Comparing Learning Gains in Cryptography Concepts Taught Using Different Instructional Conditions and Measuring Cognitive Processing Activity of Cryptography Concepts

by Joseph W. Beckman
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

COMPARING LEARNING GAINS IN CRYPTOGRAPHY CONCEPTS TAUGHT USING DIFFERENT INSTRUCTIONAL CONDITIONS AND MEASURING COGNITIVE PROCESSING ACTIVITY OF CRYPTOGRAPHY CONCEPTS

by

Joseph W. Beckman

A Dissertation

Submitted to the Faculty of Purdue University
In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Technology
West Lafayette, Indiana
August 2019

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Melissa Dark, Chair
Department of Technology
Dr. Ida Ngambeki
Department of Technology
Dr. John Springer
Department of Technology
Dr. Baijian Yang
Department of Technology

Approved by:
Dr. Kathryne Newton
Head of the Graduate Program

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Author: Beckman, Joseph, William, PhD
Institution: Purdue University
Degree Received: August 2019
Title: Comparing Learning Gains in Cryptography Concepts Taught using Different Instructional Methods and Measuring Cognitive Processing Activity of Cryptography Concepts
Committee Chair: Melissa Dark, PhD

Information security practitioners and researchers who possess sufficient depth of conceptual understanding to reconstitute systems after attacks or adapt information security concepts to novel situations are in short supply. Education of new information security professionals with sufficient conceptual depth is one method by which this shortage can be reduced. This study reports research that instructed two groups of ten undergraduate, pre-cryptography students majoring in Computer Science in cryptography concepts using representational understanding first and representational fluency first instructional treatment methods. This study compared learning results between the treatment groups using traditional paper-based measures of cognitions and fMRI scans of brain activity during cryptography problem solving. Analysis found no statistical difference in measures of cognitions or in cognitive processing, but did build a statistical model describing the relationships between explanatory variables and cryptography learning, and found common areas of cognitive processing of cryptography among the study's twenty subjects.

INTRODUCTION

Problem Statement

The United States is attempting to address a shortage of cybersecurity professionals, in part, through education. (Evans & Reeder, 2010) classified the shortage of cybersecurity professionals in the United States stating, “We not only have a shortage of the highly technically skilled people required to operate and support systems we have already deployed, we also face an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute from damage due to system failures and attacks” (p. vi). In order to produce cybersecurity professionals with the ability to design, create, and reconstitute systems, cybersecurity instruction must facilitate not only students’ mastery of technical skills, but also a facility in abstraction of cybersecurity concepts that allows students to recognize apply those concepts to novel problems and situations (McGettrick, Cassel, Dark, Hawthorne, & Impagliazzo, 2014; Schneider, 2013). Cryptography is a key component of cybersecurity and is challenging to teach because learners of cryptography must master complex cryptographic protocols and the mathematics underlying those protocols (Simms & Chi, 2011, p. 344). So, creating practitioners who are fluent in the concepts important to cryptography is challenging and must be addressed as part of a larger strategy to educate cybersecurity professionals.

Cognitive theories of learning state that learners build and revise mental models of concepts using enactive, iconic, and symbolic representations of those concepts in order to develop deeper conceptual understanding (Bruner, 1964, p. 2). Because each representational form emphasizes and de-emphasizes different characteristics of concepts, the ability to successfully translate among representational forms, representational fluency (RF), indicates deep conceptual understanding (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 146). Several researchers have shown that instructional methods that include instruction focused in representational fluency has been effective in increasing learning in students in STEM fields (Kozma, Chin, Russell, & Marx, 2000; Moore, Miller, Lesh, Stohlmann, & Kim, 2013; Hill, 2015) including in mathematics (Lesh, Post, & & Behr, Representations and translations among representations in mathematics learning and problem solving, 1987; Delice & Kertil, 2015). Representational fluency demands that individuals possess sufficient understanding of the representations among which they are translating such that the translator can properly represent concepts given the different aspects of concepts that are emphasized and de-emphasized by different representational forms (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 146).

In order to be fluent in translating concepts among different representations, one must have a deep understanding of how individual representational forms represent concepts, including what aspects of concepts may be emphasized or de-emphasized, as well as how particular representational forms may be applied to concepts in a specific domain of knowledge (Ainsworth, 2006, p. 186), which defines representational understanding. Learners may have strong understanding of how a particular representational form represents concepts generally, but still find challenging the ability to apply a learned representational form to a specific domain due the learner's lack of domain specific knowledge (Ainsworth, 2006, p. 186). For example, Ainsworth (2006) attributed children's mis-interpretation of the concept of velocity from a graph of distance over time described in (Leinhardt, Zaslavsky, & Stein, 1990) as an example of the mis-application in a specific domain of a well-understood representation. In (Kozma, Russell, Jones, Marx, & Davis, 1996) undergraduate chemistry students also mis-interpreted static, written material containing representations that they had been using during their undergraduate careers in chemistry (p. 54). In the case of the undergraduate chemistry students, mis-interpretations were corrected by instruction using multiple, linked representations rather than further, domain-specific instruction in the representations that the students were mis-interpreting (p. 56). While theoretical frameworks such as Ainsworth's provide guidance about how instruction using multiple representations is made more effective when learners have, in part, deep knowledge of the representational forms with which they interact in instruction, results from (Kozma, Russell, Jones, Marx, & Davis, 1996) show that instruction using multiple representations also improves understanding of concepts when learners lack sufficient understanding of individual representations representing those concepts. Research has not yet made clear how instruction that emphasizes representational understanding (RU) and representational fluency may work together to most effectively facilitate deep conceptual learning. Specifically, researchers do not yet understand how the order of RU and RF instruction influences conceptual learning, or if the order of instruction matters at all. Understanding the role of RU and RF instruction plays in deepening conceptual understanding of cryptography concepts is important in the continued improvement of STEM instruction broadly and cryptography instruction more specifically.

Creating deeper understanding in cryptography concepts also requires new methods and tools for the assessment of knowledge. Bloom (1956) introduced the use and of knowledge taxonomies, or organizational schemas, in education as a method of organizing knowledge in a domain and as a tool that helps educators clarify learning objectives and build assessment instruments that are consistent measures of those objectives (Bloom, 1956, pp. 3-4). Unlike other STEM disciplines such as physics (Hill, 2015), cryptography lacks a comprehensive taxonomy of domain knowledge. Because the field of cryptography lacks a comprehensive, authoritative knowledge taxonomy, building curriculum and assessments of cryptography knowledge that facilitate the broad development of practitioners with deep conceptual understanding of cryptography concepts is more difficult.

Work in the developing field of educational neuroscience is providing researchers in education with new tools that may provide new insights into how curriculum and instructional design influence learning (Szűcs & Goswami, 2007). Focused on the intersection of the brain's physical processing of information and the creation of abstract mental representations (Szűcs & Goswami, 2007, p. 115), educational neuroscience seeks, in part, to use measurements of cognitive processing to derive information about learning (p. 114) and educational performance (Szűcs & Goswami, 2007, p. 116; Blakemore, Dahl, Frith, & Pine, 2011). Educational neuroscience has already provided insight into the similarities and differences in cognitive processing of algebra between children and adults (Qin, et al., 2004), cognitive processing of equations between undergraduate students (novices) and graduate students (experts) (Thomas, Wilson, Corballis, Lim, & Yoon, 2010), and cognitive processing of cryptography concepts in undergraduate computer science students (Beckman, et al., 2017) and in undergraduate technology students (Beckman, Bari, Chen, Dark, & Yang, 2017). These studies show that the field of educational neuroscience has the potential to provide important insights into how instruction influences learning in cryptography, but research in this area is not sufficient to fully understand how educational neuroscience can inform cryptography instruction.

Significance of the Problem

Recent high-profile thefts of sensitive information from U.S. Federal agencies and organizations enabled by hacking (Nakashima, 2017; United States Office of Personnel Management, 2015) illustrate a national security threat to the United States, and underscore the importance of effective cybersecurity measures to the United States Government. A shortage of qualified cybersecurity professionals nationally and internationally frustrates efforts to adequately restrict access to electronic data (Pierce, 2016; Rowe, Lunt, & Ekstrom, 2011; Suby & Dickson, 2015), and the shortage of qualified cybersecurity professionals continues to grow. Between 2013 and 2015, the number of survey respondents reporting that their organizations employed too few cybersecurity professionals grew from 56% to 62% (Suby & Dickson, 2015) and has remained steady at that level through 2018 (63%) (ISC2, 2018). Educating a cybersecurity workforce has become one of the strategic goals of the National Initiative for Cybersecurity Education in the United States (Paulsen, McDuffie, Newhouse, & Toth, 2012).

As the science of safeguarding information, cryptography plays a central role in protecting electronic data (Schembari, 2007, p. 8; Simms & Chi, 2011, p. 344; Temkin, 2007, p. 121). Producing information security professionals who have a more robust understanding of cryptography concepts has the potential to contribute significantly to the security of electronic data. Professionals possessing a deeper understanding of cryptographic principles would also be more likely to prevent the design and implementation of flawed cryptographic systems such as they cryptosystem compromised in the "Heartbleed" vulnerability (Ristenpart & Yilek, 2010), as well as guide the proper implementation of cryptography as an information security control to prevent potential vulnerabilities.

Research in STEM fields that studied instruction focused on representational fluency has been shown to increase understanding of complex concepts in students in STEM fields (Kozma, Chin, Russell, & Marx, 2000; Moore, Miller, Lesh, Stohlmann, & Kim, 2013; Hill, 2015) including in mathematics (Lesh, Post, & & Behr, Representations and translations among representations in mathematics learning and problem solving, 1987; Delice & Kertil, 2015). Problems of mathematic complexity and the difficulty of applying complex concepts to real-world problems that are present in cryptography are also present in physics where representational fluency was found to increase learners' conceptual understanding of key physics concepts (Hill, 2015, p. 34), and also in engineering problems presented to learners in Moore, Miller, Lesh, Stohlmann, and Kim (2013), though this study focused more broadly on the use of Model Eliciting Activities as an instructional method rather than specifically on RU and RF. Based on results from studies in physics and engineering that focused on learning using RF and similarities in learning challenges among physics, engineering, and cryptography, instruction in cryptography concepts using RF appears promising as a method of building deeper conceptual understanding of cryptography in learners.

