………………………………………...60**

**1. INTRODUCTION**

For thousands of years, humans have spent considerable effort on developing methods to securely transfer sensitive data from one entity to another. Despite this, there have been many notable security failures, some of which have changed the course of history. From these experiences, governments have been motivated to continually improve their cryptographic systems. But now, increasing reliance on technology severely threatens our ability to secure transmissions and data and creates an urgent need to develop new systems and practices as the speed at which technology is being adopted has outpaced the speed at which cybersecurity professionals can secure those technologies. Currently, the cybersecurity workforce lacks adequate training and numbers to close this gap. To increase the competent workforce, students need to be exposed to cryptographic and security concepts earlier in their K­12 education. But, there is no state or federal approved curriculum for cybersecurity. For example,

the National Council for Teachers of Mathematics does not go into detail about the mathematics of cybersecurity. Even the College Board’s Advanced Placement Computer Science Course Description does not mention cybersecurity. The goal of this research is to provide a mathematical curriculum that is rich and engaging enough to encourage students to pursue a career in cybersecurity and guide state and federal agencies toward an approved curriculum in that field.

To accomplish this goal, interactive games and activities were designed to allow students to explore and develop mathematical algorithms and cryptographic protocols. The research began by examining methodologies currently used to increase interest in cybersecurity as well as student misconceptions on the nature of cybersecurity and career opportunities in

that field. Considering students’ prior knowledge and misconceptions, the research team developed two units of study to introduce and engage students in a series of activities to teach

central concepts in cryptography for middle and high school students. The units were designed to present these concepts to the students through a combination of hands­on and computer based discovery activities and games. Furthermore, each unit presents cryptosystems and their protocols with an underlying theme of ethical considerations.

**2. LITERATURE REVIEW**

Cryptography comes from the Greek words *cryptos* meaning hidden and *graphos* meaning writing. Therefore, cryptography is the study of hidden writing. Although humans have been using encryption methods to communicate secretly for thousands of years, the study of cryptography has become critically important to national security and private information in an increasingly digital world. However, there has been little research into best practices for teaching cryptography to students especially those in primary and secondary schools.

Furthermore, the mathematical concepts that underpin cryptographic systems can be complex and beyond the scope of the average citizen’s mathematical background, making it difficult to teach students these concepts. Much of the published work on teaching cryptography either focuses on higher level mathematics or teaching the systems and methods, with little to no middle ground. The teachers that participated in this project have observed that most teachers will not go beyond the required curriculum to teach a subject that they are not formally instructed in, consequently mathematics teachers are reluctant to include cryptography in their curriculum. Students are not well informed in the scope of cryptography, so many students do not know to inquire about the mathematics of cryptography. For all these reasons, there seems to be a dearth of research related to the best practices for teaching cryptography.

In 2004, a group of engineering professors designed a day­long engineering design challenge that included a cryptographic component as part of a conference. Students were broken into teams and had two challenges: 1) to build a water rocket, and 2) to decrypt a launch

code allowing them to launch their rocket before the opposing team was able to launch its rocket. There was a workshop in the middle of the day to educate students about basic cryptographic and cryptanalytic methods to prepare them for that portion of the challenge. In a self­reported survey, students indicated that they gained confidence in their ability to break ciphers after attending the workshop and using the associated skills during the activity.

In 2007, Long­Yuan Yan published a study of a student cryptography exercise used with high school students in Taiwan. Before the activities, 60% of students thought that cryptography was very difficult and 56% of students thought that cryptography was not easy to understand. After the activities, 41% of students liked using the activities as learning tools; 44% of students thought that cryptography was simple; 24% of students thought that cryptography was easy to understand.

Also in 2007, Robert Lewand published “Cryptography in a Liberal Arts Setting”, in which he describes a course he taught at Goucher College. In the article, he mentioned Simon Singh’s *The Code Book* as an engaging resource for his students in his cryptography course. This text by Singh is filled with rich material, and makes both the history and concepts of cryptography accessible and interesting to people regardless of their level of mathematical knowledge. The team found this book to be excellent background source material, and provided many good talking points in various presentations.

Students have many misconceptions concerning the field of cryptography. In a 2009 study by Taub, Ben­Ari, and Armoni, students were presented with a series of eighteen to twenty computer science activities, including cryptography, that did not require the use of a

computer. A pre­study survey found that students believed computer science (CS) to be tedious and boring. The students overwhelmingly believed that CS was a male dominated field only for

smart, anti­social people that consisted of installing hardware, programming, and required no creativity.

Perhaps the greatest limiting factor to exposing students to the study of cryptography is the lack of teacher knowledge in this field. Bachman, Brown, and Norton detailed a lesson involving the passing of M&Ms from one student to another through several classmates illustrating the Diffie­Hellman Exchange and the need for set protocols in order to ensure safe delivery to the correct recipient. The authors detail the use of modular arithmetic in a clear, concise manner. To ensure delivery of information to mathematics teachers, the authors published their work in the September 2010 edition of *The Mathematics Teacher*. However, this article failed to make connections between the Diffie­Hellman exchange and modular arithmetic. Earlier, Hall attempted to disseminate the mathematics behind cryptography in an article published in the March 2003 issue of *The Mathematics Teacher* which details the use of calculators in order to expose students to cryptology. Beyond those two articles, the research team working on this project could not find articles to support teacher understanding in this area.

In 2014, Frank Katz published a study based on a cryptography course he taught at

Armstrong State University to undergraduates. He taught the course in the Fall semester of

2011 and 2012. In 2011, he used more traditional methods of teaching, and in 2012 he implemented more interactive exercises. On a student self­reporting survey, responding to the statement: “I understand the basic principles of cryptography and can perform several very basic cryptographic schemes such as substitution and transposition ciphers”, there was an

11.11% increase in positive response after the 2011 course, as opposed to a 48.81% increase in positive response after the 2012 course. Similarly, when responding to the statement: “I can describe the differences between symmetric and asymmetric encryption”, there was only a

14.29% increase in positive response after the 2011 course, compared to a 49.38% increase in

understanding after the 2012 course. Findings seem to indicate that interactive exercises helped more students increase their understanding of cryptographic systems.

Also in 2014, Sikha, et. al. published an article emphasizing the need for interactive pedagogical tools to teach cryptographic concepts. They wrote, “To the best of our knowledge, interactive pedagogical tools available for learning the complex mathematical theories behind cryptography is very less.”

Even fewer studies can be found on the introduction of cryptography to middle school students. During the 4th IEEE Integrated STEM Education Conference, Konak presented a Cyber Security Discovery Day, for middle school students. This day long cryptography workshop guided students through several hands­on activities that introduced students to the field of cryptography. The results were measured on the students’ attitudes towards cryptography.

While most students enjoyed the activities provided, many believed cryptography was too challenging or they felt they lacked the computer skills necessary to pursue a career in this field. There was no mention of mathematics integration.

Finally, the 2008 article, “The Career Development Needs of Rural Elementary School Students”, noted the importance of exposing students to career options as early as fourth grade. According to this study, a good career curriculum consists of five key components: individual interpretations and feedback, modeling, a network of support, information on real­world applications, and written exercises. One aspect in the classroom implementation of career development is to learn areas the students are curious about and provide opportunities to explore their curiosities.

Reviewing the literature and considering the importance of national security, it is clear that cryptography is severely neglected in middle and high school curricula. There are many reasons for this deficiency: lack of teacher understanding of cryptography limiting buy­in, lack of

state or national standards that incorporate the inclusion of cryptography in schools, and lack of research on best practices for instructing students in this field. What research has been done for introducing cryptography in a K­12 setting focuses primarily on hands­on activities that illustrate the protocols, but fails to incorporate the mathematics involved. Due to a full and challenging mathematics curriculum and teachers’ focus on state testing, these activities are often neglected if they do not appear to meet crucial standards. Furthermore, failure to teach cryptography beginning at the middle school level limits students’ exposure to the field at a time when they should begin considering a career path.

**3. GOALS AND OBJECTIVES**

The goal of this research is to develop best practices for engaging students in cryptography though its mathematical foundations. The research team plans to do this by examining best practices in teaching and learning and developing student­friendly activities that convey the foundational concepts of cryptography in order to increase student interest in cryptography. The team will develop and deliver two instructional units rooted in mathematics and logic at the middle school and high school level. Finally, the research team plans to examine dissemination methods to increase teacher understanding and buy­in to incorporating cryptography into their curriculum.

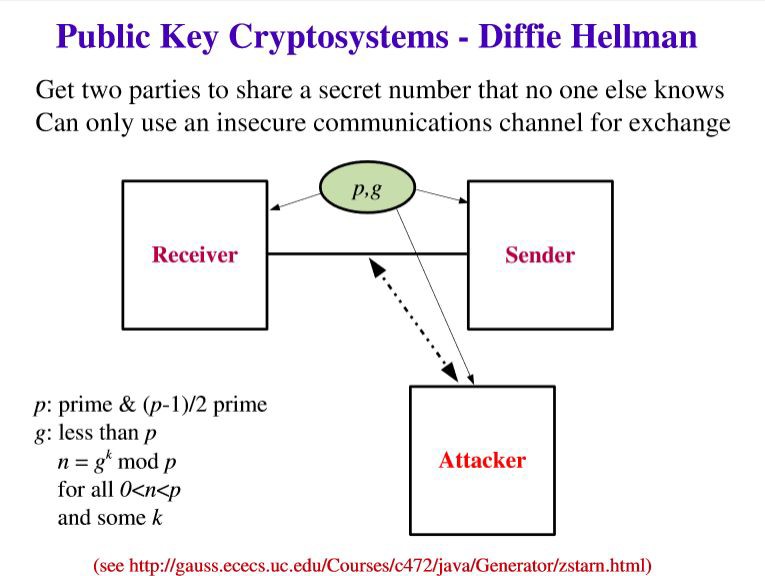
**4. RESEARCH STUDY DETAILS**

Expanding knowledge of higher mathematics and its applications such as cryptography to students is of crucial importance to protect the security of individuals and nations. There are several challenges to introducing students to the field of cryptography: students lack awareness of the important role cryptography plays in their everyday lives, they have little or no exposure to the field of cryptography in a traditional classroom setting, and teachers lack sufficient understanding of cryptographic protocols and the related mathematics.

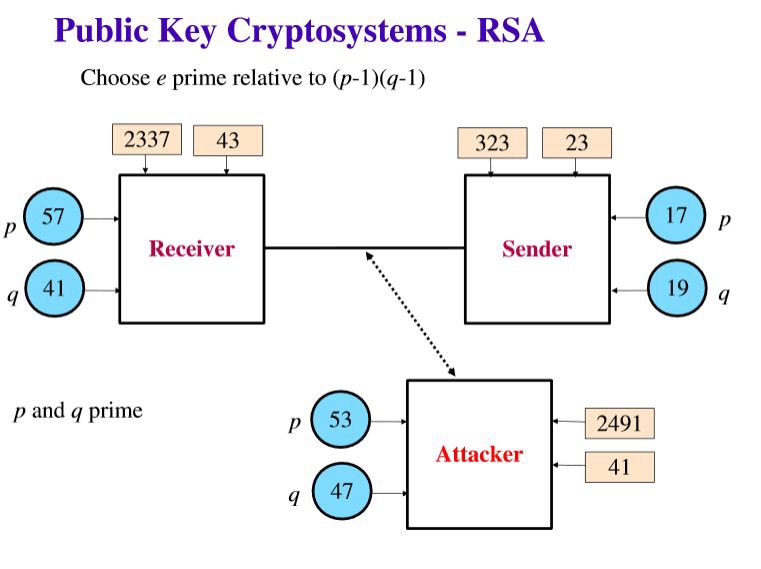
In order to develop better practices for instructing cybersecurity to engage students, the team participated in a series of training sessions on the principles of cryptography. Drawing on the diverse backgrounds of the team members, activities that engage students in the mathematics of cryptography were developed and refined through dialogue. These activities were derived from lessons that others have published, previous classroom experiences, and a series of brainstorming sessions.

Throughout the training, the team continued to discuss the underlying theme of ethics and the role it plays in the teaching and learning of cryptography. In order to convey the importance of ethics to students, activities were developed to incorporate historical events and dilemmas that involved encrypting information. The teachers developed activities dedicated to discussions focused on understanding the sometimes grave decisions surrounding ethical situations.

One objective is to build student interest in cryptography through realistic and engaging activities. A series of hands­on activities serve as a hook that demonstrates important cryptographic systems and protocols. Protocols and algorithms used as tools to accomplish everyday tasks can inform students of the magnitude of the impact cryptography has on their daily activities. AES and 3DES protocols and schemes such as Diffie­Hellman (see Fig. 1) and RSA (see Fig. 2) are ideas crucial to understanding present day encryption and decryption. It is important that students understand how these protocols work. As a result, the final challenge in each of the units requires students to develop a set of protocols to successfully transmit important data without interception. See Appendix I for detailed descriptions and examples of modular arithmetic, Diffie­Hellman, and RSA.



**Figure 1: Visual representation of the Figure 2: Visual representation of the RSA Exchange.**



**Diffie Hellman Exchange. Unless all Without authentication, this exchange is susceptible information exchanged is also made to attack.**

**public, this method is susceptible to attack.**

**5. RESEARCH RESULTS**

The research yielded two mathematics units intended for middle and high school students. The curriculum includes both the theoretical and practical aspects of cryptography, as well as activities to generate student interest in encryption. The activities address three

essential tenets of cryptography: authentication, confidentiality, and message integrity.

