# TEAM PROJECT REPORT

# Cyberspace Attack & Defense

### Submitted To

### The RET Site

### For

### Challenge-Based Learning and Engineering Design Process Enhanced Research Experiences for Middle and High School In-Service Teachers”

### Sponsored By

### The National Science Foundation

### Grant ID No.: EEC-1404766

### College of Engineering and Applied Science

### University Of Cincinnati, Cincinnati, Ohio

### Prepared By

**Sam Mizener, Math, 9th, Kings High School, Kings Mills, OH**

**James Prugh, Math, 10th, Indian Hill High School, Indian Hill, OH**

### Approved By

### \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Dr. John Franco

### College of Engineering and Applied Science

### University of Cincinnati

### Reporting Period: June 13 – July 28, 2016

### Abstract

National security, economics, bank records, and intellectual property are just a few examples of the sensitive data that is threatened by cyberspace attacks. Number theory is the basis for the computer programming tools that are designed to ensure both the security and safety of such sensitive information. Although these tools are constantly being developed and refined, and despite the best of intentions of system designers, vulnerabilities appear that can be exploited by hackers. Using the engineering design process, this paper explores the applications of number theory relating to security and safety. It examines the relationship between numbers and coding, and how they work together to increase cybersecurity and decrease vulnerabilities in code. This project will introduce high school students to basic number theory and computer programming by capturing their imagination and fascination with the field of computer science and internet security. An understanding of number theory and the experience of writing safe code will enable the high school student to develop a scientific identity. High school teachers around the county will be able to use the detailed unit topics developed by participants in the Research Experience for Teachers program to further change the way cybersecurity is taught in high school.

### Key Words

### Cybersecurity, Attack, Defense, Number Theory, Computer, Programming. Prime Numbers, Cyber Operations

### Main Body

#### INTRODUCTION

The cyberspace attack and defense unit researched that society is threatened by cyberspace attacks.  This is a major problem because sensitive data is transmitted electronically constantly every day.  Although we have developed tools to keep these transmissions safe, these tools can be vulnerable. An ongoing process occurs between those that protect data and hackers who seek to access and change data.  The ongoing process of keeping data secure needs a work force that is adept at cybersecurity.  Our goal is to foster an increase in student interest in the area of computer science and cybersecurity.  This is essential as hackers become more sophisticated and seek to cause damage to our economic structure and national security.

#### LITERATURE REVIEW

Number theory is essential in learning mathematics from the earliest age. It lays the foundation for the study of mathematics from the primary grades through high school.  Eighteenth century German mathematician Carl Friedrich Gauss considered the field of number theory to be the “queen of mathematics” (Campbell & Zazkis, 2002).  Topics such as common divisors, least common multiples, divisibility, and prime factorization are necessary for a thorough understanding of mathematics.

It has been suggested that the formal study of number theory began around 300 B.C. with Euclid’s proof that there are infinitely many prime numbers (Stein, 2009).  Euclid deduced the fundamental theorem of arithmetic, which asserts that every positive integer is a product of prime numbers.  Over a thousand years later, Arab mathematicians formulated the congruent number problem that asks for a way to decide whether or not a given positive integer is the area of a right triangle, all three of whose sides are rational numbers.  Nearly a thousand years later, Whitfield Diffie and Martin Hellman applied an algorithm for a public key cryptosystem that enabled two parties to communicate secretly over a public communication system.

``In 2011, Hendricks and Millman conducted a study to determine the effectiveness of teaching proof and number theory to high school students.  The Hendricks and Millman study involved 15 high school students who were enrolled in an 18-week course entitled Proofs and Problems in Number Theory and Algebra.  Topics covered included integers, divisibility, prime numbers, and the fundamental theorem of arithmetic.  Students were asked to rate their self-confidence by completing a post course questionnaire.  After reviewing the results of the study, investigators reported a 29.16-point difference between the students’ pre- and post-course measures of mathematical self-efficacy.