While instruction focused on RF has shown to increase depth of conceptual understanding in some STEM fields, research providing evidentiary support for increased conceptual understanding of cryptography concepts in learners is nascent. Rau, Scheines, Aleven, and Rummel (2013) investigated how instructional support for representational understanding and representational fluency impacted learning among 599 fourth and fifth grade students who were learning fractions (p. 2). Researchers used a computer-based "intelligent tutoring system (ITS)" (p. 1) for delivery of instruction and instructional treatments in which instructional support was provided for representational understanding, support was provided for representational fluency, or support was provided for both representational understanding and representational fluency. Within each experimental group, the researchers used the first eight problems per topic as control questions for which the students were not provided any instructional support. This study concluded that students who received instructional support for representational understanding and representational fluency concurrently outperformed their own answers to the control questions: $t\ (115) = 2.41$, $p < .05$. Rau, Scheines, Aleven, and Rummel (2013) provides evidence that instruction in representational understanding and representational fluency together help fourth and fifth grade students learn fractions, but does not address how order of instruction in RU and RF may impact learning. Research on how the ordering of the delivery of instruction using RU and RF impacts learning has not yet been performed. So, it is unclear whether it matters if learners are first instructed in the use and function of individual representational forms (mathematics equations, field-specific language, graphs), if simply teaching learners to translate among representational forms is sufficient to produce increased depth of conceptual understanding (Rau, Scheines, Aleven, & Rummel, 2013).

This research seeks to clarify the relationship between representational fluency and representational understanding (RU) as that relationship impacts cryptography instruction. By investigating the relationship between RF and RU in cryptography instruction, this study seeks to provide insight into cryptography instruction that can be applied in information security programs toward the goal of producing information security practitioners with greater depth of understanding of cryptography, a central aspect of information security. Additionally, the study seeks to advance the understanding of the cognitive processing of cryptography concepts by using fMRI to study how the brains of undergraduate computer science students without experience in cryptography process cryptography concepts and if the order in which RF and RU are used influences where in the brain these concepts are processed. The use of fMRI scans of subjects' brain activity while responding to cryptography questions is novel and has the potential to provide significant, new measurements of conceptual understanding of cryptography concepts that change the current understanding of how instruction shapes learning in cryptography.

Purpose of the Study

This study followed two threads of investigation. First, the research sought to determine if the order of cryptography instruction focused on RF and RU, respectively, has a significant influence on students' learning of cryptography concepts and if differences in subjects' prior knowledge of mathematics played a role in their understanding of cryptography concepts. This was the "cryptography learning" thread. Second, the research attempted, using fMRI, to find common areas of brain activation among all study participants while they process cryptography concepts and to ascertain if the order of instruction (RF-RU vs. RU-RF) produces any visible differences in how cryptography concepts are processed. This thread was focused on cognitive processing of cryptography. Better understanding of the impacts of RF and RU instructional methods on cryptography understanding attempted to provide insight into how cryptography instruction can be used more effectively toward the goal of increasing the size and effectiveness of the cybersecurity workforce. Measuring cognitive processing of cryptography concepts was performed to provide additional, novel insight into the influences of instructional methods on learning cryptography concepts, in an attempt to further assist in the development of the aspects of information security instruction related to cryptography, and potentially, other related fields. Because the two research threads undertaken in this study approached the problem of cryptography learning from very different starting points, this document discusses the supporting literature, research methodologies, and results separately. Because both research threads converge on the same problem, discussion of results, conclusions and future work have combined aspects of both research threads in order to form a common path forward.

THE STUDY OF THE ORDER OF INSTRUCTIONAL METHOD ON CRYPTOGRAPHY LEARNING

Literature Review

This study investigated the impacts that the order of cognitivist instructional interventions in support of representational understanding and representational fluency have on undergraduate information security students' learning of key cryptography concepts. Additionally, this research investigated whether the RF before RU instructional method produces activation in the brain different from the RU before RF instructional method as measured using fMRI scans. Literature in the following sub-sections defines expertise and conceptual knowledge, discusses the role of knowledge taxonomies in learning, discusses the basis in cognitive learning theory for the instructional methods used in the study including the relationship between representational understanding and representational fluency, and provides insight into why and how fMRI may be used to measure cognitive processing in support of educational goals in cryptography and more broadly, information security.

Conceptual Knowledge and Problem Solving

In their discussion of the need for greater numbers of information security practitioners in the United States, McGettrick (2011) and Schneider (2013) distinguish between technically proficient operators and those who are able to apply information security concepts to solve novel problems. The distinction between those who can apply concepts in a domain and those who are technically proficient has been the subject of research, which has attempted to understand expertise using subject matter from many domains of knowledge including physics and chemistry. Chi, Glaser, and Farr (1988) summarize the properties of expertise across knowledge domains by describing the behavior of experts during problem solving. They note that experts categorize problems within their domains of expertise by the principles of the domain represented in the problem, whereas novices categorize problems in the domain by physical objects presented in the problem or similarly superficial aspects of the problem (Chi, Glaser, & Farr, 1988, p. xix). Experiments performed using physics and chemistry problems support Chi, Glaser, and Fahr's generalizations about the process that experts use to solve problems in their domains of expertise.

Chi, Feltovich, and Glaser (1981) examined differences in the ways experts and novices in physics categorized physics problems and what types of knowledge was associated with the classifications made by each group. The examination asked eight Ph.D. students in physics and eight undergraduate students, who have recently completed one semester of physics mechanics, to categorize 24 physics problems written on index cards (Chi, Feltovich, & Glaser, 1981, p. 123). Quantitative analysis of the categorization of problems by each group of students found that both novice and expert groups produced statistically similar numbers of categories and that both groups placed a similar number of cards in each category, though experts did so more quickly -- 18:45 on average for novices versus 12:30 for experts (p. 124). Qualitative analysis of the categories generated by experts and novices revealed that novices categorized the problems by what types of objects were contained in the problem, such as classifying together rotating objects or problems with inclined surfaces, whereas problem categories produced by experts were based on physics laws, such as Newton's Laws of Motion (p. 125).

Kozma and Russell (1997) performed a variant of the physics problem sorting experiment performed by Chi, Feltovich, and Glaser (1981) using 11 chemists working in the field or Ph.D. students as experts and 10 undergraduate chemistry students as novices. Subject were asked to sort 14 note cards containing chemistry problems or phenomena. In contrast to Chi, Feltovich, and Glaser (1981), some of the notecards used in Kozma and Russell's (1997) study presented the chemistry problem or phenomenon as an image, while other cards presented material in text or using mixed media (a graph with text, for example) (Kozma & Russell, Multimedia and understanding: Expert and novice responses to different representations of chemical phenomena, 1997, pp. 953-954). The quantitative results of Kosma and Russell's (1997) two sorting activities noted that experts produced groups with more cards per group in both the first sort (experts: 3.23 average number of cards per group, SD: 1.82, novices: 2.62 average number of cards per group, SD: 0.89, $p<0.0001$) and the second (experts: 3.35 average number of cards per group, SD 1.61, novices 2.62 average number of cards per group, SD 1.06, $p <0.01$). Experts in this research also produced fewer groups in both the first sort activity (experts: 4.4 groups, SD:

1.69, novices: 6.5 groups, SD: 0.71, p<.0015) and the second (experts: 4.18 groups, SD: 1.17, novices: 5.33 groups, SD: 0.86, p<.053) (Kozma & Russell, Multimedia and understanding: Expert and novice responses to different representations of chemical phenomena, 1997, p. 955). Qualitatively, Kozma and Russell's (1997) analysis resulted in the same conclusion as Chi, Feltovich, and Glaser (1981). Experts created groups of problems or phenomena based on principles governing the field while novices categorize based on superficial features – the subject matter of the problem, or phenomena (Kozma & Russell, Multimedia and understanding: Expert and novice responses to different representations of chemical phenomena, 1997, p. 960).

What researchers have determined about expertise by studying experts and novices in a knowledge domain is that experts have deep understanding of both technical knowledge in their domains of expertise, as well as knowledge of the laws or principles governing their domains of expertise. Understanding of knowledge domains and how those domains interact with each other is conceptual knowledge (Rittle-Johnson, 2006). If the needs of the information security domain as articulated by McGettrick (2011) and Schneider (2013) are to be met, then information security practitioners with deep conceptual knowledge in the domain must be found or created.

Knowledge Taxonomies

If educators are to create professionals able to design, build, and adapt systems for security, they must: be able to understand the competencies required of information security professionals, communicate those competencies to stakeholders in education and industry, instruct learners in the appropriate competencies, and be able to assess learners' demonstrations of competencies (Bloom, 1956, p. 2). Educators are able to build standards of competencies, communicate those competencies, educate, and evaluate learners based on relevant competencies by using knowledge taxonomies. In cryptography education, understanding and communicating competencies to stakeholders, providing effective instruction, and building instruments that yield effective assessment of the desired cryptography competencies all present challenges to the creation of information security professionals with deep conceptual knowledge in the field. In order to gain a complete understanding of Evans and Reeder's (2010), McGettrick's (2011), and Schneider's (2013) knowledge goals and associated competencies for information security learners, educators and industry stakeholders first need to define the abilities and behaviors required (Bloom, 1956, p. 36-37) of new professionals and be able to communicate them within the field before learners are able to demonstrate the ability to “design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate, and reconstitute from damage due to system failures and attacks,” (Evans, & Reeder, 2010, p. iv) in systematic and reproducible ways. For example, does an information security professional need to understand how to execute the Chinese Remainder Theorem (CRT) by hand, is it sufficient for the professional to know that CRT is used to solve quickly solve equation with different moduli, or must the professional understand deeply the number theory underpinning CRT in order to design, build, and adapt secure systems? Further, what relationships between the CRT and other cryptography knowledge are essential for learners to demonstrate in order for learners to possess the appropriate depth of conceptual knowledge and what standard terminology is to be used to communicate these goals and competencies among members of the field with accuracy and precision?