The teachers involved in this research were trained in cryptographic systems and the mathematics involved in order to differentiate the material for middle school and high school students. The units will give the students an authentic experience with cryptography and its uses in securing data.

After the units are implemented, the teachers plan to review and improve their units with the expectation of delivering easy to follow instructions to more teachers for implementation. The research team also plans to disseminate findings through professional writings and professional development workshops and conferences for teachers.

**6. RESEARCH CONCLUSIONS**

It is the belief of the research team that teaching cryptography as an application of mathematics will increase interest in both mathematics and cryptography. In order to make

cryptographic topics more accessible to students, a series of hands­on activities have been researched and developed to make these abstract ideas concrete. These activities will not only illustrate cryptographic protocols, but also include in depth exploration of the mathematics involved.

The proposed activities introduce students to the foundational ideas of cryptography, mathematics, and ethics through the use of technology. The activities combine a series of interactive activities involving manipulatives and applets coded specifically to meet the students’ needs at their respective grade levels.

The teachers in this project have come away with a greater understanding of cryptography and are excited to implement their units with students. This energy will be projected to the students which will increase their interest in the discipline. Perhaps most importantly, these units will not only introduce students to the field of cryptography, but also spark interest in pursuing a career in computer science.

**7. RECOMMENDATIONS FOR FURTHER STUDY**

The team conducted research during the summer break. As a result, the teachers were unable to implement their units in their respective classrooms. However, pre and post surveys, which include space for students to comment on ways to improve the activities, were created to measure students’ knowledge of content as well as attitudes toward the field of cryptography. Upon completion of the units, the teachers plan to review the surveys and adjust their units for future implementation.

The units were created to give students a glimpse of the field of cryptography. Further studies can be conducted that give students a more intense experience over a longer period of time. More activities provided over several years of schooling could improve understanding of

the field. Periodic instruction over several years ensures continuous exposure and keeps the possibility of a career in computer science accessible and attainable.

Longitudinal studies of several groups of students exposed to a curriculum rich in cryptographic concepts over a period of time beginning in middle school should be conducted to measure increased interest in and pursuit of a career in computer science.

**8. CLASSROOM IMPLEMENTATION PLAN**

The two teachers involved in this research developed units to engage students in cryptographic concepts at the middle school and high school level. Amanda Sopko and Ben Dougherty designed units for their respective classes to teach cryptography. The underlying goal that motivated their individual unit designs was to generate interest in the field of

cryptography. Activities were organized to inform students about elements of cyber security they interact with on a daily basis such as text messages, email, and private chats with peers.

These units include a historical aspect which encourages students to examine the historical significance of cryptology and its impact on their personal lives today. Activities were designed such that students evaluate messages sent over networks through secret and public keys and use the information to send a message through a third party without divulging the information in the message.

During the challenge activity, students are encouraged to discover and ask how to encrypt or decrypt data in order to protect their data communications. The exercises in each unit display the invasive nature that code breaking and losing confidential information has on the security of data. The students will also participate in detailed discussions on the ethical use of their newfound knowledge of cryptography.

**8.1 Amanda’s Unit:**

Amanda teaches and coordinates the STEM program at Indian Hill Middle School in Cincinnati, OH. Her unit, The Mathematics of Cyber­Security and Cryptography, was designed to be taught over thirteen fifty minute sessions to sixth grade STEM students studying an advanced pre­algebra curriculum. This class is expected to have approximately thirty students on the roster. Portions of this unit will also be taught to her general sixth grade classes with a total of approximately thirty students combined. The unit has built in flexibility to be spread out over a longer period of time or over the course of several academic units. The unit covers Common Core State Standards spanning

from fifth grade to seventh grade.

The big idea of this unit is to understand and apply protocols to ensure the data we send and receive over cyber space is kept safe from attackers. The hook of this unit intends to yield the essential questions:

● How is cryptography used in my everyday communications?

● What mathematics is used in cryptography?

● How do you encrypt/decrypt data?

● How do hackers steal data?

● How can I protect my data and communications?

The students are required to answer these questions in order to be successful when completing the final challenge. For this challenge, the students will work in teams to develop a set of cryptographic protocols for securely sending coins through a third

party messenger. Meanwhile, they will attempt to break the protocols of their rival teams. The team with the best protocols will amass the most wealth and win the challenge.

The Common Core State Standards for Mathematics addressed in this unit are:

● [CCSS.MATH.CONTENT.5.NF.B.4 Lesson 2. 3](http://www.corestandards.org/Math/Content/5/NF/B/4/)

Apply and extend previous understandings of multiplication to multiply a fraction or whole number by a fraction.

● [CCSS.MATH.CONTENT.6.NS.B.2 Lessons 1.2; 2.3; and 2.5](http://www.corestandards.org/Math/Content/6/NS/B/2/)

Fluently divide multi­digit numbers using the standard algorithm.

● [CCSS.MATH.CONTENT.6.EE.A.2.C](http://www.corestandards.org/Math/Content/6/EE/A/2/c/) [Lesson 1.2](http://www.corestandards.org/Math/Content/6/NS/B/2/)

Evaluate expressions at specific values of their variables. Include expressions that arise from formulas used in real­world problems. Perform arithmetic operations, including those involving whole­number exponents, in the conventional order when there are no parentheses to specify a particular order (Order of Operations).

● [CCSS.MATH.CONTENT.7.EE.B.4 Lesson 1.1](http://www.corestandards.org/Math/Content/7/EE/B/4/)

Use variables to represent quantities in a real­world or mathematical problem, and construct simple equations and inequalities to solve problems by reasoning about the quantities.

● [CCSS.MATH.CONTENT.7.SP.C.5 Lesson 2.3](http://www.corestandards.org/Math/Content/7/SP/C/5/)

Understand that the probability of a chance event is a number between 0 and 1 that expresses the likelihood of the event occurring. Larger numbers indicate greater likelihood. A probability near 0 indicates an unlikely event, a probability around 1/2 indicates an event that is neither unlikely nor likely, and a probability near 1 indicates a likely event.

● [CCSS.ELA­LITERACY.RI.6.1](http://www.corestandards.org/ELA-Literacy/RI/6/1/) Lesson 2.5

Cite textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text.

● [CCSS.ELA­LITERACY.W.6.1](http://www.corestandards.org/ELA-Literacy/W/6/1/) Lesson 2.5

Write arguments to support claims with clear reasons and relevant evidence.

The students will utilize the Engineering Design Process in order to complete this task. They will identify the problem in this challenge, gather information through the first three activities in the unit, and design, test, & improve a set of protocols for sending their coins. Finally, the students will be required to share their final process in a presentation format and through writing in their Engineering Design Notebooks.

The unit begins with a hook that requires the students to pass secret messages

in two rounds. Round one allows them to exchange information using the method of their choice. Round two highlights the importance of a secure system as they are required to share their secrets on a posterboard on the classroom wall. The students will see the problem and develop the big idea and essential questions followed by research on historical and present day uses of cryptography.

The first activity uncovers flaws in a symmetric system which leads students to explore public or asymmetric methods to exchange secret data. The students begin this investigation with a double lock box and develop a protocol for sending a message from student A to student B with two padlocks. Student A locks a message in the box but keeps the key. Student B also has a lock and key. This activity is the springboard for introducing Diffie­Hellman, RSA, and the Chinese Remainder Theorem. The initial lockbox activity is revisited at the end of this lesson and a third party, E, is given a lock and key and attempts to intercept the message sent by student A. This leads to a discussion on the Man in the Middle Attack.

For the third activity, students learn protocols to prevent cyber attacks. Students will be presented with Ali Baba’s Cave as a hook to build engagement in the topic of authentication. The idea that Ali Baba’s Cave conveys is zero­knowledge proof which is

the use of public knowledge to authenticate a person. The discussion following this activity focuses on the question: “why is it important to authenticate a message?”.

The fourth activity presents the students with a challenge game. Students work in teams to develop protocols using cryptographic methods in order to collect the most coins. Students are required to follow the Engineering Design Process to create and evaluate their protocol design. At the game’s end, the students will write about and discuss protocols and the importance of having a strong system.

Upon completion of activity four, the students participate in a final activity focused on ethical uses of cryptography. The students will be provided with a series of situations and determine how to ethically respond.

The students will be assessed on a series of Core 6 writing tasks to be completed throughout the unit. They will also be assessed on work completed in their Engineering Design Notebooks using the Engineering Design Process as their guide. Finally, students will be assessed on their final presentation and ability to explain their understanding of the important role ethics plays in cryptography.

At the beginning and end of this unit, the students will participate in a brief survey to assess their attitudes towards cryptography as well as their ability to use the math content presented through this unit. It is expected that these students will show no less than 80% growth on the math content as well as increased attitudes towards cryptography. It is also expected that no less than 50% of the students participating in this unit will indicate cryptography as a possible career choice.

**8.2 Dougherty Unit**

The title of this unit is “Cyber Security”. It will be taught to senior Pre­Calculus students in the first quarter of the academic year. Meeting once per day for 45 minutes,

the unit should take approximately three weeks to complete. The big idea for the unit is digital security and securing internet communications. The challenge for students will be to work in teams to create their own code book to use as part of a war games simulation at the end of the unit. Some of the guiding questions for the challenge will be:

● How can I securely transmit data over an open channel?

● How can I know the true identity of the person I’m communicating with over an open channel?

● How can I intercept and break my opponents’ codes?

This unit was planned because cryptography can be related to functions and their inverses, which are an essential element of the Pre­Calculus curriculum. The pre­assessment and post­assessment both include questions about function inverses to measure student learning outcomes. The secondary goal of this unit is to get students interested in computer science, cybersecurity, and cryptography, and to expose them to the career possibilities in these fields. This unit will address the following standards:

● HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it.

● HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales.

● HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).

● HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes

the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).

● HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.

● HS.F.BF.4.b.c ­ Find inverse functions.

● HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.

In the first activity, students will be introduced to the idea of cyber security and why it is important. They will brainstorm essential questions, and learn about substitution ciphers (Caesar ciphers in particular). This activity will also include an introduction to cryptanalysis (codebreaking), focusing on methods for breaking monoalphabetic ciphers (e.g. frequency analysis). In this activity, students will draw connections between monoalphabetic ciphers and functions, and understand decryption of an enciphered message as the application of an inverse function.

The second activity will turn students’ attention to asymmetric encryption. Students will explore the Diffie­Hellman key exchange, the RSA encryption algorithm, common man­in­the­middle attacks, the mathematics of modular arithmetic that make asymmetric encryption work, and weaknesses of the RSA encryption algorithm.

The third activity is designed to get students thinking about the ethics involved in cybersecurity and cryptography. In groups, students will wrestle with current and historical ethical dilemmas surrounding cryptography and cybersecurity. Groups will present their dilemmas and resolutions to the class, and the class will have an opportunity for further discussion. This activity also provides opportunities for students to

review the major mathematical and cryptographic concepts and techniques learned in the first and second activities in preparation for the challenge.

The fourth activity, the challenge, is a multi­day war game simulation. Students will be divided into teams, and each team will create its own code book that will outline its unique cryptographic protocols that will enable it to communicate securely. In the game, the teams will be separated and will have to use the cryptographic systems in their code books to communicate vital game commands and information over open channels. At the end of each day, students will have an opportunity to refine their code books to improve their cryptographic systems.

Throughout the unit a variety of formative and summative assessments will be used. The unit itself will be bracketed by a pre­assessment/post­assessment that will measure student interest in cryptography as well as students’ understanding of the mathematics involved in the unit. In the first activity, the Caesar cipher note cards, student performance in the “head­to­head cipher breaking game”, and the short function inverse quiz will all be used as formative assessments. During the second activity, frequent whole class Q&A sessions along with a Diffie­Hellman written exercise, and the RSA activity Google documents will serve as formative assessments to check student understanding. In the third activity, student presentations and class discussion will be used as an assessment to see how well they have understood the ethical dimensions of cryptography and cybersecurity. Finally, in the challenge, the fourth activity, students’ ability to encrypt and decrypt messages successfully, as well as their ability to break the opposing teams’ ciphers, will be formative assessments, and after the war games simulation is over, teams will present their code book used in the game and how they refined it as their summative assessment.

This unit will be implemented with approximately thirty students. It is expected that this unit will have a strong positive impact on student learning growth because: 1) Students are relatively unfamiliar with cryptography and modular arithmetic; 2) the interactive approach taken to teaching the material should increase student interest, retention, and understanding; and 3) students will be applying what they have learned to accomplish a task.

**9. ACKNOWLEDGEMENTS**

We would like to thank the following people for sharing their time, wisdom, and patience throughout this project:

Dr. John Franco, Faculty Mentor, Professor of Computer Science

Amin Makani, Graduate Research Assistant

Nicholas Maltbie, High School Research Assistant

RET is funded by the National Science Foundation, Grant ID # EEC­1404766. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

**10. BIBLIOGRAPHY**

[1] Bachman, D.J.,Brown, E. A.,and Norton, A.H. (2010). "Chocolate Key Cryptography."