An earlier study showed that study in number theory concepts leads to an appreciation of proof and a more sophisticated reasoning ability (Quinn, 2009).  It was determined that while just 8% of participating students utilized inductive reasoning on a pretest, 88% did so on a posttest.   The study recommended that teachers spend time on problems involving patterns that do not continue as students might anticipate.  This will challenge the students’ presumption that inductive reasoning is equivalent to proof. (Miele, 2014)

The successful learning of mathematics depends in large part on the way mathematics is presented to the learner, and the manner in which the learner interacts with the learning environment (Yara, 2009)  Internet security is an important issue in today’s society, and has a direct impact on the lives of today’s student.  Therefore, internet security can be used to generate interest in number theory.  Modular arithmetic, the Euclidean algorithm, and Euler’s theorem are just a few examples of mathematical tools that were used long before computers and the need for internet encryption. Modern cryptographic algorithms, such as Diffie-Hellman and RSA, are based on ancient mathematics.  Since modern cryptography is based in large part on elementary number theory, the topics of cryptography and internet security are used to engage and educate students in number theory.  Due to the increase in electronic data traffic, internet security is relevant to all students.  Personal passwords, financial information, and intellectual property are just of few examples of data that requires integrity, confidentiality, and authentication. By developing an appreciation and understanding of such foundational mathematics, students will be able to apply mathematics and gain exposure to the growing field of computer programming and internet security.

Encryption is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be decrypted before it can be read by the recipient. The root of the word encryption is crypt, which comes from the Greek word kryptos, meaning hidden or secret. The Assyrians used encryption as early as 600 B.C. to protect their trade secret of manufacturing pottery.  A cipher named for Julius Caesar was used to protect military communication around 100 BC.  The Germans attempted secret communication with Mexico prior to World War I, and later attempted to protect their military secrets by using their famous Enigma machine. Modern encryption requires advanced number theory that relies on the discrete logarithm problem in order to secure sensitive information.  Internet security is a growing field that requires some of our country’s great thinkers.

Number theory provides the foundational blocks used to encrypt and decrypt data sent electronically.  Cybersecurity hinges on the discrete log problem because it is difficult to factor large composite prime numbers.  This fact allows the single handshake, reflection attack, Diffie-Hellman, and timestamp (the four vulnerabilities we will explore) to work.  It is essential for students to build a strong understanding of number theory to develop their skills in cybersecurity.

#### GOALS AND OBJECTIVES

Goal: Foster an increase in student interest in computer science and cybersecurity.

Objectives:

1. Apply number theory to internet security
2. Research and develop units rooted in number theory and cryptography.
3. Research real world applications where cyberspace security was exploited.
4. Find vulnerabilities and solutions to specific cyberspace protocols.

#### RESEARCH STUDY DETAILS

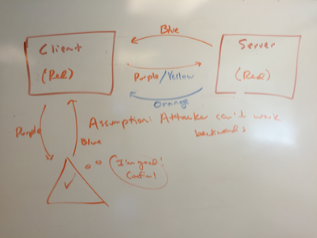
**4.1 Tasks**

Application of basic theorems and algorithms of number theory are helpful in gaining an understanding of modern encryption and internet security.  Euclid’s algorithm provides a method for finding common divisors that can be used in finding mod inverses.  The Diffie-Hellman algorithm used to generate a shared key between two parties is based on the mathematical concepts of modular arithmetic.  RSA, a public key cryptosystem that was publicly introduced in 1977 by Rivest, Shmir, and Adleman, is widely used to secure data transmission and relies upon the factorization of large composite prime numbers.  The simple fact that prime factorization mod *n* on composite numbers with factors roughly of equal size is a fundamentally hard problem leads to the discrete logarithm problem, which lies at the heart of internet security.

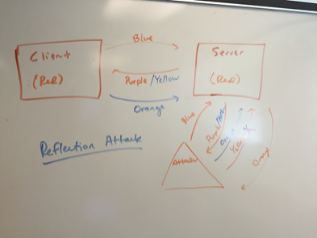
**4.1 Handshake Protocol Vulnerabilities**

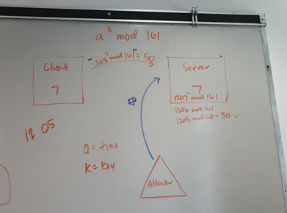
A handshake protocol is a series of steps used to authenticate a client (such as an Iphone) and a server (such as the Apple store).  The security of this protocol is essential due to the sensitive information that is sent over cyberspace.  Although there are several different types of vulnerabilities, we will outline a few of the handshake protocols.