Based in educational psychology, educational taxonomies of knowledge have been created to classify knowledge goals, provide a common language for communication of knowledge goals, and assist educators in assessing learners’ knowledge against educational goals and stages of learning (Bloom, 1956, pp. 2-3; O’Neill & Murphy, 2010). The most used taxonomies of knowledge define levels or stages of understanding of domain knowledge and organize knowledge levels hierarchically with levels of understanding increasing in abstraction as learners move from lower to higher levels within the taxonomy (Bloom, 1956, p. 2; Anderson, et al., 2001; Biggs & Collis, 2014, p. 212). Knowledge taxonomies also associate behaviors to be exhibited by learners at each level of understanding. Because knowledge taxonomies also provide in-depth descriptions of levels of understanding and associated behaviors including sample evaluation questions, knowledge taxonomies facilitate educational goal setting and a standardized reference for the communication of educational goals (Bloom, 1956; Biggs & Collis, 2014).

The classifications of understanding and behavioral associations developed in knowledge taxonomies can also facilitate the creation in information security of instruction and evaluation tools that effectively instruct and evaluate learners in the behaviors and competencies required of information security professionals who possess the requisite skills. The cognitive domain of Bloom's Taxonomy, for example, defines a six level hierarchy of complexity by which leaners' understanding of domain knowledge can be classified. At its most basic, Bloom defines learners' understanding of information in a domain as "Knowledge", the ability to recall and or recognize domain information that was presented. As learners' understanding of the domain grows in complexity, learners become able to demonstrate: "Comprehension" by interpreting or translating domain information, "Application" by applying domain principles to specific situations, "Analysis" by categorizing, comparing, and contrasting information in the domain, "Synthesis" by integrating new information into categorizations of information, and "Evaluation" by making judgements about information using domain-specific standards. Through knowledge taxonomies such as Bloom's, stakeholders in information security education can map learning goals and behaviors, such as those presented broadly by Evans and Reeder (2010), McGettrick (2011) and Schneider (2013) using a structured methodology. The common understanding of domain-specific learning behaviors, knowledge and competencies, standardized through the use of knowledge taxonomies, serve as the basis for communication, development and implementation of instruction, and evaluation in the field.

In addition to a lack of formal educational goals, instruction in information security is also challenged because research into the use of novel instructional methods and evaluation tools in support of educational goals in STEM fields is ongoing, so providing effective instruction and evaluation remains a work in progress. For example, research in STEM instruction provide evidence that knowledge of information in a knowledge domain may require different methods of instruction and evaluation than understanding of concepts, laws, and interactions between knowledge in a domain (Lesh, Post, & & Behr, Representations and translations among representations in mathematics learning and problem solving, 1987; Kaput, Noss, & Hoyles, 2002). In terms of Bloom's Taxonomy as it applies to STEM fields, different instructional methods may be required to produce understanding at the Knowledge and Comprehension levels than are needed to produce understanding at the Synthesis or Evaluation levels. If different levels of understanding of a domain among learners were best facilitated by different instructional methods and if information security experts, consistent with the definitions of expertise developed through research in expertise such as Chi, Feltovich, and Glaser (1981), then research focused on how different instructional methods impact learning within the information security domain can provide critical information to educators seeking to build information security experts. Because the ability to build conceptual knowledge is a key aspect of creating expertise in learners, research which supports the creation in STEM fields of instruction designed to build conceptual knowledge may provide insight into how the creation of conceptual knowledge may be built through instruction in the information security domain.

The Role of Representational Understanding and Representational Fluency in Constructivist Theories of Learning

Constructivist theories of learning begin with the assertion that all knowledge is constructed (Lesh & Doerr, Beyond constructivism: Models and modeling perspectives on mathematics problem solving, learning, and teaching, 2003). Primary work in constructivist learning theory was performed by Jean Piaget who theorized that, while acquisition of knowledge required physical development of the brain, the processes of physical development and learning were distinct (Piaget, 1964, p. 176). Development is a biological process (p. 176) which occurs in stages (p. 177) and concerns all of the structures of knowledge (p.176) while learning is a process that impacts particular knowledge structures based on specific problems or encounters with objects and is gained through experiences (Piaget, 1964, p. 176) that build and revise logical frameworks in the mind (p. 186). Experiences with objects transform what is to be known, rather than simply encountering passively what is to be known (Piaget, 1964, p. 176). Piaget also theorizes that knowledge structures, or mental models in more recent research, (Lesh & Lehrer, Models and modeling perspectives on the development of students and teachers, 2003; Dark & Manigault, 2006; Delice & Kertil, 2015) are dynamic, not static, structures. That is, when one interacts with an object to be known multiple times, each interaction may modify existing mental models (Piaget, 1964, p. 177).

Jerome Bruner extended Piaget's theories by proposing that knowledge is represented in enactive, symbolic, and iconic forms. Knowledge in these three representational forms is processed into human mental models (Bruner, 1964, p. 2). Bruner refers to enactive representations as the use of gestures or activities to refer to previously encounters with concepts, symbolic representations as coded systems such as language or mathematical formulae that reference concepts in abstract ways, and iconic representations as images or other ways of organizing objects in time, space, or quantity (Bruner, 1964, p. 2). Bruner adds that iconic representations “summarize events” (Bruner, 1964, p. 2) and emphasize both qualitative and quantitative aspects of knowledge through the organization of objects and images (Bruner, 1964, p. 2). In other words, Bruner’s description of iconic representation includes physical and visual models of events and phenomena.

More recent research by Moore, Miller, Lesh, Stohlmann, and Kim (2013) extended Bruner’s original three representational forms by which humans process knowledge (p. 145) to five: concrete, symbolic, language, pictorial, and realistic, in support of post-secondary education in engineering (p. 146). The realistic representational form refers to real-world experiences like those described by Piaget (1964) and Bruner’s enactive representational form. More, Miller, Lesh, Stohlmann, and Kim’s (2013) symbolic and language representational forms separate the language component from Bruner’s symbolic representation from other types of written symbolic representations, such as mathematical formulae. Bruner’s iconic representational form is similarly separated by Moore, Miller, Lesh, Stohlmann, and Kim into a pictorial representational form inclusive of graphical representations and concrete representations, such as physical models (Moore, Miller, Lesh, Stohlmann, and Kim, 2013, p. 145).

In constructivist theory as expressed by Piaget and Bruner, active interactions with objects build and modify mental models, but the representations in which the interaction takes place matters. Mental models contain domains of knowledge content with which one has interacted, as well as knowledge about the interaction between knowledge domains. Subsequent interactions with an object provide a learner with more information about the object in different ways including when the object is presented to the learner using a different form of representation since each type of representation emphasizes or de-emphasizes different aspects of concepts or phenomena (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 146). Therefore, knowledge gained by learners through an individual representation, such as a mathematical formula describing an object, change if that learner subsequently interacts with a graphical representation of the object, such as a graph or image. The representational form in which knowledge is presented to a learner impacts which properties of an object a learner learns.

When learners first interact with a representation of knowledge, learners must determine what information the new representation is presenting and how it is being presented, as well as how the new knowledge fits into the existing mental model (Ainsworth, 2006). Learners may be presented with multiple representations of knowledge in the same representational form in order to assist them in the process of integrating the new knowledge into their existing mental models. Employing both a pie chart and a number line to illustrate fractions of a whole is an example of instruction using of two pictorial representations, for example. Learners are able to demonstrate understanding of the concept of fractions by expressing the connections between the two pictorial representations (Rau, Scheines, Aleven, & Rummel, 2013, p. 1), such as what represents the part in each graphic and what represents the whole. Learners who are able to demonstrate concepts in a knowledge domain using multiple representations in the same form have achieved a “conceptual understanding of these representations” (Rau, Scheines, Aleven, & Rummel, 2013, p. 1), which defines representational understanding according to Rau, Scheines, Aleven, & Rummel, (2013). Defined in more detail, when a learner knows what information is presented in a particular representation, how the information is presented, and how to evaluate the knowledge presented in terms of his existing mental model using a particular representational form, the learner has achieved representational understanding, an understanding of a representational form at the conceptual level (Ainsworth, 2006, pp. 186-187).

Longitudinal research on the development young learners’ conceptual understanding of evaporation provides an example of building of understanding using a single type of representation, as well as the key drawback of the use of a single representational form when instructing or evaluating conceptual knowledge (Tytler, Prain, & Peterson, 2007). Researchers in this study attempted to teach nine eleven-year-old students about the concept of evaporation using the pictorial representational form as defined by (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 145). While participating in the instructional activities about evaporation, the learners filled out worksheets on which they were asked to represent their understanding of the concept of evaporation in a series of drawings and in an interview with researchers (Tytler, Prain, & Peterson, 2007, pp. 319-320). Learners were subjected to a final interview with researchers to discuss the learners’ views on the concept of evaporation one year after the presentation of the instructional module (p. 320). After analyzing the content of the final interviews that four of the nine research subjects held a “scientifically accurate” view of evaporation (p. 321). While it is not clear how many of the subjects in this study held “scientifically accurate” views of the concept of evaporation prior to the instructional module, it is clear that only roughly half of the subjects held a “scientifically accurate” view of the concept a year after the module was instructed and some of the learners came to their understanding during verbal exchanges with researchers during the interview process (p. 321). Conceptual understanding of evaporation in this study came from the use of pictorial representation alone for very few (or none) of the learners and assessment of conceptual knowledge was not sufficiently demonstrated through pictorial representation alone. Evidence presented in this study supports the claim that, if learners were to demonstrate “scientifically accurate” view of the concept of evaporation, learners would have to translate their understanding from a pictorial representation to a language representation.