*Mathematics Teacher,* 104(2), 100­104.

[2] Beutelspacher, A (1994). *Cryptology: An introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding and Safeguarding Described Without any Arcane Skullduggery but not Without Cunning Waggery for the Delectation and Instruction of the General Public.* The Mathematical Association of America, Washington, D.C.

[3] Dowling, T. (2006). “The Design and Evaluation of a Cryptography Teaching Strategy for

Software Engineering Students.” *European Journal of Engineering Education*, 31(5), 593­606.

[4] Hall, M. (2003). "Sharing teaching ideas: Calculator cryptography." *The Mathematics*

*Teacher,* 96(3), 210­212.

[5] Holden, J. (2004). “A Comparison of Cryptography Courses.” *Cryptologia*, 28(2), 97­111. [6] Holden, J., Layton, R., Merkle, L., Hudson, T. (2006). “Underwater Hacker Missile Wars: A

Cryptography and Engineering Contest.” *Cryptologia*, 30(1), 69­77.

[7] Hsin, W. (2005). "Teaching Cryptography to Undergraduate Students in Small Liberal Art Schools." *Proceedings of the 2005 Information Security Curriculum Development Conference: September 23­24, 2005*, KSU Center, Kennesaw State University Kennesaw, GA, 38­42.

[8] Katz, F.H. (2014). “A Comparison of Different Methods of Instruction in Cryptography.”

*Information Security Curriculum Development Conference*, Kennesaw, GA.

[9] Konak, A. (2014). “"A cyber security discovery program: Hands­on cryptography”, 4th

IEEEIntegrated STEM Education Conference, Princeton, NJ.

[10] Leward, R. (2007). “Cryptology in a Liberal Arts Setting.” *Mathematics and Computer*

*Education*, 41(3), 211­218.

[11] Schembari, P. (2007). “’Hands­On Crypto’: Experiential Learning in Cryptography.” *Proceedings of the 11th Colloquium for Information Systems Security Education: June 4­7, 2007*, Boston University, Boston, MA, 7­13.

[12] Sikha, O., Kuchithra, M., Prabha, P., Soman, K.P. (2014). “An Interactive Visualization Tool for the Interpretation of Mathematical Concepts behind Public Key Cryptography.” *International Journal of Computer Applications*, 90(5), 36­39.

[13] Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum*

*Cryptography*. Doubleday, New York, NY.

[14] Trigui, M., Daniyal, A. (2012). “Learning the Related Mathematics to Cryptography by

Interactive Way.” *International Journal of Modern Education and Computer Science*, 2, 8­14.

[15] Wood, C., Kaszubowski, Y. (2008). "The Career Development Needs of Rural Elementary

School Students." *The Elementary School Journal,* 108(5), 431­444.

[16] Yan, L. (2007). “Teaching Cryptography Activity in Taiwan’s High Schools.” *Supporting*

*Learning Flow through Integrative Technologies*, IOS Press, 553­560.

[17] Yang, L., Kizza, J., Wang, A., Chen, C.H. (2011). “Develop Case Studies to Teach Cryptography in a Collaborative Environment.” *Proceedings of the 2011 International Conference on Frontiers in Education Computer Science & Computer Engineering*, 2011

International Conference on Frontiers in Education Computer Science & Computer Engineering: July 18­21, 2011, Las Vegas, NV, 542­544.

**11. APPENDIX I**

**11.1 Modular Arithmetic**

Modular arithmetic is arithmetic within a defined range of numbers. The range is zero (inclusive) to the modulus (exclusive) unless otherwise specified. If a value is out of the range, it will “wrap around” to fit within the range. The “wrapping” is defined as if any number a is x greater than the modulus then a is x in that specific modulus. For example, if we consider 10 modulus 7, 10 is 3 units greater than 7, so 10 modulus 7 is 3. Operations are only completed in integers so decimal values are not used in the

modulus. An example of this is time of day which is counting in modulus twelve (but the range is [1, 12] because zero is not used). For example, if it is nine in the morning, in five hours it will be three in the afternoon (9 + 5 = 3). This is why modular arithmetic is sometimes referred to as “clock arithmetic”.

Modular arithmetic can also be used as a mathematical operator. When the operator is used, it is referred to as “modulus” or “mod”. To compute any number a modulo any other number b, as long as a is greater than zero, the result will be the remainder from dividing a by b. For example, 87 mod 45 = 42 and 87 divided by 45 has a remainder of 42.

**11.2 Diffie­Hellman**

Diffie­Hellman is a secure way to establish a shared secret between two entities communicating over a public network. The shared secret can then be used as the basis of some encryption method for further communication. Figure 3 below illustrates an example of the exchange.

Step 1: The two communicating entities first agree upon a large prime number (n) and a generator (g) such that g is a generator mod n (i.e. The sequence of values g^c mod n,

where c is the sequence 1,2,3,...,n­1, produces all the values from 1 to n­1 without repetition.). These values are public and visible to all.

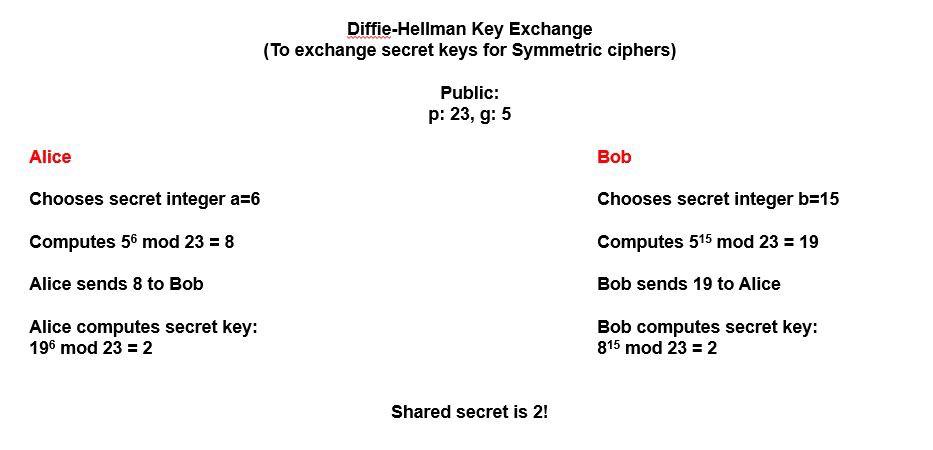
Step 2: Entity 1 (Alice) then selects a secret integer (a) and calculates its public key as ga mod n. Likewise, entity 2 (Bob) selects a secret integer (b) and calculates its public key as gb mod n. Now, each entity shares its public key so both entities know the other’s public key.

Step 3: Alice has its own secret integer(a) and public key of Bob (gb mod n). She computes the value of Bob’s public number raised to her integer (a) mod (n), ((gb mod n)a mod n), which is same as gab mod n.

Step 4: Similarly Bob also has his own secret integer (b) and public key of Alice (ga mod n). He computes the value of Alice’s public number raised to his secret integer (b) mod (n), ((ga mod n)b mod n), which is same as gab mod n.

Thus, both the entities have established a shared secret key (gab mod n) which can be

used with encryption methods to communicate secretly, and neither has divulged their secret number.



***Figure 3: Example of the Diffie Hellman Exchange***

**11.3 RSA**

The RSA cryptosystem allows for public­key encryption. It is used to send sensitive data over an insecure network. RSA is an asymmetric system that was created by Ron Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology in 1977 to utilize two different keys, one public and one private.

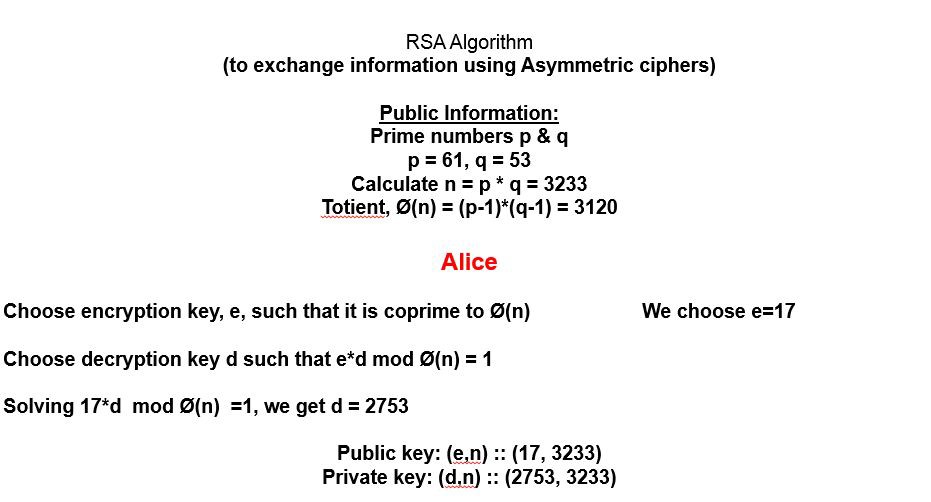
Figures 4 and 5 will be used to help illustrate the exchange.

Step 1: Select prime numbers (p and q) and calculate *n* by multiplying p\*q. Step 2: Find the totient of n by multiplying (p­1)\*(q­1)

Step 3: Alice chooses an encryption key and uses the variable *e* that is coprime to the totient of *n*. Numbers that are coprime do not share a common factor other than 1. In the example below, Alice, chose 17. This number and the number she calculated for *n* become her public key. Alice will post this information publically so that everyone can

see it.

Step 4: Alice also chooses a decryption key represented by the variable “d” so that when she calculates e\*d mod Øn the result is 1. The number she finds for “d” and “n” will become her private key.



***Figure 4: Example of the RSA Exchange. This illustration demonstrates how to derive the public and private key for the recipient of an encrypted message.***

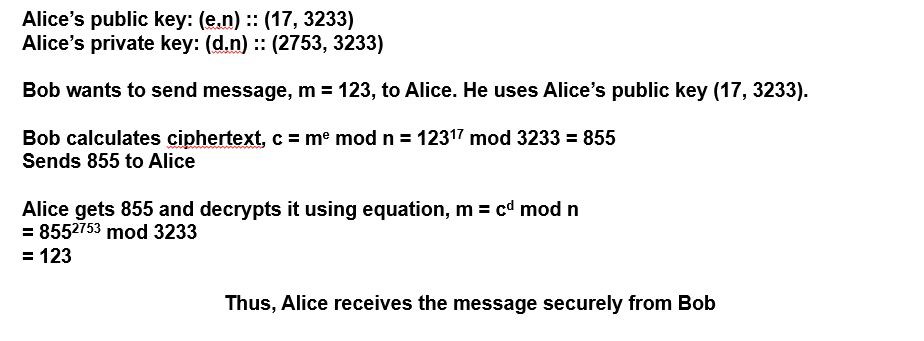
If Bob wants to send a message, 123, to Alice, he will use Alice’s public key to encrypt his message.

Step 1: Bob raises his message to the *e* power that he received from Alice then mod *n*

which was shared publicly.

Step 2: Bob shares his resulting answer, *c*, from step 1 to Alice publicly.

Step 3: Alice decrypts Bob’s message using her private key. She does this by taking the information sent from Bob, *c*, raised to the *d* she calculated earlier mod *n*. If all calculations were performed correctly, the result of this calculation is the message Bob intended to send.



***Figure 5: Example of the RSA Exchange. This illustration demonstrates how to encrypt and decrypt a secret message.***

**11.4 Chinese Remainder Theorem**

The Chinese Remainder Theorem is based on a problem enumerated in Chinese mathematical texts dating back to the 3rd to 5th centuries AD. There exists a number x that when divided by 4 has a remainder of 1; divided by 5 has a remainder of 2; and divided by 7 has a remainder of 3. The goal is to find the smallest number x that satisfies the conditions. For an example as simple as this, an exhaustive method would be sufficient, but there is a formula for finding the number under any conditions. Let’s call

the remainders a1 = 1, a2 = 2, a3 = 3 (it is purely accidental that the remainders match the subscripts here).

Step 1: First calculate a value for M, which is the product of all the divisors (4\*5\*7 = 140

= M).

Step 2: For each divisor, calculate a Mi, such that M1 is M divided by the first divisor, M2 is M divided by the second divisor, M3 is M divided by the third divisor, and so on for all the divisors…

M1 = 140/4 = 35

M2 = 140/5 = 28

M3 = 140/7 = 20

Step 3: Find yi such that y1 is the inverse of M1 mod the first divisor, and so on for all divisors.

y1\*35 = 1 (mod 4) … y1 = 3 y2\*28 = 1 (mod 5) … y2 = 2 y3\*20 = 1 (mod 7) … y3 = 6

Step 4: Sum all of the terms Mi\*yi\*ai. M1\*y1\*a1 = (35)(3)(1) = 105

M2\*y2\*a2 = (28)(2)(2) = 112

M3\*y3\*a3 = (20)(6)(3) = 360

105 + 112 + 360 = 577

Step 5: Take the sum from step 4 modulus M.

577 mod 140 = 17

To check our answer, we see if 17 meets the initial requirements of the problem…

17 divided by 4 has a remainder of 1

17 divided by 5 has a remainder of 2

17 divided by 7 has a remainder of 3

**11.5 Finding the Modular Multiplicative Inverse**

The inverse of a number n mod m is that number which, when multiplied by n and divided by m gives a remainder of 1.