***4.1.1 Single Handshake***

 *The single handshake protocol has a particular vulnerability that allows an attacker to impersonate the server to the client.  This happens when a client and a server establish a connection and attempt to authenticate each other.  In a single handshake the server authenticates that it is connected to the correct client; however, the client does not authenticate that it is connected to the correct server.  This is vulnerable to an attacker posing as the server and establishing a connection with the server.  To remedy this vulnerability, a double handshake is required where both parties authenticate each other.*

***4.1.2 Reflection***

 *The reflection attack occurs during the remedy of the single handshake vulnerability.  This remedy is a mutual authentication where the client and server authenticate each other.  In the reflection attack the attacker poses as the client by opening up two connections with the server.  First, the attacker authenticates the server.  When the server authenticates the attacker, the attacker opens up a second connections using the requested key from the server.  After receiving the correct response from the server, the attacker abandons the second connection and completes the servers request for authentication.*

 ***4.1.3 Timestamp***

*A timestamp is attached to a key that is sent between the client and the server as a way to protect against the replay attack.  The replay attack is when the attacker will copy the transmissions between the client and the server and pose as either.  A timestamp can be added to the key so that the receiving party will know the time when the sending party sent the key, this is important because the attacker cannot reproduce the key at the exact same time as the sender.*

**4.2 Cryptography**

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.

#### RESEARCH RESULTS

The research produced two teaching units for high school students.  The teachers involved in these units researched number theory, cryptography, internet security, and coding.  The research was directed at developing activities that high school students would find both interesting and useful in their study of mathematics and computer science. All units and activities were researched and developed with an emphasis on integrity, authentication, and confidentiality  Further research explored the growing need for internet security, the ethical issues that exist, and the increased demand for the skills needed to provide security both domestically and internationally.

One unit was developed for tenth grade precalculus students, and was designed for implementation at the beginning of the school year.  Research was directed toward several 20th century events in which cryptography played an important role.  The Zimmerman Telegram was a communication from Germany to Mexico proposing an alliance prior to the United States’ entering World War I.  British codebreakers used frequency analysis to decode the signals and warn the United States of Germany’s intent.  The Enigma Machine was a polyalphabetic substitution cipher developed by the Dutch and later used by the Germans to protect military communications during World War II. Poor operating procedures led to the machines being reverse engineered by the allies.  More recently, an attempt to sabotage Iran’s nuclear program resulted in a cyberattack against a power plant in Iran and was traced to a computer virus called Stuxnet.  The virus caused extensive damage to Iranian nuclear centrifuges.  After considering several newsworthy events in cryptography, it was decided that the unit begins with a video clip describing the implications of the Stuxnet virus.

The first two activities within the unit provide an introduction to number theory, while the third and fourth activities are designed to demonstrate the use of number theory with encryption.  Research has found that prime numbers are the building blocks of encryption.  The first activity introduces students to the concept of prime numbers, Fermat’s Little Theorem, and the fundamental theorem of arithmetic.  The research has also found that algorithms are not only helpful in the study of all levels of mathematics, but also play an important role in internet encryption.  The second activity is designed to explore the algorithms used to find square roots and common divisors.

The research indicated that exposure to number theory leads to a deeper understanding of mathematics.  The research into such concepts as the Babylonian algorithm, Euler’s Theorem, Fermat’s Little Theorem, and modular arithmetic has found that number theory is prevalent in providing integrity, authentication, and confidentiality of information.  Assessments will be used to show that activities involving encryption can reinforce some of the basic theorems and algorithms present in number theory.  The final two activities in the unit apply mathematical concepts to public key encryption, using a public key to encrypt a message while the user keeps a separate, private key that will decrypt the message. A substitution cipher will be used, along with a shared key, padding, and a xor operator. By attempting to securely encrypt and send a message, students will apply the earlier lessons in number theory.

The first activity is preceded by a pretest that will measure mathematical skills and basic encryption.  A posttest will follow the final activity in order to measure student growth number theory and encryption with particular emphasis on the methodology used.

The unit will close with a lesson on the mathematics behind RSA, a widely used public key system.

The other unit is intended for students in a course entitled “Introduction to Computer Science.’  This is an entry level computer class that will introduce students to Python as well as other basic programming concepts.  After students have been introduced to python programming they will start the unit by listening to an FBI guest speaker report on the importance of cybersecurity and computer programming in law enforcement and homeland security.  This will act as a hook for students to capture their imagination and increase interest in the field of computer science.  Students will then research vulnerability protocols and real world applications.  This knowledge will build their ability to adapt and change the code of “Game of Codes” which will be the last activity.  “Game of Codes” will be used to provide students with a game where they apply the concepts of vulnerabilities to try and intercept messages sent to each other.  All of these activities will showcase the power of computer programming and emphasize the importance of writing safe code in a world that transmits so much information electronically.