The ability to translate knowledge among different representational forms is known as “representational fluency” (Lesh & Lehrer, Models and modeling perspectives on the development of students and teachers, 2003). Translation among representational forms further integrate Piaget’s (1964) theories of learning in which additional experiences force the learner to modify the learner’s mental model in order to incorporate new information. Successfully integrating new knowledge into a mental model effectively when new and existing knowledge has been presented in different representational forms requires the ability to translate between representations. That is, one must understand the connections between representations of knowledge in several different forms, rather than within a single representational form. Because different representational forms emphasize some aspects of the knowledge they represent and remove emphasis from other aspects, one must possess a deep understanding of the knowledge being translated in order to do so accurately and precisely. Since translating knowledge into multiple representational forms requires deep understanding of the knowledge represented, the ability to translate among different representational forms serves as a proxy for deep conceptual knowledge (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 145).

Several researchers have shown that instructional methods that include instruction in representational fluency have been effective in increasing learning in students in STEM fields (Kozma, Chin, Russell, & Marx, 2000; Moore, Miller, Lesh, Stohlmann, & Kim, 2013; Hill, 2015) including in mathematics (Lesh, Post, & & Behr, Representations and translations among representations in mathematics learning and problem solving, 1987; Delice & Kertil, 2015). Benefits of information assurance instruction that includes representational fluency have also been proposed by Dark and Manigault (2006). Kozma, Chin, Russell and Marx (2000) built on Kozma and Russell (1997), which studied differences in expert and novice knowledge of chemistry by performing an observational study of three practicing chemists, two graduate students, and one post-doctoral fellow in an academic lab. Kozma and Russell analyzed written artifacts, observations, and interview transcripts with the study participants and determined that the practicing chemists (including the post-doctoral researcher) moved easily between representational forms when interacting to solve problems presented by their work (Pp. 119-122). Further, the researchers discovered that, when the professional chemists worked assisted the graduate students, the professional chemists guided the graduate students through the translation in representational forms in order to illustrate the problem and solution to the problem most effectively (Pp. 129-134). Kozma, Chin, Russell, and Marx (2000) provides support for the use of representational fluency in chemistry education to solve real-world chemistry problems. In order to attempt to determine how the use of representational forms and representational fluency impacted students' conceptual understanding, Moore, Miller, Lesh, Stohlmann, and Kim (2013) performed an observational study of 55 engineering graduate students (16 groups of 3 or 4 students) as they worked through the process of learning the concept of heat transfer (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 147). In order to instruct students in heat transfer, students were tasked with completing a model-eliciting activity designed to expose and correct two misconceptions about heat transfer widely observed in undergraduate students by their instructors: that heat and temperature are equivalent and that temperature of an object determines how someone perceives the temperature of that object when contacting it (Moore, Miller, Lesh, Stohlmann, & Kim, 2013, p. 147). The authors observed and recorded the students at work, then examined and coded data from recordings and artifacts. As students began to explore the concept of heat transfer, researchers observed the students demonstrating an incomplete and fluid understanding of heat transfer concepts. As students worked through and completed the MEA, which facilitated representational fluency, researchers found that students' conceptual understanding of heat transfer evolved from partial understanding containing misconceptions and distortions to a sharper and more complete understanding of the concept.

Research in representational understanding and representational fluency provides evidence in support of the importance of both representational understanding and representational fluency in building deep conceptual understanding in STEM fields. However, it remains uninvestigated how the order of instruction in representational understanding and representational fluency impact learning. For example, must learners first achieve representational understanding in several representational forms within a knowledge domain in order to maximize learning from instruction in representational fluency? Is the reverse true? Or, does the order of instruction in terms of representational understanding and representational fluency matter at all? Understanding the potential impacts of the order of instruction focused on representational understanding and instruction focused on representational fluency in cryptography learning is important to educators' ability to produce information security professionals with conceptual facility that will be able to meet current and future industry and national security needs for information security professionals.

Calculus and its Influence on Cryptography Learning

As an applied discipline of mathematics, cryptography depends on learners' development of an understanding of a sub-set of mathematical principles because cryptographic systems derive their strength from mathematical calculations that are computationally simple to compute in one direction, but difficult to reverse without knowledge of a key. The hard mathematical problem underlying cryptosystems (factorization of large numbers, finding discrete logarithms, finding points on elliptic curves) can vary among those cryptosystems and some systems can operate using more than one type of hard mathematical problem. Yet, despite the varied mathematics underpinning cryptosystems, cryptography courses in computer science programs usually require knowledge of calculus as prerequisite. It is often (as is the case at the university in which this study was performed) the only mathematical prerequisite to the undergraduate introductory cryptography course. This section explores the relationship between calculus and cryptography learning.

Calculus is a gateway course to further study in many science and engineering disciplines (Bressoud, Carlson, Mesa, & Rasmussen, 2013). According to the International Journal of Mathematical Education in Science and Technology, approximately 300,000 students take an introductory calculus course (p. 685) each fall on their way to such disciplines. The volume of students from various science and engineering disciplines taking calculus suggest that the study of calculus imparts knowledge foundational to the understanding of science and engineering disciplines. Calculus is the study of the relationship between changing systems (Boyer, 1959, p. 6). A commonly-used example of calculus at work illustrates the relationship between distance, velocity, and acceleration. Through calculus, learners are shown how, through differentiation and integration, distance traveled of an object relies on its derivative velocity, which is itself dependent on its derivative, acceleration. Accordingly, change in acceleration impacts velocity, and by extension, distance traveled (Boyer, 1959, p. 9). The example of the relationship between distance and velocity and velocity and acceleration modeled by calculus illustrates how calculus models logic in physics, but extrapolation of the principles of calculus to cryptography is slight. Beyond direct applications of calculus to cryptography problems, the study of calculus teaches learners a process by which they can model and understand relationships between continuously changing systems that applies broadly across scientific disciplines (Boyer, 1959, p. 6). Specific applications of calculus to cryptography are numerous. Basic cryptography concepts, such as the cancellation of cryptographic strength once the adversary has the key, have been modeled in calculus as have electronic attestation schemes, electronic voting protocols, and zero-knowledge proofs, among others (Chadha, Delaune, & Kremer, 2009). While calculus is clearly applicable to cryptography and cryptography learning, the nuances of how cryptography learning is impacted by various aspects of calculus has not been sufficiently investigated.

Methodology

Research Questions

This research explored whether undergraduate-level university students majoring in computer science, but without formal instruction in cryptography, gained deeper understanding of cryptography concepts when instruction focused on representational fluency first, rather than representational understanding or vice-versa. Further, how does prior knowledge impact success in learning cryptography concepts?

Hypotheses

The hypotheses tested in this research were:

1) H_{0a}: The order in which instructional methods are ordered, "Representational Understanding before Representational Fluency" or "Representational Fluency before Representational Understanding" produce no statistically significant difference in learning gain at α=0.05. The alternate hypothesis investigated in this research was bi-directional.

2) H_{0b}: Differences in prior knowledge of mathematics in pre-cryptography, undergraduate computer science majors have no statistically significant effect on cryptography learning at α=0.05. Again, the alternative hypothesis was that any statistically significant effect was observed.

Variables and Operationalization

In order to test hypotheses H_{0a} and H_{0b}, the independent variable "Instructional Method" (IM) was defined. IM represents the order in which instructional goals of representational understanding and representational fluency in cryptography were supported by instructional methods and had two potential states. The "Representational Understanding First" (RU-RF) condition represents the instructional goal of representational understanding of language, mathematics, and graphic representations using instruction in cryptography and is followed by instructional support for representational fluency. The "Representational Fluency First" (RF-RU) condition represented the condition in which representational fluency was presented in instruction prior to support for representational understanding. "Learning Gain" (Gain) and "Combo" (Combo) were operationalized as measurements of the cryptography learning dependent variable. "Learning Gain" was defined by differences in pre and posttest results is the dependent variable. Statistically significant differences in pre and posttest results among instructional conditions provide evidence for hypothesis 1a related to the order of instructional conditions. The "Combo" operationalization of the dependent variable combined subjects' posttest score and their score on the cryptography questions presented to them under fMRI scan, the “fMRI Score” operationalization of the dependent variable. The “Combo” and “fMRI Score” variables provide different perspective on subjects’ cryptography learning, in part, because the pre and posttests focused on testing conceptual knowledge while “fMRI Score” focused on testing representational fluency. Both the “Learning Gain” and “Combo” operationalizations of cryptography learning served as regressands in the analysis of hypothesis 1b.

Data collection and analysis of the second set of learning hypotheses made in this study also used the “Learning Gain” and “Combo” as regressands representing the dependent variable cryptography learning, but representations of the independent variable “Prior Mathematics Knowledge” were defined as regressors. “Prior Mathematics Knowledge” was operationalized in support of hypothesis 2a by collecting from each subject a list of the University’s mathematics courses that they had passed at the University either by attending the course or by testing out prior to attendance. Table 1 below lists the University’s alphanumeric designation of the courses used as regressors in this analysis, followed by the University’s course description (Purdue University, 2019).