Example: Find the multiplicative inverse of 7 mod 5. (i.e. What number times 7, divided by 5, gives a remainder of 1?)

1\*7 mod 5 = 2

2\*7 mod 5 = 4

3\*7 mod 5 = 1

Thus, 3 is the modular multiplicative inverse of 7.

**11.6 Zero­knowledge Proof**

Zero­knowledge Proof is a protocol that allows one person to prove to another person that s/he has a secret, without actually divulging the secret.

This protocol can best be illustrated by the example of Ali Baba’s Cave. Imagine you are standing at the mouth of a cave. Inside the cave is a locked door hidden behind a wall. Ali Baba is the only person in the world with a key to the door. As you are standing at the mouth of the cave, you are approached by a person claiming to be Ali Baba. However, he does not want to give up his key. To determine if he is Ali Baba, you decide to have Ali Baba go down into the cave and chose to stand on one side of the door. Once he is in place, you go into the cave and ask him to come out on a particular

side. If he is Ali Baba, he will be able to do this one hundred percent of the time because if he is on the opposite side, he will simply unlock the door to come out the correct side. However, an imposter only has a fifty percent chance of coming out on the side you chose. This process must be repeated increasing the probability of Ali Baba being who he claims until the verifier is satisfied.

**12. APPENDIX II: SOPKO UNIT**

**Name: Amanda Sopko Contact Info:**

[**amanda.sopko@ih.k12.oh.us**](mailto:amanda.sopko@ih.k12.oh.us)

**Date: 6/29/15**

**Unit Number and Title: #1 The Mathematics of Cyber­Security and Cryptography**

**Grade Level: 6**

**Subject Area:**

**Pre­Algebra**

**Total Estimated Duration of Entire**

**Unit:**

**13 ­ 50min. sessions**

**Note: The lessons in this unit can be taught in isolation or over a period of time throughout an entire unit. You do not need to stop teaching in order to implement this unit. Teach these lessons as they flow with your overall curriculum.**

**Part 1: Designing the Unit**

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

[**CCSS.MATH.CONTENT.5.NF.B.4 Lesson 2. 3**](http://www.corestandards.org/Math/Content/5/NF/B/4/)

**Apply and extend previous understandings of multiplication to multiply a fraction or whole number by a fraction.**

[**CCSS.MATH.CONTENT.6.NS.B.2 Lessons 1.2; 2.3; and 2.5**](http://www.corestandards.org/Math/Content/6/NS/B/2/)

**Fluently divide multi­digit numbers using the standard algorithm.** [**CCSS.MATH.CONTENT.6.EE.A.2.C**](http://www.corestandards.org/Math/Content/6/EE/A/2/c/) [**Lesson 1.2**](http://www.corestandards.org/Math/Content/6/NS/B/2/)

**Evaluate expressions at specific values of their variables. Include expressions that arise from formulas used in real­world problems. Perform arithmetic operations, including those involving whole­number exponents, in the conventional order when there are no parentheses to specify a particular order (Order of Operations).**

[**CCSS.MATH.CONTENT.7.EE.B.4 Lesson 1.1**](http://www.corestandards.org/Math/Content/7/EE/B/4/)

**Use variables to represent quantities in a real­world or mathematical problem, and construct simple equations and inequalities to solve problems by reasoning about the quantities.** [**CCSS.MATH.CONTENT.7.SP.C.5 Lesson 2.3**](http://www.corestandards.org/Math/Content/7/SP/C/5/)

**Understand that the probability of a chance event is a number between 0 and 1 that expresses the likelihood of the event occurring. Larger numbers indicate greater likelihood. A probability near 0 indicates an unlikely event, a probability around 1/2 indicates an event that is neither unlikely nor likely, and a probability near 1 indicates a likely event.**

[**CCSS.ELA­LITERACY.RI.6.1**](http://www.corestandards.org/ELA-Literacy/RI/6/1/) **Lesson 2.5**

**Cite textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text.**

[**CCSS.ELA­LITERACY.W.6.1**](http://www.corestandards.org/ELA-Literacy/W/6/1/) **Lesson 2.5**

**Write arguments to support claims with clear reasons and relevant evidence.**

**2. Unit Summary**

**The Big Idea (including global relevance):**

**How secure is the data you send via text messages, email, and private chats with friends? In this unit, students will use mathematics to examine the historical and personal significance of cryptology. Students will evaluate messages sent over networks through secret and public keys and use this information to send a message through a third party without divulging the information in the message.**

**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):**

**● How is cryptography used in my everyday communications?**

**● What mathematics is used in cryptography?**

**● How do you encrypt/decrypt data?**

**● How do hackers steal data?**

**● How can I protect my data and communications?**

**3. Unit Context – Check all that apply.**

**Justification for Selection of Content:**

☐​**Students previously scored poorly on standardized tests, end­of 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:**

**● Students will be given a secret message to pass along to their partner across the room. They can use any methods to deliver the message without speaking.**

**● Next students will pass a second message without the use of technology on a poster board on the wall.**

**● Groups will be given a historically or currently significant security breach to research and create a 5 minute video to present to the class.**

**● Develop essential questions for this unit of study.**

**The Challenge and Constraints:**

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

|  |  |
| --- | --- |
| **Description of Challenge (Either Product or Process is clearly explained below):** | **List the Constraints**  **Applied** |
| **Secret Agent: Design a message to pass from one secret agent to the other through a third party.** | **Materials: Calculator, Pen, Paper, Google Sheets**  **Time: 2 days to decrypt code.** |

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

**What is the best way to prevent digital data from being compromised?**

**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.**

**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. See Communicate Solutions below.**

**Identify the**

**Problem**

**Using a calculator and your engineering design notebook (EDN), develop a plan to cryptically send combinations to other members of your team to unlock your coins in your team box.**

|  |  |
| --- | --- |
| **Gather Information** | **Throughout this unit, the students will have gathered information on historical cryptographic “bloopers” and analyzed current methods of sending and receiving encrypted messages.** |
| **Select Solutions** | **They will summarize what they learned and work as a team to identify alternative plans to successfully pass their coin using the Diffie­Hellman or RSA methods of sending cryptographic messages.** |
| **Implement**  **Solution** | **Students will test their cryptographic plan through a simulated game of passing coins without allowing another team to intercept.** |
| **Evaluate Solution** | **Students will work in their EDNs evaluating their methods throughout the game. Breaks will be given throughout the game for teams to come together to evaluate their plan.** |
| **Refine** | **Teams can make adjustments to their plan as they play and during planned breaks for team meetings.** |
| **Communicate**  **Solution** | **At the end of the game, students will complete a brief writing activity in their EDNs and teams will create a report (in any format, presentation, video, ppt, prezi, etc...) to share with their results with the teams. A whole class discussion will take place on the methods that worked and why as well as the ethics of cryptography. Students will be allowed to continue this game during free time in class and a running public key will be**  **posted in the back of the room. Awards will be given periodically throughout the year for the teams who have acquired the most coins at which time, teams will be reset.** |

**What academic content is being taught through this Challenge?**

***Students will learn the engineering design processes, using the standard algorithm for division with remainders, and writing algebraic expressions from patterns, solve word problems leading to equations of the form px + q = r .***

**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.**

**Core 6 Writing Task to summarize learning along with the pros and cons of public vs.**

**Writing Rubric** ☐​**formative** ☐

**summative**

**private key systems. (During**

**Gather Information)**

**Student plans in the EDN. (After Select Solutions)**

**Student notes and**

**adjustments noted in the EDN. (In the Evaluate and Refine)**

**Summary writing in the EDN at the end of the project. (In Communicate Solution)**

**Final Group Presentation**

**Checklist** ☐​**formative** ☐

**summative**

**Checklist and Q/A with teacher.** ☐​**formative**

☐ **summative**

**Checklist and small group discussion.** ☐​**formative**

☐ **summative**

**Rubric for Group Presentation** ☐​**formative**

☐ **summative**

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

☐​**Has clear constraints that limit the solutions**

☐​**Will produce more 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: Students send digital data across networks multiple times on a daily basis. It is important to discuss the importance and methods of keeping this information safe and secret from a third party.**

**What activities in this Unit apply to real world context? Activity 1, 2, 3, and 4.**

**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: There have been multiple security breaches that have changed the course of history and greatly reduced the length of wars. These breaches have driven the systems we have in place today to keep all data including short text messages we share with peers out of public view. These changes have also provided a need for creating and enforcing strict laws for the sharing of data over a network. With these new technologies, there is also a great need for the direct instruction of ethical practices.**

**What activities in this Unit apply to societal impact? Activities 1 and 4.**

**Careers: What careers will you introduce (and how) to the students that are related to the Challenge? (Examples: career research assignment, guest speakers, field trips, Skype with a professional, etc.) Students will be introduced to the field of cryptography. They will be exposed to professionals in the NSA.**

**6. Misconceptions:**

**Data sent via email or text message are protected by passwords and can not be seen by anyone other than the intended recipient.**

**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.)**

**Lesson 1: What is Cryptography and why is it important? (7 days)**

**● Activity 1: Sharing Messages (3 days)**

**● Activity 2: Secret Key vs. Public Key Systems (4 days) Lesson 2: How do I keep my information safe? (6 days)**

**● Activity 3: Cyber Attacks (1 day)**

**● Activity 4: Collecting Coins Challenge (4 days)**

**● Activity 5: When is it ethical to use cryptography? (1 day)**

**8. Additional Resources:**

[**http://www.cryptoclub.org/**](http://www.cryptoclub.org/)

[**http://questgarden.com/140/45/8/120312062817/index.htm**](http://questgarden.com/140/45/8/120312062817/index.htm)

**9. Pre­Unit and Post­Unit Assessment Instruments:**

**Survey, Pre­ and Post Unit test.**

**10.** [**Poster**](https://drive.google.com/file/d/0B0sFwJqbpO8PZXhvQ1hyOE82U1E/view?usp=sharing) **11. 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 New Learning Standards for Science (ONLS)** |
| **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:**

**Common Core State Standards ­­ Mathematics (CCSS)**

**Standards for Mathematical Practice (Check all that apply)**

☐​**Make sense of problems and persevere in solving them** ☐​**Use appropriate tools strategically**

☐​**Reason abstractly and quantitatively** ☐​**Attend to 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**

**Part 2: Post Implementation­ Reflection on the Unit**

**Results: Evidence of Growth in Student Learning ­ After teaching the Unit, present the evidence below that growth in learning was measured through one the instruments identified above. Show results of assessment data that prove growth in learning occurred.**

**Please include:**

**● Any documents used to collect and organize post unit evaluation data. (charts, graphs and /or tables etc.)**

**● An analysis of data used to measure growth in student learning providing evidence that student learning occurred. (Sentence or paragraph form.)**

**● Other forms of assessment that demonstrate evidence of learning.**

**● Anecdotal information from student feedback.**

**Reflection: Reflect upon the successes and shortcomings of the unit. Refer to the questions posed on the Unit Template Instruction sheet. Describe how the actual Engineering Design Process was actually used in the implementation of the Unit.**

**Name: Amanda Sopko Contact Info:** [**Amanda.sopko@ih.k12.oh.us**](mailto:Amanda.sopko@ih.k12.oh.us)

**Date: 7/02/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : What is Cryptography?** | **Unit #:**  **1** | **Lesson #:**  **1** | **Activity #:**  **1** |
| **Activity Title: Sharing Messages** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **7 days** |
| **Estimated Activity Duration:** | **3 days** |

**Setting: Classroom**

**Activity Objectives:**

**Students will**

**1. compare and contrast the pros and limitations of sharing messages privately vs. publicly.**

**2. explain the historical relevance of cryptography and identify common errors in coding.**

**3. explain present day security concerns and identify specific flaws in cryptographic systems.**

**4. describe the big idea of the unit and essential questions.**

**Activity Guiding Questions:**

**∙ How can I share a private message publicly?**

**∙ How can I use patterns to write function rule to describe keys to various ciphers?**

**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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☐​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☐​**Reason abstractly and quantitatively** | ☐​**Attend to 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, ONLS and/or CCSS):**

[**CCSS.MATH.CONTENT.7.EE.B.4**](http://www.corestandards.org/Math/Content/7/EE/B/4/)

**Use variables to represent quantities in a real­world or mathematical problem, and construct simple equations and inequalities to solve problems by reasoning about the**

**quantities.**

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

**Computers or Phones for students**

**Poster Boards (1 per pair) Markers**

**Introduction to Cryptography PPT Caesar Cipher Practice Cryptography** [**WebQuest**](http://questgarden.com/author/create/preview.php?u=182279&amp;l=182279-150702115934&amp;a&amp;p=introduction&amp;pt=student) [**Class Cryptography Blog**](http://ihms6cryptography.blogspot.com/)

[**4­2­1 Summarizer**](https://docs.google.com/document/d/1-yyexvylauX4-h5p0WnWxsWe-mN4kX_EhaCD3zgxzNM/edit?usp=sharing)

**Teacher Advance Preparation:**

**1. Ask students to bring their devices to class or arrange for the students to have school devices.**

**2. Hang posters around the room and place markers next to the posters.**

**3. Print Caesar Cipher Worksheet**

**4. Place link to Survey,** [**WebQuest**](http://questgarden.com/author/create/preview.php?u=182279&amp;l=182279-150702115934&amp;a&amp;p=introduction&amp;pt=student)**, and** [**Blog**](http://ihms6cryptography.blogspot.com/) **in a commonly shared location, such as**