After the units are implemented, the teachers will review 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.

#### CONCLUSIONS

The research completed during this program and the experience with Challenge-Based learning will have a direct impact on my future teaching.  It is imperative that students are given the opportunity to apply mathematical and computer science content to real world applications as well as the insight to career opportunities that relate to those concepts.  High school students are taught math as a means to being successful in the next math class, instead of inspired to apply these concepts to solve societal problems.  This research experience has instilled a fundamental belief that Challenge-Based learning is an incredibly effective avenue for student inspiration.  This inspiration is essential specifically in the world of cybersecurity, as hackers become more sophisticated and gain access to dangerous information that can harm our society.

#### RECOMMENDATIONS

The study of cybersecurity and how number theory relates to computer programming could be taught over several years and at multiple different grade levels.  The research done during these two units is introductory and opens up students’ vision for computer science.  These units could and should be taught at every school to introduce students to computer science.  Although this topic is incredibly important, the focus is specific so we recommend that study should only continue if students have a desire to enter the field of computer science.  Delving deeper into the area of study should only be for students who intend to major in computer science.  This means the curriculum for future classes should be determined by individual schools to decide if there is enough student interest to fill classes.

#### CLASSROOM IMPLEMENTATION PLAN

#### The first cyberspace unit is designed to introduce students to number theory and apply number theory to internet security.  Students are shown a video that describes a recent cyber-attack, followed by a discussion of internet security.  The big idea of cybersecurity is introduced, and essential questions are generated. The activities all use challenge based learning to introduce students to concepts such as prime numbers, theorems, and algorithms that are directly related to internet encryption.  The final activity requires students to implement the engineering design process to securely encrypt and send a message.  A discussion follows about the methods used, as well as ethical issues that exist in internet security.

The second cyberspace unit that will be implemented in Intro to Computer Science will start with a guest speaker from the FBI - Cyberspace division.  He will be interviewed and answer questions regarding the role of law enforcement in cybersecurity as well as give a convincing hook that will introduce real world applications, career opportunities, and societal impact of cyberspace.  This will be followed up with the introduction to the challenge where students will send messages to each other while trying to intercept and change other messages.  The challenge will occur at the end of the unit; students will be researching vulnerabilities and how to change Python code to increase and decrease vulnerabilities prior to completing the challenge.

A pre-test and post-test as well as formative assessments will be used to evaluate student learning throughout the entire activity. Examples of formative assessments will include exit slips, understanding checks, and rubric evaluations.

#### ACKNOWLEDGEMENTS

We would like to acknowledge and thank the National Science Foundation, the University of Cincinnati, Dr. Kukreti, Debbie Liberi, Dr. Franco, Carlo Perottino, and Nick Maltbie.  The National Science Foundation funded “Challenge-Based Learning and Engineering Design Process Enhanced Research Experiences for Middle and High School In-Service Teachers”.  The Grant ID No. is EEC-1404766.  The University of Cincinnati in partnership with the NSF has made this research possible and contributed greatly to making this research a powerful tool that will continue to guide student growth for years to come.  We would also like to thank Dr. Kukreti for his leadership and commitment to the grant as well as Debbie Liberi who was a monumental help through the entire process. We would like to specifically thank our research team, Dr. Franco, Carlo Perottino, and Nick Maltbie, who taught us more about cybersecurity in the past several weeks than we could have possibly learned on our own.  Dr. Franco’s wisdom and insight made our research meaningful and inspired us to begin teaching cybersecurity to our students in a way that will build their scientific and professional identity in the field of computer science. Carlo Perottino was instrumental in the basic understanding of computer programming and Python code.  Nick Maltbie used his knowledge of computer programming and vulnerabilities to write and create “Game of Codes” so that Sam could use it in his class.