Table 1: Course Designations and Descriptions representing “Prior Mathematics Knowledge”

MA161	"Introduction to differential and integral calculus of one variable, with applications"
MA162	"Continuation of MA 161. Vectors in two and three dimensions, techniques of integration, infinite series, conic sections, polar coordinates, surfaces in three dimensions."
MA163	"Topics from plane analytic geometry. Introduction to differentiation and integration. Applications."
MA165	"Introduction to differential and integral calculus of one variable, with applications. Conic sections. Designed for students who have had at least a one-semester calculus course in high school, with a grade of "A" or "B", but are not qualified to enter MA 16200 or 16600, or the advanced placement courses MA 17300 or 27100, or the honors calculus course MA 18100. Demonstrated competence in college algebra and trigonometry."
MA166	"Continuation of MA 16500. Vectors in two and three dimensions. Techniques of integration, infinite series, polar coordinates, surfaces in three dimensions."
MA261	"Planes, lines, and curves in three dimensions. Differential calculus of several variables; multiple integrals. Introduction to vector calculus."
MA351	"Systems of linear equations, finite dimensional vector spaces, matrices, determinants, eigenvalues and eigenvector applications to analytical geometry."

In addition to individual course regressors, the "Group" regressor was defined, which served as a operationalization of "Prior Mathematics Knowledge" by level, rather than by course. That is, subjects who had taken neither MA165 nor MA166 were designated as group 3, those who had taken either MA165 or MA166 were designated as group 2, and those who had taken both MA165 and MA166 were designated as group 1. These groupings were created in order to isolate cryptography knowledge by level, which allowed more accurate testing of the influence of subjects' prior mathematical knowledge on cryptography learning.

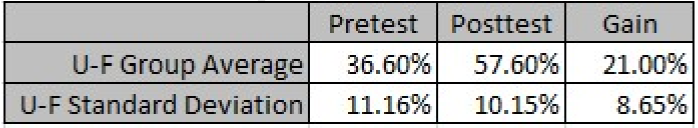
Results

Data analysis in support of the proposed learning gain hypotheses was performed from three perspectives. First, learning gain was compared between the U-F and F-U treatment groups using a t-test of the Gain variable. This test was this study's designed evaluation of learning gain. Further post hoc analyses seeking to model the direct and indirect relationships between operationalizations of the study's independent and dependent variables were also performed using linear regression. Results of these three analyses are detailed in the following three sub-sections.

Learning Gain as Proposed

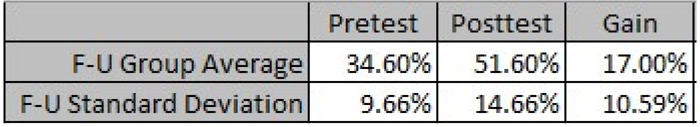
Tables 2 and 3 below present pretest, posttest, and learning gain (Gain) by subject followed by the averages and standard deviations of each by group.

Table 2: Scores and Descriptive Statistics: UF Instructional Method



	Pretest	Posttest	Gain
U-F Group Average	36.60%	57.60%	21.00%
U-F Standard Deviation	11.16%	10.15%	8.65%

Table 3: Scores and Descriptive Statistics: FU Instructional Method



	Pretest	Posttest	Gain
F-U Group Average	34.60%	51.60%	17.00%
F-U Standard Deviation	9.66%	14.66%	10.59%

Average learning gain in the representational understanding first (UF) treatment group was (μ=21.00%, σ=8.65%). UF treatment group learning gain was derived from posttest scores described as (μ=57.60%, σ=10.15%) and pretest scores (μ=36.60%, σ=11.16%). Learning gain in the representational fluency first (FU) treatment group was (μ=17.00%, σ=10.59%), derived from posttest scores (μ=51.60%, σ=14.66%) and pretest scores (μ=34.60%, σ=9.66%). Learning gain comparisons between the UF and FU groups are shown graphically in Figure 1 below. Pretest to posttest trends in score average and standard deviation are shown in Figures 2 and 3, respectively.

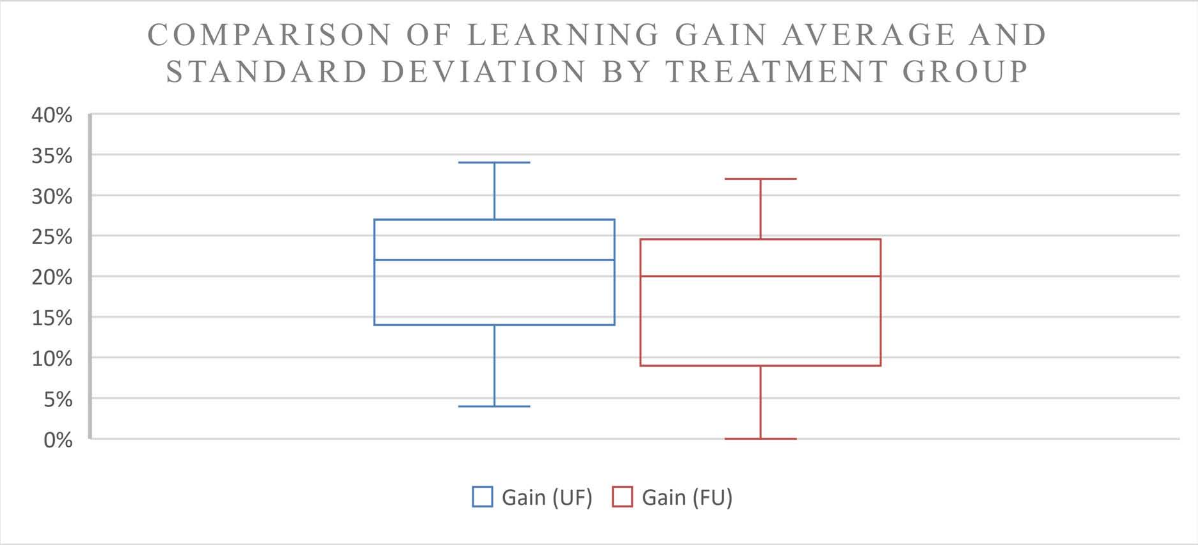


Figure 1: Comparison of Learning Gain Average and Standard Deviation by Treatment Group