**Blackboard, for students to easily access. Activity Procedures:**

**1. Have students take the pre­unit survey/pre­test.**

**2. Hook: Share a message privately vs. publicly**

**a. Break the class into partners and have one them sit across the room from each other.**

**b. Give one partner a message (famous quote) to secretly pass along to their partners without moving from their seat or speaking to their partner.**

**c. Take away all electronic devices and tell the students the second partner will now pass a message. However, this time, they have an added constraint, they can ONLY share the message using the markers and poster boards on the wall. The posters must remain on the wall.**

**3. Conduct a group discussion over the challenges of sharing a private message over a public forum.**

**4. Develop the Big Idea and Essential Questions for the Unit.**

**a. Conduct a** [**4­2­1 activity**](https://docs.google.com/document/d/1-yyexvylauX4-h5p0WnWxsWe-mN4kX_EhaCD3zgxzNM/edit?usp=sharing)**. On their own, have students generate a list of the 4 most important things we need to learn based on the hook.**

**b. Once all student have 4 items on their chart, have them work with a partner to share and narrow down their list to find the 2 most important things we need to learn. c. Finally, have the students work with their teams (groups of 4) to decide on the 1 most important idea from our hook.**

**d. Conduct a full class discussion on their final choice and choose a big idea as a class.**

**e. Have the students summarize the big idea on their sheets and with a partner write**

**3­4 essential questions (EQs) they will need to answer in order to understand the big idea.**

**f. Share EQs on the board and select 3­4 as a class to guide our unit.**

**5. Introduce Cryptography and Ciphers (Caesar and Substitution) (Use PPT to assist presentation)**

**6. Break students into 6 groups and allow them to complete the** [**WebQuest**](http://questgarden.com/author/create/preview.php?u=182279&amp;l=182279-150702115934&amp;a&amp;p=introduction&amp;pt=student) **in order to learn about and create a** [**Blog**](http://ihms6cryptography.blogspot.com/) **Post on their assigned topic (Historical ­ Zimmerman Telegram – WWI, Enigma – WWII; JN­25b ­ Midway – WWII; Present Day Considerations – Passwords and Cell Phones; Credit Cards and Bank Information; Target/Samsung/Anthem)**

**7. Allow groups to share their** [**Blog**](http://ihms6cryptography.blogspot.com/) **Post while members of the class comment on their work and ask questions.**

**8. Explain that in our next lesson, we will begin learning about Public Key**

**Cryptosystems.**

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

**Class discussion over the Hook.**

**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.**

**Students will be assessed according to the** [**blog**](http://ihms6cryptography.blogspot.com/) **presentation rubric on the** [**WebQuest**](http://questgarden.com/author/create/preview.php?u=182279&amp;l=182279-150702115934&amp;a&amp;p=introduction&amp;pt=student)**.**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**Reflection: Reflect upon the successes and shortcomings of the lesson.**

**Name: Amanda Sopko Contact Info:** [**Amanda.sopko@ih.k12.oh.us**](mailto:Amanda.sopko@ih.k12.oh.us)

**Date: 7/02/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : What is Cryptography?** | **Unit #:**  **1** | **Lesson #:**  **1** | **Activity #:**  **2** |
| **Activity Title: Secret Vs. Public Keys** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **7 days** |
| **Estimated Activity Duration:** | **4 days** |

**Setting: Classroom**

**Activity Objectives:**

**Students will**

**1. compare and contrast the pros and limitations of sharing messages privately vs. publicly.**

**2. use the order of operations to evaluate expressions.**

**3. use algorithms to substitute values in order to generate a secret key with a partner.**

**Activity Guiding Questions:**

**∙ How can I share a private message publicly?**

**∙ What algorithms can I use to send private information over a public forum?**

**∙ Why is it important to use the order of operations when evaluating algorithms?**

**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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☐​**Use appropriate tools strategically** |
| ☒​**Reason abstractly and quantitatively** | ☒​**Attend to 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, ONLS and/or CCSS):**

[**CCSS.MATH.CONTENT.6.NS.B.2**](http://www.corestandards.org/Math/Content/6/NS/B/2/)

**Fluently divide multi­digit numbers using the standard algorithm.**

[**CCSS.MATH.CONTENT.6.EE.A.2.C**](http://www.corestandards.org/Math/Content/6/EE/A/2/c/)

**Evaluate expressions at specific values of their variables. Include expressions that arise from formulas used in real­world problems. Perform arithmetic operations, including those involving whole­number exponents, in the conventional order when there are no**

**parentheses to specify a particular order (Order of Operations).**

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

**Diffie­Hellman and RSA Videos Diffie­Hellman and RSA Practice Worksheet Engineering Design Notebooks (EDN)**

**10 boxes with 2 latches (or 1 box for each group of 3)**

**30 padlocks with keys (or one for each student)**

**Teacher Advance Preparation:**

**1. Prior to the lesson, have students watch the Diffie­Hellman and RSA videos.**

**2. Put out boxes to there is one box for every group of 3 students.**

**3. Put 2 locks with corresponding keys in each box.**

**4. Print off DIffie­Hellman and RSA Practice Worksheets.**

**Activity Procedures:**

**DAY 1**

**1) Hook: Box Problem**

**a) Arrange groups of three such that two students are sitting across from one another (students A and B) at a table/desk and the third student (E) is sitting between. b) Tell students that they must pass a coin from A to B in the box so that E cannot steal the coin.**

**c) A and B cannot pass the box directly to each other, it must be passed through E. d) Allow groups to complete this task until they can successfully pass the coin without E taking it.**

**e) Discuss successful strategies as a whole group.**

**f) Have students write their strategies/strategies observed in their EDN.**

**2) Diffie­Hellman**

**a) Introduce Diffie­Hellman and its significance to Cyber Security**

**b) Review the video assignment and practice several problems with the students until they feel comfortable using the algorithm.**

**c) Give students the Diffie­Hellman applet.**

**d) With a partner, have the students work through the problems to discover that after**

**2 exchanges, both partners will always get the same remainder. Students should record all observations in their EDN.**

**e) Conduct a whole group discussion on this phenomena and allow students to respond in their EDNs**

**DAY 2**

**3) RSA**

**a) Introduce RSA and its significance to Cyber Security**

**b) Review the video assignment and practice several problems with the students until they feel comfortable using the algorithm.**

**c) Give students the RSA applet.**

**d) Allow students to work with a partner and make observations in their EDN. e) Discuss solutions as a class.**

**DAY 3**

**4) Review the Chinese Remainder Theorem**

**a) In their EDNs have students brainstorm ways to use the CRT to authenticate a message.**

**b) Allow students to share their thoughts with the class.**

**5) Conduct a whole class discussion on the pros and cons of using each method. Allow students to make observations in their EDNs.**

**a) Allow students to stand in one of three spots in the room depending on the method they think is most secure. Students who are undecided can stand in the middle of the room.**

**b) Allow each side to give evidence to support their stance trying to win over students.**

**DAY 4**

**6) Revisit Box Problem with Active Attacker a) Review the Box Problem.**

**b) This time, give person E a lock with key.**

**c) Allow students to complete the exchange allowing person E to attempt to steal the coin.**

**d) Discuss successful solutions and allow students to respond in their EDN.**

**7) Man in the Middle Attack**

**a) Explain that this is a common attack used by hackers. b) Conduct a “Man in the Middle Attack” with the class.**

**c) Revisit Diffie Hellman applet. Have students work in groups of 3 and allow interception.**

**d) Have students write observations in their EDN and discuss the limitations of protecting a message from a Man in the Middle Attack.**

**e) Assign students to research methods to prevent the middle man from stealing their data and write their findings in their EDNs.**

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

**Class discussion over the Hook.**

**Diffie­Hellman and RSA Practice work from applets**

**Diffie­Hellman/RSA Debate**

**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.**

**All work in this lesson is prerequisite to the final “Coin Collection Challenge”. (See Lesson 2, Activity 4)**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**Reflection: Reflect upon the successes and shortcomings of the lesson.**

**Name: Amanda Sopko Contact Info:** [**Amanda.sopko@ih.k12.oh.us**](mailto:Amanda.sopko@ih.k12.oh.us)

**Date: 7/02/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : How do I keep my information safe?** | **Unit #:**  **1** | **Lesson #:**  **2** | **Activity #:**  **3** |
| **Activity Title: Cyber Attacks** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **6 days** |
| **Estimated Activity Duration:** | **1 day** |

**Setting: Classroom**

**Activity Objectives:**

**Students will**

**1. describe the importance of authentication when sending private information.**

**2. use concepts from the Chinese Remainder Theorem to build confidence when sending messages to an unknown receiver.**

**Activity Guiding Questions:**

**∙ How can I make sure the correct person gets my message?**

**∙ How can I use remainders and the standard algorithm for division to authenticate a message?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☒​**Reason abstractly and quantitatively** | ☒​**Attend to 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, ONLS and/or CCSS):**

[**CCSS.MATH.CONTENT.5.NF.B.4**](http://www.corestandards.org/Math/Content/5/NF/B/4/)

**Apply and extend previous understandings of multiplication to multiply a fraction or whole number by a fraction.**

[**CCSS.MATH.CONTENT.7.SP.C.5**](http://www.corestandards.org/Math/Content/7/SP/C/5/)

**Understand that the probability of a chance event is a number between 0 and 1 that expresses the likelihood of the event occurring. Larger numbers indicate greater likelihood. A probability near 0 indicates an unlikely event, a probability around 1/2 indicates an event that is neither unlikely nor likely, and a probability near 1 indicates a likely event.**

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

**20 yes/no questions**

**Engineering Design Notebooks (EDN)**

[**Cryptography PPT**](https://docs.google.com/presentation/d/1n0V34DZ1BkcALGWGg0f4eBqToUbQP6O9R6FoSJ8Sdj4/edit?usp=sharing) **Slides 30­32**

**Teacher Advance Preparation:**

**1. Create 20 yes/no questions to ask one student in a sequestered location. Activity Procedures:**

**1) Hook: Alli Baba’s Cave**

**a) Before class begins, take two students from the classroom and put them in separate locations where they have no contact with each other.**

**b) Ask one student the 20 yes/no questions and bring both students back to class. c) Explain that today we will be reenacting a famous proof used to determine if someone is who they say they are.**

**d) Tell the story of Ali Baba’s Cave. “You are standing at the mouth of a cave waiting for Ali Baba. He has the key to open a locked room of buried treasure. The key he holds will also open the door in the bottom of the cave where you are waiting for him.**

**However, there are many imposters who will pose as Ali Baba and you must determine if the man who approaches you is who he says he is. To test his authenticity, you send Ali Baba into the cave and ask him to stand on one side of the door. Then you follow him down into the cave and command him to exit from one side of the door. If he comes out, he might be Ali Baba (50%). What can you do to be more sure that his man is who he says he is?**

**e) Bring back the 2 sequestered students and allow the class to choose one student to ask the yes/no questions.**

**f) Begin asking questions until the class decides that the student is or is not Ali**

**Baba.**

**2) Discuss the importance of authentication when sending a private message.**

**3) Explain that Ali Baba’s Cave is an example of Zero Knowledge Proof. Discuss ways to prove a person by Zero Knowledge.**

**4) Discuss the use of timestamps in cryptography.**

**5) Writing: Why is it important to authenticate a message?**

**a) Allow students to share in a whole group discussion.**

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

**Class discussion over the Hook.**

**Class discussion on the importance of authenticating a message.**

**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.**

**All work in this lesson is prerequisite to the final “Coin Collection Challenge”. (See Lesson 2, Activity 4)**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**Reflection: Reflect upon the successes and shortcomings of the lesson.**

**Name: Amanda Sopko Contact Info:** [**Amanda.sopko@ih.k12.oh.us**](mailto:Amanda.sopko@ih.k12.oh.us)

**Date: 7/02/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title: How do I keep my information safe?** | **Unit #:**  **1** | **Lesson #:**  **2** | **Activity #:**  **4** |
| **Activity Title: Collecting Coins Challenge** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **6 days** |
| **Estimated Activity Duration:** | **4 days** |

**Setting: 2 Classrooms that have no contact with each other than the information projected on the board.**

**Activity Objectives:**

**Students will**

**1. develop protocols using cryptographic methods to collect the most coins.**

**Activity Guiding Questions:**

**∙ How can I send encrypted messages without allowing attackers to steal my wealth?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☒​**Reason abstractly and quantitatively** | ☒​**Attend to 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, ONLS and/or CCSS):**

[**CCSS.MATH.CONTENT.6.NS.B.2**](http://www.corestandards.org/Math/Content/6/NS/B/2/)

**Fluently divide multi­digit numbers using the standard algorithm.**

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

**1 lock box per group**

**About 20 combination locks with combinations written on a slip of paper.**

**1 Coin jar for each group (pasta sauce jar)**

**Projector with** [**Public Key**](https://docs.google.com/spreadsheets/d/1Cx9XGghx7RzXBwXLsllM7xxHZrWs8QfIn6npCz-eD98/edit?usp=sharing) **posted in both classrooms. Large bag of pennies, poker chips, or play coins. Engineering Design Notebooks (EDN)**