#### BIBLIOGRAPHY

1. Booher, J. (2008). “Number Theory in Cryptography.”
2. Campbell, S. R. (2002). “Toward number theory as a conceptual.” *Learning and teaching number theory: Research in cognition and instruction*, R. Zazkis, ed., essay, Ablex Publishing, Westport, CT, 1–14.
3. Carvalho , M., DeMott, J., Ford, R., and Wheeler, D. A. (2014). “Heartbleed 101.” *IEEE Security & Privacy*, 12(4), 63–67.
4. Company, T. T. (2015). Stuxnet - The first Cyber Guided Missle. Kanopy, Kanopy Streaming Videos.
5. Hardy, G. H., and Wright, E. M. (1979). “Some Notations.” *An Introduction to the Theory of Numbers*, essay, Clarendon Press, Oxford, England, 7–8.
6. Herrmann, D., and Sally, P. J. (2013). *Number, shape, and symmetry: an introduction to number theory, geometry, and group theory*. A K Peters/CRC Press, Boca Raton, FL.
7. Klembalski, K. (2012). “Cryptography and number theory in the classroom -- Contribution of cryptography to mathematics teaching.” *Proceedings of the tenth International Conference Models in Developing Mathematics Education*, 323–327.
8. Miele, A. M. (2014). *The Effects of Number Theory Study on High School Students’ Metacognition and Mathematics Attitudes*. ProQuest LLC, Ann Arbor, MI.
9. Nguyen, M. V. (n.d.). “Number Theory and the RSA Public Key Cryptosystem.” *Sage Documentation v7.2*, SageMath, <http://doc.sagemath.org/html/en/thematic\_tutorials/numtheory\_rsa.html> (Jul. 14, 2016).
10. Quinn, A. L., Evitts, T. A., and Heinz, K. (2009). “Count on Number Theory to Inspire Proof.” *The Mathematics Teacher*, 103(4), 298–304.
11. Radha, K., BALAJI, G., and Sudha, J. (2013). “Number Theory in Providing Security.” *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(7), 254–256.
12. Speciner, M., Perlman, R., and Kaufman, C. (2002). *Network Security: Private Communication in a Public World, Second Edition*. Prentice Hall, Upper Saddle River, NJ.
13. Stein, W. (2009). *Elementary Number Theory: Primes, Congruences, and Secrets*. Springer-Verlag, New York, NY.
14. Zhang, J., Zhang, D., and Drew, A. (2015). “Number Theory Applied to RSA Encryption.” http://www.supercomputingchallenge.org/14-15/finalreports/46.pdf, New Mexico.

#### APPENDIX I: NOMENCLATURE USED

Python - A computer programming language.

Prime number - Any integer greater than 1 that has only 1 and itself as factors.

Composite number - A whole number is divisible by numbers other than 1 and itself.

The fundamental theorem of arithmetic - Every positive integer except 1 can be expressed in exactly one way apart from rearrangement as a product of one or more primes. (Hardy and Wright 1979, pp. 2-3).

Euclid’s algorithm – A method for computing the greatest common divisor of two numbers, the largest number that divides both of them without leaving a remainder.

Euler’s theorem - m(x) = 1 mod (n)

Babylonian algorithm - an algorithm used for computing the principal square root of a nonnegative real number.

Fermat’s little theorem - If *p* is a prime number and *a* is a natural number, then  a^p=a (mod p). 

Modular arithmetic - Also known as “clock arithmetic”, a system of arithmetic for integers where numbers "wrap around" upon reaching a certain value called the modulus.

Diffie-Hellman algorithm - A method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel.

Euler’s totient function - A function that counts the positive integers up to a given integer *n* that are relatively prime to *n.*

RSA - A public key cryptography that uses a public and a private key used to secure data transmissions.

#### APPENDIX II: RESEARCH SCHEDULE

* Week 1
  + Engineering Foundations Class
* Week 2
  + Introduction to research
  + Introduction to Python and Computer Programming
    - Programmed calculator, quadratic function, and square roots
    - Geometric Sequence
  + Introduction to Number Theory
* Week 3
  + Basic Computer Programming
  + Lessons in specific security protocols
    - Diffie-Hellman
* Week 4
  + Start work on Attack & Defense game “Game of Codes”
  + RSA protocol
* Week 5
  + Continued work on “Game of Codes”
  + Constructed Pre-test and Post-test in Vulnerabilities
    - Researched single handshake, reflection, Diffie-Hellman, and timestamp
* Week 6
  + Continued work on “Game of Codes”
  + Finalized poster, PowerPoint presentation, video, and activities
* Week 7
  + No Research - Prepare for presentation