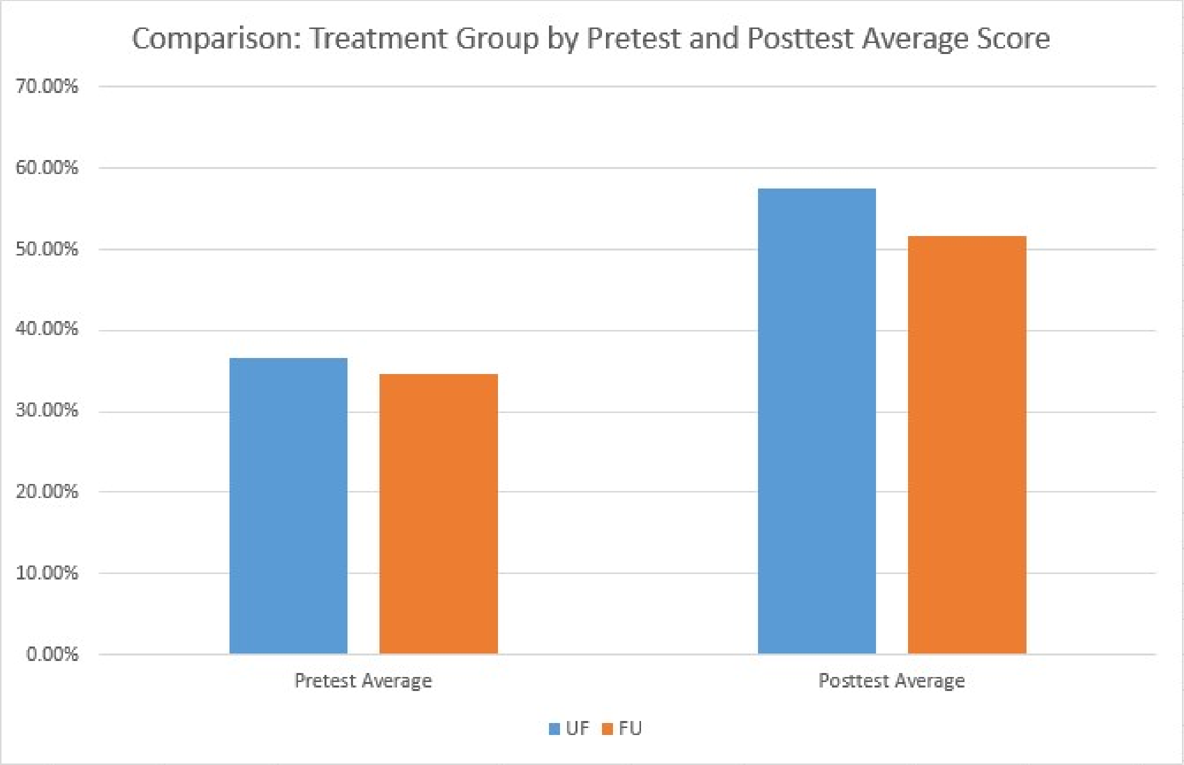


Figure 2: Comparison of UF and FU Pretest and Posttest Average Scores

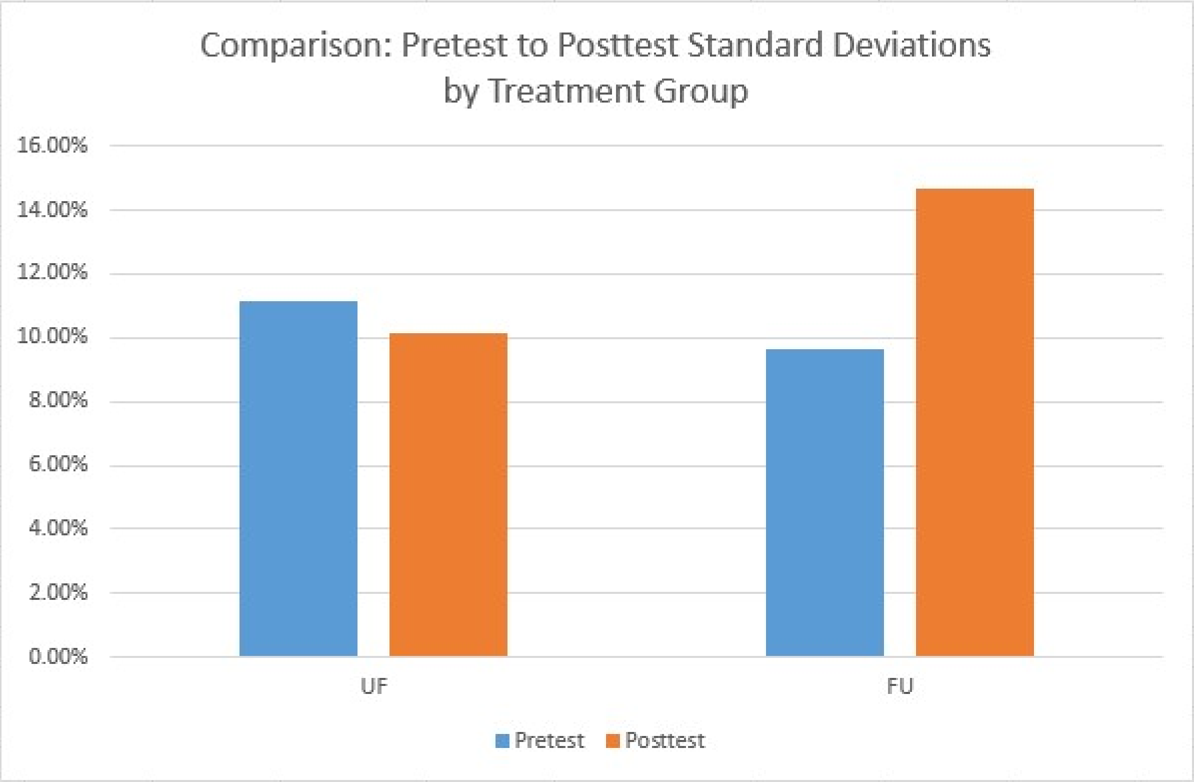
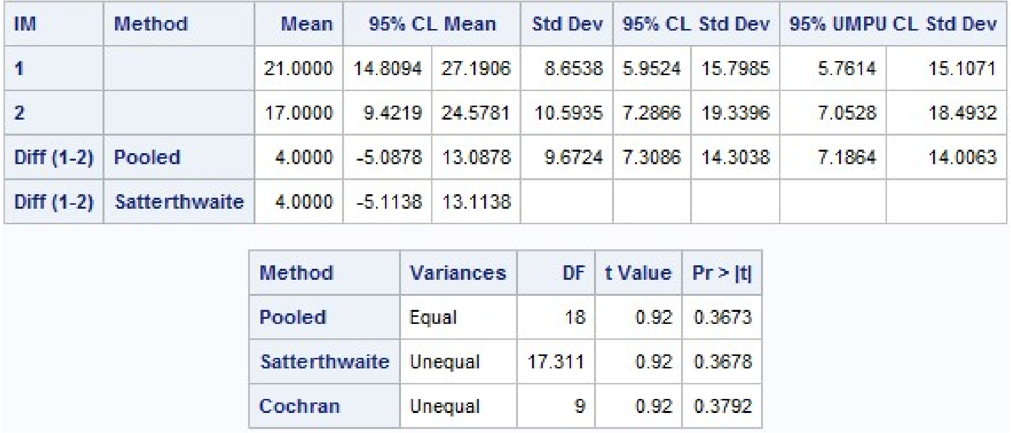


Figure 3: Comparison of UF and FU Pretest and Posttest Standard Deviations

A t-test comparing average learning gain achieved by the UF treatment group against the learning gain of the FU treatment group showed that the difference in learning gain between the UF and FU treatment groups was not statistically significant at α=0.05 (t-pooled=-0.92, p=0.37), as shown in Table 4, below.

Table 4: Results of T-test Comparing Learning Gain (Gain) by Instructional Method (IM)



IM	Method	Mean	95% CL Mean		Std Dev	95% CL Std Dev		95% UMPU CL Std Dev	
1		21.0000	14.8094	27.1906	8.6538	5.9524	15.7985	5.7614	15.1071
2		17.0000	9.4219	24.5781	10.5935	7.2866	19.3396	7.0528	18.4932
Diff (1-2)	Pooled	4.0000	-5.0878	13.0878	9.6724	7.3086	14.3038	7.1864	14.0063
Diff (1-2)	Satterthwaite	4.0000	-5.1138	13.1138					

Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	18	0.92	0.3673
Satterthwaite	Unequal	17.311	0.92	0.3678
Cochran	Unequal	9	0.92	0.3792

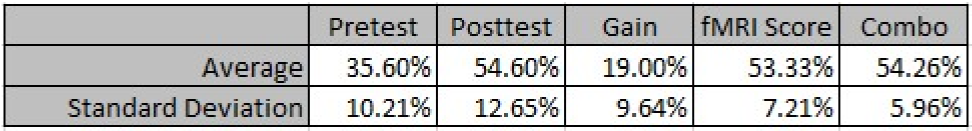
Difference in variances between treatment groups were not significant (F=1.50, p=0.56). A t-test also confirmed that the two treatment groups' pretest scores did not differ in a statistically significant way (α=0.05) (t-pooled=-1.59, p=0.13); the UF treatment group averaged a pretest score of 36.60% (σ=11.16%) while the FU treatment group averaged 34.60% (σ=9.66%). Variances of the groups' pretest scores were not significant at α=0.05 (F=2.20, p=0.26). The results of this analysis support the null hypothesis inH_{0a}. Cryptography learning did not differ significantly in this study based on the order in which instructional support was given for representational fluency and representational understanding.

Post-Hoc Analysis of Direct Effects of Explanatory Variables on Learning Gain

The proposed analysis of learning gain was limited in this study by the small sample size of the treatment groups. A second set of analyses was performed using stepwise linear regression of data from all twenty subjects. These data included pretest and posttest scores and data collected from subjects about their prior knowledge of mathematics as explanatory variables, Learning Gain as a response variable, and a second response variable, Combo, which combined subjects' posttest score percentage with the percentage correct that subjects achieved when answering the cryptography questions presented during the fMRI scan. Subjects' prior mathematics knowledge was operationalized by asking subjects to select the University's mathematics courses in which they either took at the University and passed, or tested out of from a list of course numbers and names. In addition to analyzing prior mathematical knowledge as individual explanatory variables, a Group variable was created which categorized subjects' prior knowledge of mathematics into the following. Group 1 includes subjects who have taken or tested out of both MA165 and MA166. Group 2 includes subjects who have taken or tested out of either MA165 or MA166. Group 3 includes subjects who have taken neither MA165 nor MA166.

Table 5 summarizes pretest, posttest, and fMRI scores from all 20 subjects', as well as scores for the "Gain" and "Combo" dependent variables. The "Combo" dependent variable was derived by adding subjects' fMRI Score results to their "Gain" results.

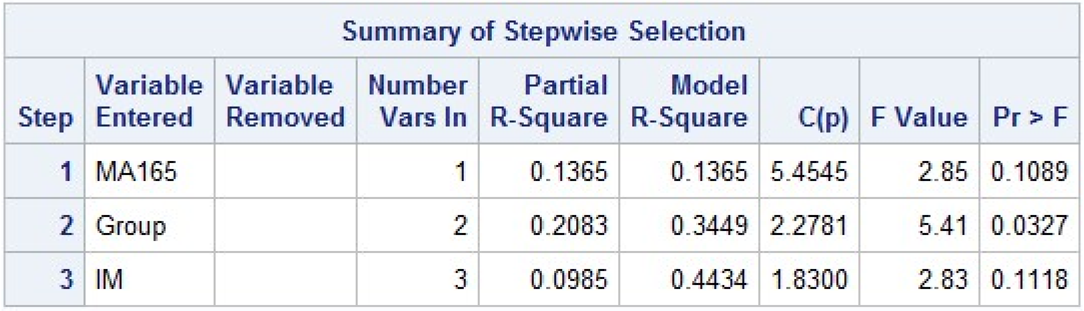
Table 5: Descriptive Statistics (n=20) Pretest, Posttest, Learning Gain (Gain), fMRI Score and Combo



	Pretest	Posttest	Gain	fMRI Score	Combo
Average	35.60%	54.60%	19.00%	53.33%	54.26%
Standard Deviation	10.21%	12.65%	9.64%	7.21%	5.96%

A summary of results of the stepwise regression that included pretest score, posttest score, and subjects' prior mathematics knowledge as explanatory variables and learning gain as represented by the Gain variable are shown in Table 6. In this analysis, the model was significant and moderately explanatory (p=.02, r^2=.44). Individually, explanatory variables representing prior successful completion of the MA165 mathematics course (understanding of the knowledge contained therein), prior mathematics knowledge (represented by the Group variable), and instructional method (represented by the IM variable) were individually significant.