**Teacher Advance Preparation:**

**1. Laminated Game Rules sheets for students**

**2.**

**Activity Procedures:**

**1) Introduce the challenge. See rules here.**

**2) In both classrooms, project the shared** [**Google Sheet**](https://docs.google.com/spreadsheets/d/1Cx9XGghx7RzXBwXLsllM7xxHZrWs8QfIn6npCz-eD98/edit?usp=sharing) **(Public Key) for all groups to see.**

**3) Allow students to work with their groups to develop a protocol for the challenge. Have students detail their protocols in their EDNs.**

**4) Separate groups into two rooms. Allow the students to play the game.**

**5) Teams can ask the notary (teacher) to project information for the other half of their team via the public key.**

**6) Periodically, collect all boxes/locks and allow the students a few minutes to assess their progress and make adjustments to their protocols.**

**7) When game play has ended, allow students to reflect in their EDN. Give groups time to share their strategies and write changes they would make to their protocols if they were to complete this challenge again.**

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

**Small group redesign discussions.**

**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.**

**Final writing assignment in the EDN. “Coin Collection Challenge”.**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**Reflection: Reflect upon the successes and shortcomings of the lesson.**

**Name: Amanda Sopko Contact Info**[**: amanda.sopko@ih.k12.oh.us**](mailto:amanda.sopko@ih.k12.oh.us) **Date: 7/10/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : How do I keep my information safe?** | **Unit #:**  **1** | **Lesson #:**  **2** | **Activity #:**  **5** |
| **Activity Title: When is it ethical to use cryptography?** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **7 Days** |
| **Estimated Activity Duration:** | **1 Day** |

**Setting: Classroom**

**Activity Objectives:**

**Student will**

**1. respond to historical ethical dilemmas involving cryptography. Activity Guiding Questions:**

**1. When throughout history have ethics intersected with cryptography?**

**2. What criteria should we use to evaluate the ethics of cryptography and cyber security?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☐​**Make sense of problems and persevere in solving them** | ☐​**Use appropriate tools strategically** |
| ☐​**Reason abstractly and quantitatively** | ☐​**Attend to 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, ONLS and/or CCSS):**

[**CCSS.ELA­LITERACY.RI.6.1**](http://www.corestandards.org/ELA-Literacy/RI/6/1/)

**Cite textual evidence to support analysis of what the text says explicitly as well as inferences drawn from the text.**

[**CCSS.ELA­LITERACY.W.6.1**](http://www.corestandards.org/ELA-Literacy/W/6/1/)

**Write arguments to support claims with clear reasons and relevant evidence.**

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

**Handouts with a variety of ethical dilemmas related to cryptography and cyber security listed. Large signs (Ethical, Not Ethical) to along a fairly empty wall of the classroom.**

**Resource:**

**Core 6 Book that describes the Top Hat Organizer**

**Teacher Advance Preparation:**

**∙ Printout enough handouts for every student.**

**∙ Divide students into groups of 3­4.**

**∙ Hang “Ethical” sign on the far left corner along a generally empty wall and the “Not Ethical”**

**sign in the right corner of the same wall.**

**Activity Procedures:**

**Day 1: Ethical Considerations**

**1) Give every student a handout with a variety of ethical dilemmas related to cryptography and cyber security.**

**2) Assign one dilemma per group. Explain that each group will have 5 minutes to discuss their dilemma and come up with a resolution, which will be shared with the class.**

**3) Each group should assign a recorder to takes notes on their group discussion, to be turned in at the end of class (see “Group Notes Sheet”).**

**4) After the 5 minutes are up, have groups present their dilemma, resolution, and criteria along with any special considerations (3­4 minutes each). After each presentation, have students rate the ethical dilemma by standing along the sliding scale.**

**5) Host a brief discussion/debate to allow students to defend their position and address the positions of others.**

**6) Introduce the “Coventry Dilemma” to the whole class, tell each group that they are the Primer Minister of England, during World War II, and that they have received intelligence from the broken Engima code that the Germans plan to bomb Coventry tonight. They have 5 minutes to decide whether to alert Coventry to the attack and try to evacuate or to safeguard the broken code.**

**7) Have students complete the Top Hat Organizer and respond to their chart in a one paragraph persuasive writing to defend their stance.**

**a. After 5 minutes, allow students to share their writing with a partner then revise their writing for 2 minutes.**

**8) At the end of the 5 minutes, take a tally on the board to see how many would let the**

**Germans bomb Coventry, and how many would try to save it.**

**9) Discuss the historical decision Churchill made to allow the city to undergo attack.**

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

**Use student presentations on the ethical dilemmas.**

**Students’ stance and arguments/justifications of ethical rating.**

**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.**

**Core 6 writing will be collected and scored according to the middle school writing rubric.**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**Reflection: Reflect upon the successes and shortcomings of the lesson.**

**13. APPENDIX III: DOUGHERTY UNIT**

**13.1 Unit Plan**

**Name: Ben Dougherty Contact Info:** [**Dougherty.benjamin@gmail.com**](mailto:Dougherty.benjamin@gmail.com)

**Date:**

**6/22/15**

**Unit Number and Title: Unit #1: Securing Cyberspace**

**Grade Level: 11­12**

**Subject**

**Area:**

**Mathematics**

**Total Estimated Duration of**

**Entire Unit:**

**3 weeks**

**Part 1: Designing the Unit**

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

**HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it. HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales. HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).**

**HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).**

**HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.**

**HS.F.BF.4.b.c ­ Find inverse functions.**

**HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.**

**2. Unit Summary**

**The Big Idea (including global relevance):**

**Cybersecurity – This is important because of all the recent internet security breaches that have compromised the health and financial data of individuals.**

**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):**

**How is cryptography used in my everyday communications? What mathematics is used in cryptography?**

**How do you encrypt/decrypt data? How do hackers steal data?**

**How can I protect my data and communications?**

**3. Unit Context – Check all that apply. Justification for Selection of Content:**

☐​ **Students previously scored poorly on standardized tests, end­of 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 unit aligns with my RET research.**

**The Hook:**

**1) Stories about recent internet security breaches.**

**2) Stuxnet Video (https:**[**//www.youtube.com/watch?v=scNkLWV7jSw)**](http://www.youtube.com/watch?v=scNkLWV7jSw))

**3) NSA Speaker**

**The Challenge and Constraints:**

☐​**Product or** ☒​**Process (Check one)**

|  |  |
| --- | --- |
| **Description of Challenge (Either Product or Process is clearly explained below):** | **List the Constraints Applied** |
| **To pass encoded information to your teammates without getting your code broken and to break the “enemy” team’s codes.** | **Students will only be allowed to use pen, paper, calculator, and Google Sheets as computational resources; messages must**  **be passed through the “enemy” team; students will have limited time to encrypt and decrypt**  **messages; students can only send messages provided by the moderator** |

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

**What cryptographic systems are available to use? How do I encrypt a message?**

**How do I decrypt a message?**

**How do protocols increase or decrease the effectiveness of a cryptographic system?**

**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.**

**The methods of encryption and decryption and the protocols surrounding those methods that students develop will be tested throughout the challenge, by the opposing team trying**

**to “break” their ciphers. Evidence that the solution worked will be will be if their team’s code is not broken, or if they are able to break their opponents’ codes.**

**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. See below.**

|  |  |
| --- | --- |
| **Gather**  **Information** | **Throughout the unit, students will learn about various cryptographic systems and protocols** |
| **Select**  **Solutions** | **In teams, students will design their own cryptographic system and protocol.** |
| **Implement**  **Solution** | **Students will use their cryptographic system and protocol to send ciphertext over an open channel** |
| **Evaluate**  **Solution** | **Evaluation of the strength of the cryptographic systems and protocols will happen throughout the challenge, while students are trying to break each other’s ciphertext.** |
| **Refine** | **Based on whether their codes are being broken by the opposing team or not, students can refine their cryptographic systems and protocols.** |
| **Communicat e Solution** | **At the end of the activity, each team will give a presentation describing their cryptographic system and protocol, how well it worked, what changes they made, and why.** |

**What academic content is being taught through this Challenge? Linear equations**

**Modular arithmetic and the remainder theorem**

**Properties of exponents**

**Basic number theory**

**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.** |
| **Gather Information – students will be challenged to encrypt and decrypt messages using various methods**  **as we learn them.**  **Select Solutions – students will submit a draft model of their cryptographic system and protocol to me for evaluation**  **Implement Solution – while students are implementing their cryptographic systems during the challenge, they will have the opportunity to win**  **“points” for their team by breaking the opposing teams codes or by creating a code that the opposing team doesn’t break.**  **Communication of Solution – student teams will present their solution, along with their**  **refinements, and discuss their process** | **\_Games, Q/A** ☒​**formative** ☐  **summative**  **\_Model** ☒​**formative**  ☐​**summative**  **\_Game** ☒​**formative**  ☐​ **summative**  **\_Rubric** ☐​**formative** ☒  **summative** |

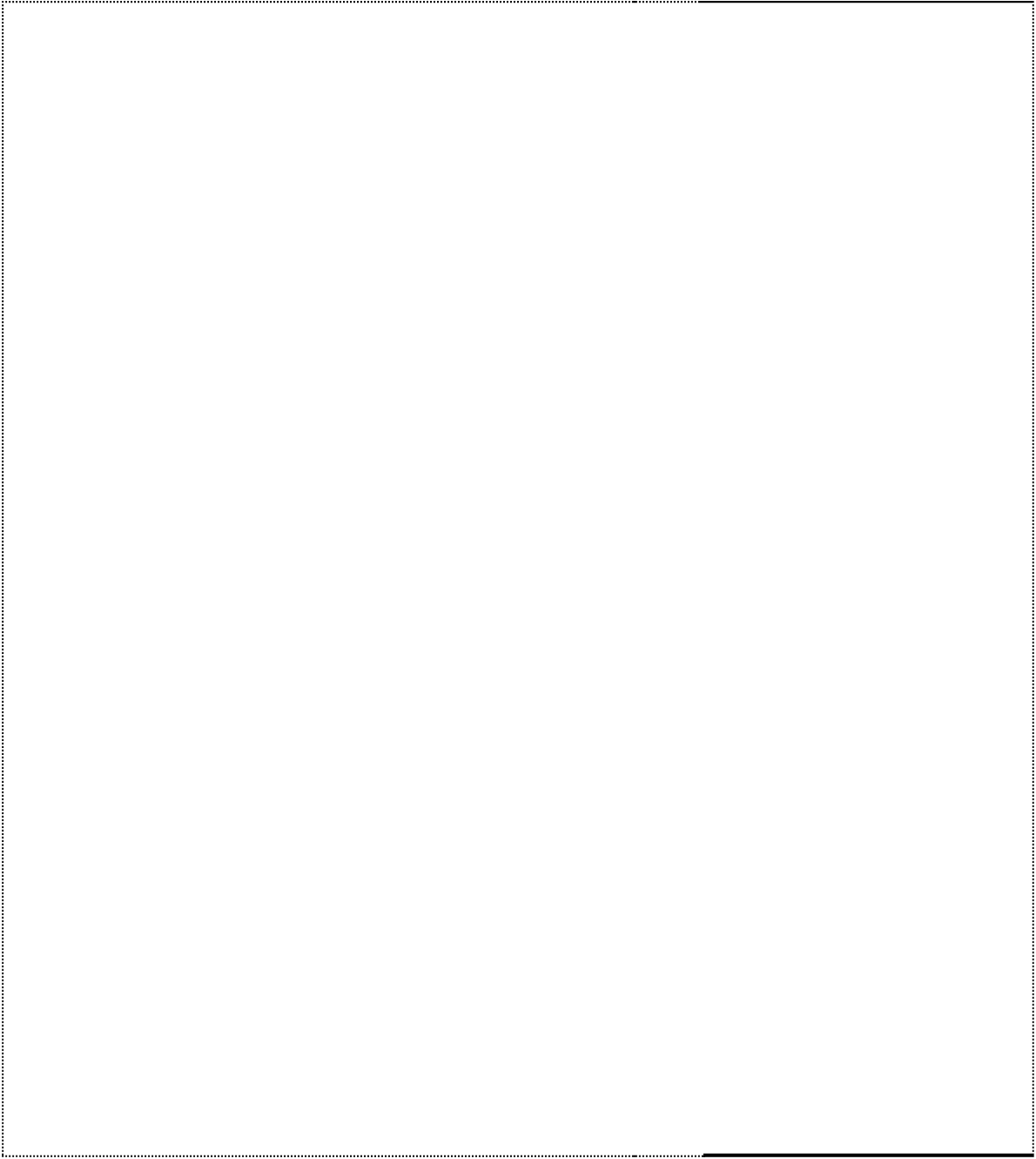
**Check below which characteristic(s) of this Challenge will be incorporated in its implantation using EDP. (Check all that apply.)**

☒​**Has clear constraints that limit the solutions**

☒​**Will produce more 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 Strongly Applies to the Real World**

**Provide a brief rationale for where you placed the X: Students will be engaged in a scaled­down version of what cyber security experts go through on a daily basis.**

**What activities in this Unit apply to real world context? \_The introduction to cryptography and protocols as well as the final challenge.**

**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: \_When cyber security fails, the societal impact is high in terms of lost financial resources or compromised personal data. Studying how to protect against the cyber security breaches thus has high societal impact.**

**What activities in this Unit apply to societal impact? \_The activity related to the ethics of cyber security as well as the challenge itself.**

**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.)**

**I’ll use a guest speaker to introduce students to careers in cyber security and computer science in general.**

**6. Misconceptions:**

**Students believe that the information they transmit via telephones and computers is secure.**

**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.)**

**Lesson #1: Introduction to Cryptography and the Mathematics of Cryptographic Systems The first lesson will introduce the big idea of cybersecurity and “hook” the students into the unit by showing them how devastating a lack of cybersecurity can be such as with the Stuxnet virus. Students will be introduced to monoalphabetic ciphers through the Caesar**

**cipher, and they will learn how to break them using frequency analysis. Students will also learn about the difference between symmetric and asymmetric encryption systems, and have an opportunity to encrypt and decrypt using the popular RSA algorithm. Throughout this first lesson, students will be interpreting ciphers as kinds of functions, and learning decryption as a kind of inverse function.**

**Activity #1: Introduction (3 days)**

**∙ Introduce the “Big Idea”: Hook: Stuxnet Video**

**(**[**https://www.youtube.com/watch?v=scNkLWV7jSw**](https://www.youtube.com/watch?v=scNkLWV7jSw)**)**

**∙ First message exchange exercise with debrief**

**∙ Introduction of Caesar Cipher**

**∙ Methods for Breaking Caesar Cipher**

**∙ Decryption as a kind of inverse function**

**∙ Head­to­head Decrypt exercise**

**Activity #2: Public Key (Asymmetric) Cryptography (4 days)**

**∙ Diffie­Hellman**

**∙ Man­in­the­Middle Attacks**

**∙ Modular Arithmetic**

**∙ RSA Encryption Demonstration**

**∙ RSA Encrypt/Decrypt Exercise**

**∙ Can RSA be broken? What are the weaknesses? Lesson #2: Cryptography and Ethics**

**The second lesson will introduce students to some of the ethical dilemmas (both historical and current) related to cryptography and cybersecurity. Students will have the opportunity to debate various dilemmas and establish criteria for considering the ethics of a situation. Students will review and condense their knowledge of cryptography and cryptographic systems. Finally, students will participate in a multi­day war simulation game in which they will be using the cryptography from the unit to communicate securely with their team to**

**win the game.**

**Activity #3: Ethical Considerations and Review (2 day)**

**∙ Cybersecurity Ethics Exercise**

**∙ Review of Cryptographic Systems**

**∙ Protocols**

**Activity #4: War Games (5 days)**

**∙ Challenge: Pass a message between members of your team over an open channel without the opposing team breaking your cryptographic system.**

**The Engineering Design Process will be applied throughout this unit.**

**∙ Gathering Information – Students will be gathering information on different encryption systems and their connections to mathematics in lesson 1 in both activities 1 and 2.**

**∙ Identify Alternatives – Throughout lesson 1 in activities 1 and 2, as students learn to break ciphers, they will naturally seek alternate cipher systems.**

**∙ Select Solution – In lesson 2 activity 4, student teams will produce their own codebook using the encryption systems they studied earlier in the unit.**

**∙ Implement Solution – In lesson 2 activity 4, student teams will use the codebook they wrote to communicate securely with their team to try to win the game. Opposing teams will be actively trying to break their encryption systems.**

**∙ Evaluate Solution – In lesson 2 activity 4, as groups use their codebook to send messages, they will receive feedback from the moderator as to whether or not their encryption systems has been “broken”. Broken encryption will tell students that their**

**codebook was not secure enough, unbroken encryption will tell students that they have created a secure code.**

**∙ Refine – In lesson 2 activity 4, when groups’ codes are broken, they can re­write their codebook to try to strengthen their encryption system for the next rounds of the game.**

**∙ Communicate Solution – In lesson 2 activity 4, after the game is over, each team will present their original codebook and describe the process by which it was updated throughout the game.**

**The following elements of Challenge Based Learning will be implemented in this unit:**

**∙ The Big Idea – Lesson 1 activity 1**

**∙ The Hook – Lesson 1 activity 1**

**∙ Essential Questions – Students will brainstorm essential questions in lesson 1 activity**

**1.**

**∙ The Challenge – The challenge will take place in lesson 2 activity 4.**

**8. Additional Resources:**

**9. Pre­Unit and Post­Unit Assessment Instruments:**

**Inventory measuring student interest and knowledge regarding cryptography, cyber security, and computer engineering. (Same inventory to be used before and after unit)**

**10. Poster (Link here.) 11. 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 New Learning Standards for Science (ONLS)** |
| **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:**

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☐​**Reason abstractly and quantitatively** | ☒​**Attend to 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** |

**13.2 Activity 1**

**Name: Ben Dougherty Contact Info:** [**Dougherty.benjamin@gmail.com**](mailto:Dougherty.benjamin@gmail.com)

**Date:**

**7/6/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Introduction to Cryptography and the Mathematics of Cryptographic Systems** | **U**  **n i**  **t**  **#**  **:**  **1** | **Less on**  **#:**  **1** | **Activ ity #:**  **1** |
| **Activity Title: Introduction** |

|  |  |
| --- | --- |
| **Estimated Lesson**  **Duration:** | **7 Days** |
| **Estimated Activity**  **Duration:** | **3 Days** |

**Sett ing:**

**Classroom**

**Activity Objectives:**

**1) Students will be able to encrypt and decrypt messages using monoalphabetic ciphers (including the Caesar cipher).**

**2) Students will be able to break monoalphabetic ciphers.**

**3) Given a function, students will be able to find its inverse.**

**Activity Guiding Questions:**

**1) How do cryptographic systems work?**

**2) How can I break a code?**

**3) How can I make a code unbreakable?**

**4) What is a function inverse and how is it related to cryptography?**

**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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |

|  |  |
| --- | --- |
| ☒​**Reason abstractly and quantitatively** | ☒​**Attend to 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, ONLS and/or CCSS):**

**HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it. HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales. HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).**

**HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).**

**HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.**

**HS.F.BF.4.b.c ­ Find inverse functions.**

**HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.**

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

**Calculators (scientific or graphing) Pen and Paper**

**Projector/Computer to show Stuxnet video**

**Extra blank paper**

**Handout on Caesar cipher**

**Handout on inverse functions (what they are and how to find them) Pre­encrypted messages to be broken in head­to­head game Flashcards**

**(Optional) Timer**

**Teacher Advance Preparation:**

**Have photocopies of handouts ready**

**Encrypt some famous quotes using the Caesar cipher and write the plaintext on one side of a flashcard and the cipher text on the other as a model for the activity.**

**Select famous quotes and encrypt them using various offsets of a Caesar cipher; print them out on a slip of paper (2 copies for each quote; 1 for each team) in the head­to­head**

**game.**

**Activity Procedures:**

**Day 1: Introduction and Caesar Cipher**

**Show Stuxnet video (**[**https://www.youtube.com/watch?v=scNkLWV7jSw**](https://www.youtube.com/watch?v=scNkLWV7jSw)**) and use**

**TPS to get students thinking and talking about cyber security.**

**Break students into groups of 3 [person A (sender), person B (interceptor), and person C(receiver)]**

**A wants to see a movie with C, but doesn’t want B to know what movie or what time.**

**Permutation 1**

**All the A’s go in one room, all the C’s go in another; the B’s will be the couriers between.**

**Rules:**

**1. A and C cannot pass information directly to one another.**

**2. All messages passed between A and C must go through B. Goal:**

**1. A’s goal is to pass the information to C through B without B getting the information.**

**Time Limit: 3 minutes**

**Teacher Notes: Most students will probably be unsuccessful at this first exercise; the purpose is to show them how difficult it is to pass secure secret communications through open channels. If anyone is successful, make sure to get their strategy in the debrief.**

**First Debrief:**

**1. Was anyone successful? How?**

**2. What made the goal difficult to achieve?**

**3. How might we accomplish this?**

**4. What real­world situations does this situation simulate?**

**5. What are the implications of this exercise for those situations and are they significant?**

**6. Why would it be important to pass information securely?**

**Hopefully, students come up with the idea of “encoding” the message as one possible solution. Their initial ideas will probably rely on a “secret key” system.**

**Review rules for brainstorming and the criteria for a good essential question. Break students into groups, and have them brainstorm essential questions in the**

**realm of the big idea using the guided handout (to be turned in by each group).**

**Tell students that you will review their questions and try to come up with a unifying theme and challenge.**

**Introduce the Caesar cipher.**

**Explain the historical significance of the Caesar cipher, distribute the handout, and let students practice encrypting and decrypting a simple message on the handout.**

**Give each student a note card. Have them look­up a famous quote, and write the quote in plaintext on one side of the card, and in a Caesar cipher text on the other side. Turn it in.**

**Permutation 2**

**Send B’s into other room and let A’s and C’s agree on a Caesar cipher key. Give A’s a message (quote) on a piece of paper to transmit, and send them into the room with the B’s. Once they’ve encrypted their message, they pass the ciphertext to B to give to C.**

**Rules:**

**1. A and C cannot pass information directly to one another.**

**2. All messages passed between A and C must go through B.**

**Goal:**

**1. A’s goal is to pass the information to C through B without B getting the information.**

**Time Limit: 10 minutes**

**Teacher Notes: In theory, A and C should now be able to pass information securely through B.**

**Second Debrief:**

**1. How did it go? Were you able to successfully pass information through B**

**without B knowing?**

**2. What did the B’s think about this development?**

**3. Are there any weaknesses to this method? (at least 1: A and C have to share the key privately beforehand)**

**4. What are some scenarios when we would want to be able to “break” the cipher?**

**Day 2: Code Breaking 101**

**Have students TPS on the weaknesses of the Caesar cipher and how to break it. Project the cipher text of a famous quote (“A PERSON WHO NEVER MADE A**

**MISTAKE NEVER TRIED ANYTHING NEW.” –ALBERT EINSTEIN) on the board and present common methods for breaking Caesar ciphers:**

**∙ Character frequency analysis**

**∙ Common character patterns**

**∙ Common 2 and 3 letter words**

**∙ Brute Force**

**Break students into groups and let them practice breaking Caesar ciphers with the flashcards made the day before.**

**Head­to­Head Cipher Breaking Game**

**Divide class in half (Team A and Team B) and pair students up with one person from each team.**

**Give each student a slip of paper with a Caesar cipher encrypted message (make sure that each pair gets the same cipher).**

**Student work to decrypt their message before the other half of their pair (from the other team) does.**

**For each unique cipher, the first person to decrypt it earns 1 point for her/his team.**

**The winning team will be the team with the most points at the end.**

**The game ends when time runs out or all messages have been decrypted. (Timer optional)**

**Day 3: Caesar Cipher and Functions**

**Start class with a simple Q&A session to lead students to the realization that encryption is a kind of 1­to­1 function. If encryption is a function, what is decryption? Hopefully students will realize it is also a function. Get students to see that encryption and decryption have an inverse relationship. Get students to detail how encryption and decryption are inverses and what that means.**

**Introduce the idea of the mathematical inverse, and demonstrate how we find the inverse of a function.**

**Have students practice finding the mathematical inverse of various functions:**

**1. Linear**

**2. Square Root**

**3. Quadratic**

**4. Exponential/Logarithmic**

**5. Trigonometric**

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

**While students are working through the “Caesar Cipher Handout”, I’ll be moving around the room answering questions, clarifying, and checking students’ understanding.**

**Students will be given a formative quiz to assess their ability to find the inverse of mathematical functions.**

**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.**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**During the head­to­head activity, students may be allowed to use notes on code breaking if necessary. While working on inverse functions, students will be allowed to use a calculator as needed.**

**13.3 Activity 2**

**Name: Ben Dougherty Contact Info:** [**Dougherty.benjamin@gmail.com**](mailto:Dougherty.benjamin@gmail.com)

**Date:**

**7/6/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Introduction to Cryptography and the Mathematics of Cryptographic Systems** | **U**  **n i**  **t**  **#**  **:**  **1** | **Less on**  **#:**  **1** | **Activ ity #:**  **2** |
| **Activity Title: Public Key (Asymmetric) Cryptography** |

|  |  |
| --- | --- |
| **Estimated Lesson**  **Duration:** | **7 Days** |
| **Estimated Activity**  **Duration:** | **4 Days** |

**Sett ing:**

**Classroom**

**Activity Objectives:**

**1) Students will be able to describe the difference between symmetric and asymmetric cryptographic systems.**

**2) Students will be able to use the Diffie­Hellman Key Exchange protocol to establish a secure channel with another party.**

**3) Students will use modular arithmetic to encrypt and decrypt messages.**

**Activity Guiding Questions:**

**1) What is the difference between symmetric and asymmetric key encryption systems?**

**2) Can two users establish a shared secret when communicating over an open channel?**

**3) Are asymmetric cryptographic systems breakable? If so, how?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☒​**Reason abstractly and quantitatively** | ☐​**Attend to 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, ONLS and/or CCSS):**

**HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it. HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales. HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).**

**HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).**

**HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.**

**HS.F.BF.4.b.c ­ Find inverse functions.**

**HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.**

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

**Teacher Advance Preparation:**

**Select values for g and p to simulate a Diffie­Hellman exchange (g=7 and p = 37). Select your own “b” value, and calculate your public key (33 in the example below).**