Table 6: Summary of Stepwise Regression for Response Variable Gain (n=20)

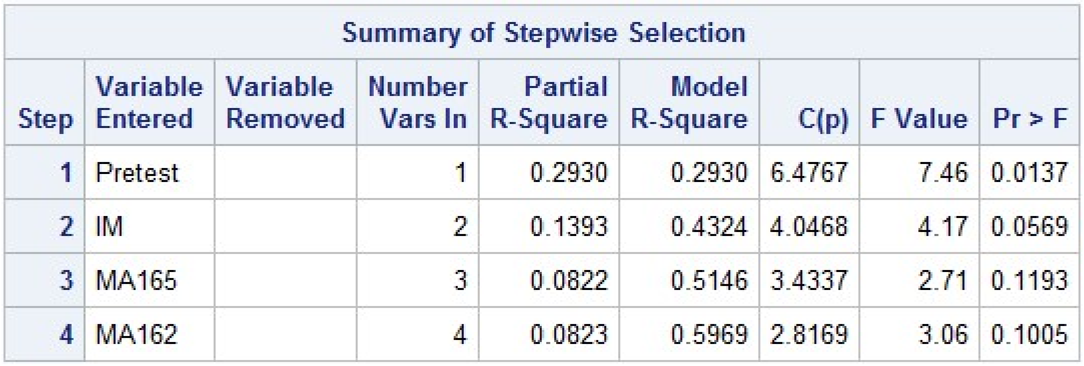


Summary of Stepwise Selection

Step	Variable Entered	Variable Removed	Number Vars In	Partial R-Square	Model R-Square	C(p)	F Value	Pr > F
1	MA165		1	0.1365	0.1365	5.4545	2.85	0.1089
2	Group		2	0.2083	0.3449	2.2781	5.41	0.0327
3	IM		3	0.0985	0.4434	1.8300	2.83	0.1118

A second stepwise regression was performed with the same set of explanatory variables using Combo as the response variable. The model with Combo, rather than Gain, as the regressand achieved greater significance and explanatory power (p=.01, r^2=.60). Results for individual variables are summarized in Table 7. Significant variables in this analysis were: pretest score, instructional method (IM), successful completion of MA165 course material (MA165), and successful completion of MA162 course material (MA162).

Table 7: Summary of Stepwise Regression for Response Variable Combo, all subjects (n=20)

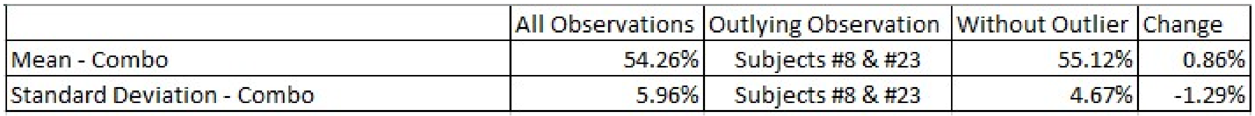


Summary of Stepwise Selection

Step	Variable Entered	Variable Removed	Number Vars In	Partial R-Square	Model R-Square	C(p)	F Value	Pr > F
1	Pretest		1	0.2930	0.2930	6.4767	7.46	0.0137
2	IM		2	0.1393	0.4324	4.0468	4.17	0.0569
3	MA165		3	0.0822	0.5146	3.4337	2.71	0.1193
4	MA162		4	0.0823	0.5969	2.8169	3.06	0.1005

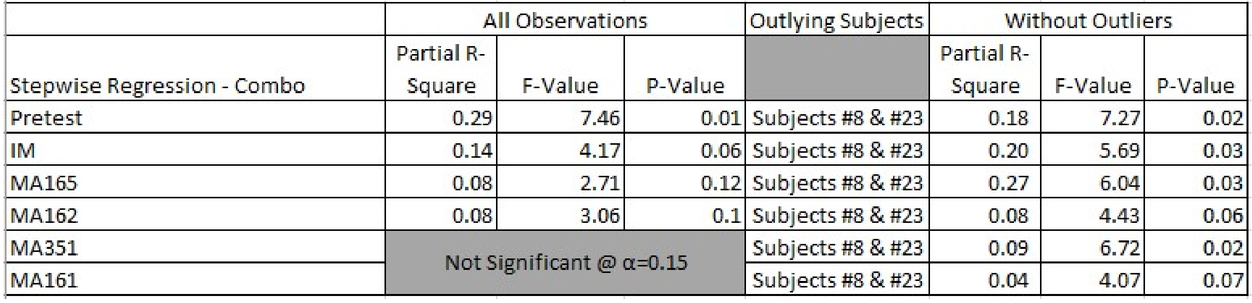
Analysis of observations of the Combo variable noted that two observations were statistical outliers. Subject #23 scored further than two standard deviations below the mean of the Combo variable score; Subject #8 scored more than two standard deviations higher than the Combo mean. To understand how these observations impacted the results above, the regression in which Combo was the regressand was re-run without the outlying observations. A comparison of the two sets of results are shown in Tables 8 and 9.

Table 8: Summary of Changes to Mean and Standard Deviation with (n=20) and without (n=18) outliers



	All Observations	Outlying Observation	Without Outlier	Change
Mean - Combo	54.26%	Subjects #8 & #23	55.12%	0.86%
Standard Deviation - Combo	5.96%	Subjects #8 & #23	4.67%	-1.29%

Table 9: Comparison of Combo Stepwise Regression Results with (n=20) and without outliers (n=18)



	All Observations			Outlying Subjects	Without Outliers		
Stepwise Regression - Combo	Partial R-Square	F-Value	P-Value		Partial R-Square	F-Value	P-Value
Pretest	0.29	7.46	0.01	Subjects #8 & #23	0.18	7.27	0.02
IM	0.14	4.17	0.06	Subjects #8 & #23	0.20	5.69	0.03
MA165	0.08	2.71	0.12	Subjects #8 & #23	0.27	6.04	0.03
MA162	0.08	3.06	0.1	Subjects #8 & #23	0.08	4.43	0.06
MA351	Not Significant @ α=0.15			Subjects #8 & #23	0.09	6.72	0.02
MA161				Subjects #8 & #23	0.04	4.07	0.07

When the outlying observations were removed from the regression against the Combo variable, the model became increasingly significant and explanatory (p<.0001, r^2=.60) and nearly all of the explanatory variables placed in the model became significant. Though six variables were statistically significant in this model, the Pretest, IM, and MA165 variables were no less than twice as explanatory as the MA162, MA351, and MA161 variables. Because of their significance and explanatory power in the modeling of direct effects, the Pretest, IM, MA165, and Group explanatory variables were further analyzed for indirect relationships with the Gain and Combo variables in an effort to understand those relationships in greater depth.

Post-Hoc Analysis of Indirect Effects of Explanatory Variables on Learning Gain using Mediation, Moderation, and Conditional Analysis

Analyses of direct relationships between the study's explanatory variables and learning gain, as operationalized by the Gain and Combo response variables, have yielded the models illustrated in Figures 4 and 5.

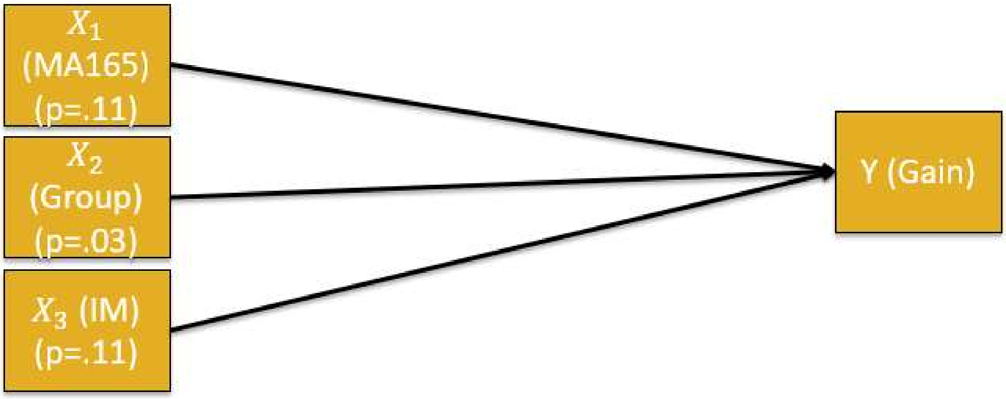


Figure 4: Direct relationship model: MA165, Group, and IM to Gain (p=.02, r^2=.44)

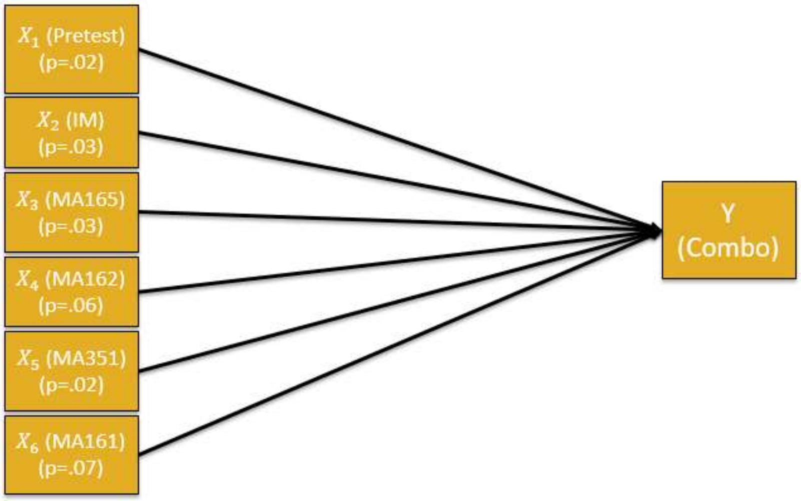


Figure 5: Direct relationship model: Significant Explanatory Variables to Comb (without outliers) (p<.0001, r^2=.65)

While the direct linear relationship models in Figures 4 and 5 were both significant and moderately explanatory, the possibility remained that a more complex model may provide more explanatory power. Further analysis investigated potential mediating, moderating, and conditional relationships among the Pretest, IM, MA165, and Group explanatory variables and the impact of those relationships on the Gain and Combo response variables.

Basic Mediation and Moderation Analysis

Unlike the direct linear relationship model shown in Figures 4 and 5 above, mediating and moderating relationships, illustrated in Figure 6, consider the influence on the response variable(s) of intervening variables or influences (Muller, Judd, & Yzerbyt, 2005, p. 853; Hayes, 2013). In mediation, variables provide a vehicle by which the influence of the explanatory variables is conveyed to the response variable(s), while in moderation, variables provide boundaries and influence the magnitude of the response to explanatory variables (Barron & Kenny, 1986; Hayes, 2013).