**Activity Procedures:**

**Day 1:**

**When students walk into class the following instructions will be on the board: Warm­up: Follow the instructions below using a calculator where needed:**

**1) Select a secret whole number (we’ll call this your “a”)**

**2) Raise the number 7 to the power of your secret number (“a”)**

**3) Divide the result of step 2 by 37, and record the REMAINDER. This is your special number.**

**4) Write your special number (the result of step 3) next to your name on the board.**

**5) Take Mr. Dougherty’s special number (33), raise it to the power of your secret number (“a”).**

**6) Divide the result of step 5 by 37, and record the REMAINDER. This is your second secret number (“s”).**

**7) Keep your first and second secret numbers private!**

**You can use this time to take attendance or whatever else you need to do. Also, as students write their “special” numbers up on the board, you can plug them into the Diffie­Hellman algorithm to get your shared secret with each student.**

**Start class with a Q&A session reviewing what you’ve covered so far with secret key encryption, substitution ciphers, function inverses, and the pros and cons of using these. Through the Q&A, lead students back around to the idea that a secret key (symmetric) requires a prior exchange of knowledge (a shared secret), and this is a problem when communicating at a distance over an open channel. Ask students if they still have their two secret numbers. Ask them if they would be impressed if you could tell them their**

**second secret number (“s”) from step 6. Use the results of the Diffie­Hellman algorithm on their “special numbers” that they wrote on the board to “WOW” them by telling them their**

**second secret number (“s”). Ask them if they’d like to know how you did that; presumably you will have sufficiently “WOW”ed them enough that they will want to know the trick. This opens the door to explain Diffie­Hellman.**

**Explain that the “special” number they wrote next to their names is their “public key”. Pair students up and have them run the Diffie­Hellman algorithm (steps 5­6) on their partner’s public key, and see if they get the same result. This would be a good place to introduce ideas of modular arithmetic and remainders. Also the identities:**

**Bring class back together for more Q&A:**

**So, you can establish a shared secret key with someone, what can you do with that? What good is that?**

**Hopefully someone comes up with the idea of using the shared secret as the numerical offset in a Caesar cipher. Have the pairs pass a message using a Caesar cipher with their shared secret as the Caesar cipher offset (use Diffie­Hellman Exercise Handout).**

**For homework have students come up with a plan for how an interceptor between the communicating parties could disrupt the security of Diffie­Hellman.**

**Day 2:**

**Start class off by having students present their plans to disrupt Diffie­Hellman. Put two random students as the sender and receiver; put the student with the plan between them**

**as the interceptor, and let them try to disrupt the exchange. After a few attempts, introduce the concept of “man­in­the­middle” attacks, particularly the reflection attack. After you show this to the students (or they figure it out themselves), break them into groups and have them try to figure out how to thwart the MITM attack.**

**Ideally, students will arrive at the idea of needing authentication. We’ll use this as a way to introduce RSA Encryption.**

**Present instructional component on asymmetric key cryptography and RSA. This includes an activity for students to practice RSA encryption and decryption via a shared Google Document.**

**Special note to teacher: encrypt a silly or appropriately teasing comment using a student’s public key and put it on the Google Doc using another student’s name before the next class. (You can enlist a student as a co­conspirator in this plan.)**

**Day 3:**

**Open class by reviewing the RSA exercise from the previous day. Say you want to use an example from our Google Document. Pull up the Google document and pick the message that you planted there the previous day. Use the student’s private key to decrypt the message, and then chastise the student whom you impersonated for putting a slightly “negative” message up. That student will hopefully protest that it wasn’t them (you could**

**inform this student ahead of class what you’re doing), which brings up the issue of someone impersonating someone else, and how, on an open channel, can we really be sure we’re talking to the person we think we are. At this point, I would tell the whole class that I had posted the message impersonating the student to illicit the conversation about authentication.**

**Present authentication PowerPoint, and have students send RSA encrypted messages with authentication per the instructions in the PointPoint. During the exercise, try to post fake messages to various students posing as other students so they can see what happens when a message does NOT authenticate!**

**Once everyone has practiced RSA authentication, group students and have them brainstorm ways to break RSA encryption. Give them the RSA Code Breaking Exercise for homework.**

**Day 4:**

**Begin class with a Q&A session to lead students toward the weaknesses of RSA. Lead students to the idea that “n” (the modulus) is a composite of two primes. If someone can find the primes p and q, then they can find (p­1)\*(q­1), and they already know your “e”, so they can solve (ex­dy=1) for a whole number solution that will decrypt.**

**See if anyone got this, and see if they broke the code. If they did, let them explain their process. If no one got this, then put students into groups and let them work on breaking this code using this method. Also have groups come up with a plan to prevent this attack.**

**Students may also realize that knowing the public key they can encrypt the alphabet using the receiver’s key and do a backwards lookup from the ciphertext back to the plaintext through such a table. Have them derive methods for preventing this attack as well.**

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

**The Diffie­Hellman exercise handout**

**The Google documents listed in the RSA activities**

**The RSA Code Breaking Exercise**

**13.4 Activity 3**

**Name: Ben Dougherty Contact Info:** [**Dougherty.benjamin@gmail.com**](mailto:Dougherty.benjamin@gmail.com)

**Date:**

**7/6/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Cryptography and Ethics** | **U**  **n i**  **t**  **#**  **:**  **1** | **Less on**  **#:**  **2** | **Activ ity #:**  **3** |
| **Activity Title: Ethical Considerations and**  **Review** |

|  |  |
| --- | --- |
| **Estimated Lesson**  **Duration:** | **7 Days** |
| **Estimated Activity**  **Duration:** | **2 Days** |

**Sett ing:**

**Classroom**

**Activity Objectives:**

**1) Students will brainstorm the criteria for evaluating ethical dilemmas**

**2) Students will apply their criteria to evaluate ethical dilemmas**

**3) Students will suggest possible resolutions to a variety of ethical dilemmas**

**4) Students will practice encryption, decryption, and cipher breaking with the cryptographic systems studied throughout the unit**

**Activity Guiding Questions:**

**1) What are the ethics surrounding the usage of cryptography and cyber security?**

**2) When throughout history have ethics intersected with cryptography?**

**3) What criteria should we use to evaluate the ethics of cryptography and cyber security?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☐​**Make sense of problems and persevere in solving them** | ☐​**Use appropriate tools strategically** |
| ☐​**Reason abstractly and quantitatively** | ☐​**Attend to 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, ONLS and/or CCSS):**

**HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it. HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales. HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).**

**HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).**

**HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.**

**HS.F.BF.4.b.c ­ Find inverse functions.**

**HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.**

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

**Handouts with a variety of ethical dilemmas related to cryptography and cyber security listed.**

**A guided notes sheet for the recorder on Day 1.**

**Practice codes and messages for students to encrypt, decrypt, and break on Day 2.**

**Teacher Advance Preparation:**

**Printout enough handouts for every student. Divide students into groups of 3­4.**

**Activity Procedures:**

**Day 1: Ethical Considerations**

**1) Give every student a handout with a variety of ethical dilemmas related to cryptography and cyber security.**

**2) Assign one dilemma per group. Explain that each group will have 5 minutes to discuss their dilemma and come up with a resolution, which will be shared with the class.**

**3) Each group should assign a recorder to takes notes on their group discussion, to be turned in at the end of class (see “Group Notes Sheet”).**

**4) After the 5 minutes are up, have groups present their dilemma, resolution, and criteria along with any special considerations (3­4 minutes each). After each presentation, give other students opportunities to add any additional thoughts.**

**5) After all groups have presented, have a class discussion about the criteria, and use consensus to build a list of shared criteria for determining the ethics of a situation.**

**6) Introduce the “Coventry Dilemma” to the whole class, tell each group that they are the Prime Minister of England, during World War II, and that they have received intelligence from the broken Engima code that the Germans plan to bomb Coventry tonight. They have 5 minutes to decide whether to alert Coventry to the attack and try to evacuate or to safeguard the broken code.**

**7) At the end of the 5 minutes, take a tally on the board to see how many would let the**

**Germans bomb Coventry, and how many would try to save it.**

**8) (Optional if time): Change the scenario from Coventry to Pearl Harbor or the World Trade Center Towers on 9/11, to see if students’ responses change when it’s their own country.**

**Day 2: Review Cryptographic Systems and Protocols**

**1) Divide students into groups of 3 (sender, receiver, and attacker); switch roles throughout exercise**

**2) Have students practice Diffie­Hellman Key Exchange and Man­in­the­Middle attacks**

**3) Have students practice Caesar ciphers**

**4) Have students practice RSA algorithm**

**5) Have students practice Chinese Remainder Theorem**

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

**Use student presentations on the ethical dilemmas from Day 1 as a formative assessment to see where students are with understanding the ethical dilemmas related to cryptography and cyber security. Use Q&A where needed to bring them along.**

**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.**

**Differentiation: Describe how you modified parts of the Lesson to support the needs of different learners.**

**Refer to Activity Template for details.**

**For the ethical portion of the activity, students will be in groups, and so some students might talk less during the presentation based on their comfort level.**

**For the review portion of the activity, students will be allowed to use notes, a calculator, and be provided handouts for the various cryptographic systems we’ll be reviewing.**

**13.5 Activity 4**

**Name: Ben Dougherty Contact Info:** [**Dougherty.benjamin@gmail.com**](mailto:Dougherty.benjamin@gmail.com)

**Date:**

**7/2/15**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Cryptography and Ethics** | **U**  **n i**  **t**  **#**  **:**  **1** | **Less on #:**  **2** | **Activ ity #:**  **4** |
| **Activity Title: Challenge: War Games** |

|  |  |
| --- | --- |
| **Estimated Lesson**  **Duration:** | **7 Days** |
| **Estimated Activity**  **Duration:** | **5 Days** |

**Sett ing:**

**Classroom**

**Activity Objectives: Students will use the cryptographic knowledge and ability they have developed throughout the unit to participate in the War Games simulation and communicate securely with their team.**

**Activity Guiding Questions:**

**How do we communicate securely with our team?**

**How can we break the enemy teams’ encoded messages?**

|  |  |
| --- | --- |
| **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 New Learning Standards for Science (ONLS)** |
| **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)** |

|  |  |
| --- | --- |
| **Common Core State Standards ­­ Mathematics (CCSS)** | |
| **Standards for Mathematical Practice (Check all that apply)** | |
| ☒​**Make sense of problems and persevere in solving them** | ☒​**Use appropriate tools strategically** |
| ☒​**Reason abstractly and quantitatively** | ☒​**Attend to 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, ONLS and/or CCSS):**

**HS.A.SSE.2 ­ Use the structure of an expression to identify ways to rewrite it. HS.A.CED.2 ­ Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales. HS.A.REI.10 ­ Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).**

**HS.F.IF.1 ­ Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes**

**the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).**

**HS.F.BF.1.a.b.c ­ Write a function that describes a relationship between two quantities.**

**HS.F.BF.4.b.c ­ Find inverse functions.**

**HS.F.LE.5 ­ Interpret the parameters in a linear or exponential function in terms of a context.**

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

**War Games Rules Code Book Template Blank Grid Paper**

**Pieces to represent different teams’ units (preferably different colored pieces; consider**

**using pieces from another board game)**

**Teacher Advance Preparation:**

**Prepare a game map**

**Prepare a way to transmit messages between students through the teacher (Google Doc?) Run copies of “War Games Rules” handout**

**Run copies of “Code Book Template”**

**Have student groups ready to go**

**Activity Procedures:**

**Day 1:**

**Before the game can begin, students must be familiar with the rules. To accomplish this, the teacher will begin by distributing a copy of the rules to every student. Students will be divided into groups and each group will be responsible for explaining a portion of the rules to the class. Groups will have 5­10 minutes to read their section of the rules and come up with a plan to present to the class. Each group will have 2­3 minutes to present**

**their section of the rules. At the end of all presentations, make sure to clarify anything that the groups did not make clear and to solicit any student questions.**

**Give students their groups, and give them the remainder of the class to strategize, assign roles, and come up with a cryptographic system and protocols for communication. Each team should complete a “Code Book” document which can be revised at any time. As the moderator, you should always have a current copy of each team’s code book.**

**Day 2:**

**Begin Round 1 by informing each team of the pre­assigned positions of their pieces and letting them know what might be visible in their field of view (it would be easiest if this was nothing).**

**Give students 20 minutes to encrypt and decrypt messages and orders. Remember that all successfully decrypted orders must be passed on to the moderator.**

**At the end of the round, perform all the orders, and let Surveillance know what they can see going into the next round.**

**Run Round 2 the same as Round 1. Day 3:**

**Solicit any new code books from teams. Run Round 3.**

**Run Round 4. Day 4:**

**Run Round 5**

**Run Round 6**

**Day 5:**

**Run Round 7**

**Run Round 8**

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

**During each round, students will get formative feedback on whether they are being successful at encrypting and decrypting messages within their team.**

**At the end of each round students will get formative feedback on the success of their ciphers and strategies when the results of the attacks are made known.**

**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.**

After the challenge, each team will give a presentation to the class about the cryptographic systems they used during the challenge, and analyze how and why they were successful or not.