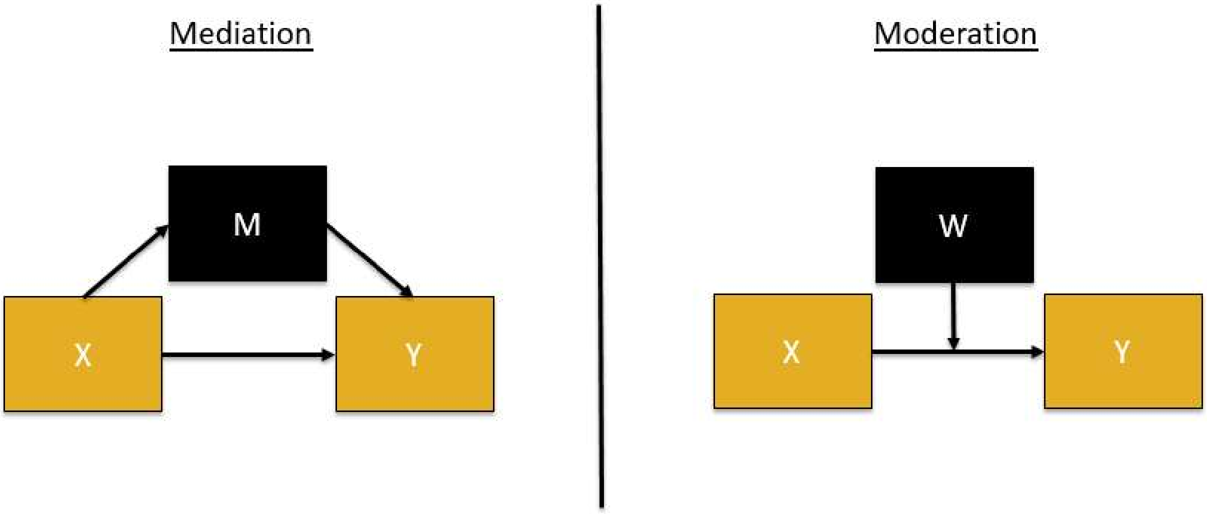
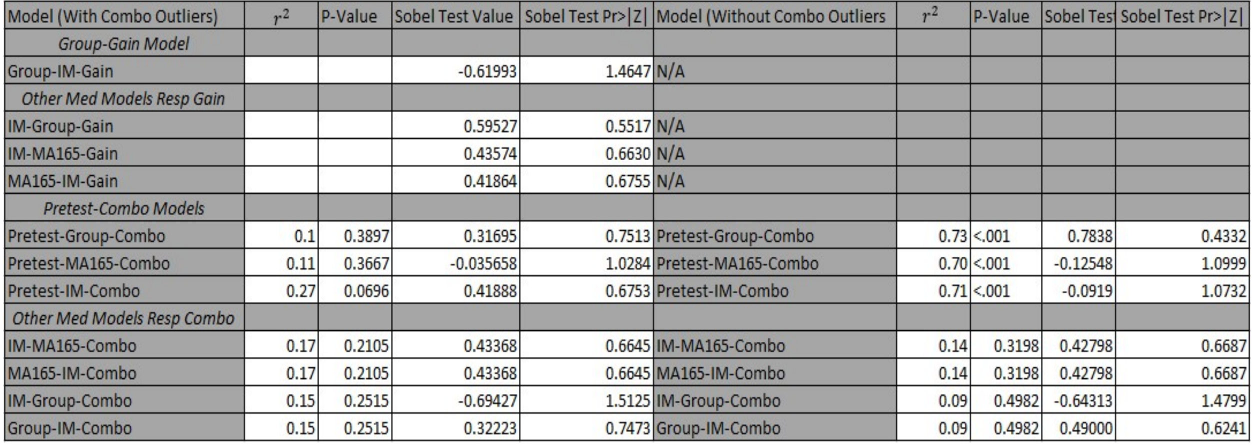


Figure 6: Examples of Mediation and Moderation Relationships among Variables where M mediates and W moderates.

Investigations of basic mediation and moderation relationships between IM and Group variables as those relationships impacted the Gain or Combo variables in this study were performed using SAS version 9.4 TS Level 1M4. Whereas later versions of SAS allowed the use of the CAUSALMED command for mediation, each mediation analysis in this sub-section was performed by combining the results of three separate regression analyses as described in (Tavakoli, Jackson, Moneyham, & Birmingham, 2009) and conducting a Sobel Test for mediating effects. Table 10 shows the results of linear regression tests of mediation effects of several relationship models. In Table 10, the r^2 and P-Value columns describe the explanatory power and significance, respectively of the model. The Sobel Test Value and Sobel Test Pr>Z columns provide the test value and significance of the mediation effect in the model. Because the Sobel Test is a Z-test, significance at ∝= .05 requires the Sobel Test Pr<Z value to be greater than 1.96 or less than -1.96. No individual variables tested produced statistically significant mediating effects.

Table 10: Mediation Analysis using the Sobel Test

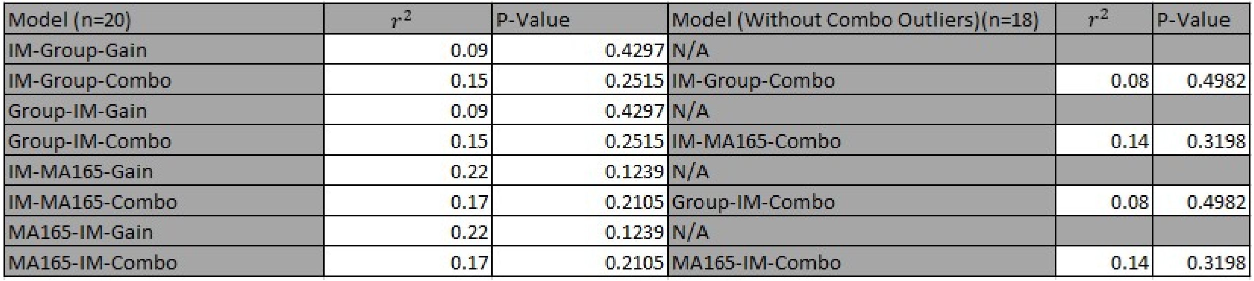


Model (With Combo Outliers)	r^2	P-Value	Sobel Test Value	Sobel Test Pr>|Z|	Model (Without Combo Outliers	r^2	P-Value	Sobel Tes	Sobel Test Pr>|Z|
Group-Gain Model									
Group-IM-Gain			-0.61993	1.4647	N/A				
Other Med Models Resp Gain									
IM-Group-Gain			0.59527	0.5517	N/A				
IM-MA165-Gain			0.43574	0.6630	N/A				
MA165-IM-Gain			0.41864	0.6755	N/A				
Pretest-Combo Models									
Pretest-Group-Combo	0.1	0.3897	0.31695	0.7513	Pretest-Group-Combo	0.73	<.001	0.7838	0.4332
Pretest-MA165-Combo	0.11	0.3667	-0.035658	1.0284	Pretest-MA165-Combo	0.70	<.001	-0.12548	1.0999
Pretest-IM-Combo	0.27	0.0696	0.41888	0.6753	Pretest-IM-Combo	0.71	<.001	-0.0919	1.0732
Other Med Models Resp Combo									
IM-MA165-Combo	0.17	0.2105	0.43368	0.6645	IM-MA165-Combo	0.14	0.3198	0.42798	0.6687
MA165-IM-Combo	0.17	0.2105	0.43368	0.6645	MA165-IM-Combo	0.14	0.3198	0.42798	0.6687
IM-Group-Combo	0.15	0.2515	-0.69427	1.5125	IM-Group-Combo	0.09	0.4982	-0.64313	1.4799
Group-IM-Combo	0.15	0.2515	0.32223	0.7473	Group-IM-Combo	0.09	0.4982	0.49000	0.6241

Of note among these results, however, were: the high significance (<.001) and explanatory power (≥.71), both absolute and relative to other models, of models in which "Pretest" was the explanatory variable and "Combo" (without outliers) was the response variable, as well as the relatively high Sobel Test PR>|Z| values of models in which "Group" and "IM" interacted.

Further regression analysis considered the potential moderating effects of the Group, IM, and MA165 variables on the IM-Gain and IM-Combo (with and without outliers) relationships. Table 11 presents results of the various regression models tested. No significant moderation effects by individual moderating variables were noted, nor were any notable patterns found.

Table 11: Moderation Analysis IM-Group-Gain



Model (n=20)	r^2	P-Value	Model (Without Combo Outliers)(n=18)	r^2	P-Value
IM-Group-Gain	0.09	0.4297	N/A		
IM-Group-Combo	0.15	0.2515	IM-Group-Combo	0.08	0.4982
Group-IM-Gain	0.09	0.4297	N/A		
Group-IM-Combo	0.15	0.2515	IM-MA165-Combo	0.14	0.3198
IM-MA165-Gain	0.22	0.1239	N/A		
IM-MA165-Combo	0.17	0.2105	Group-IM-Combo	0.08	0.4982
MA165-IM-Gain	0.22	0.1239	N/A		
MA165-IM-Combo	0.17	0.2105	MA165-IM-Combo	0.14	0.3198

Multiple Moderation and Moderated Mediation Relationshp Results

Because the possiblity exists that the relationships in this research between the instructional method used and subjects' prior mathematics knowledge may be more complex than were modeled by simple mediation or moderation analyses separately, the PROCESS procedure (Hayes, 2013) was employed to perform statistical analysis of more complex relationship models. In order to model these more complex types of relationship, the models tested were "Pretest", a measure of cryptography knowledge prior to learners' receipt of instruction, was used as the explanatory variable with IM, Group, and MA165 as mediators or moderators. The first of these tests used IM, Group, and MA165 as additive moderators. The additive moderator relationship with two moderators is illustrated in Figure 7.

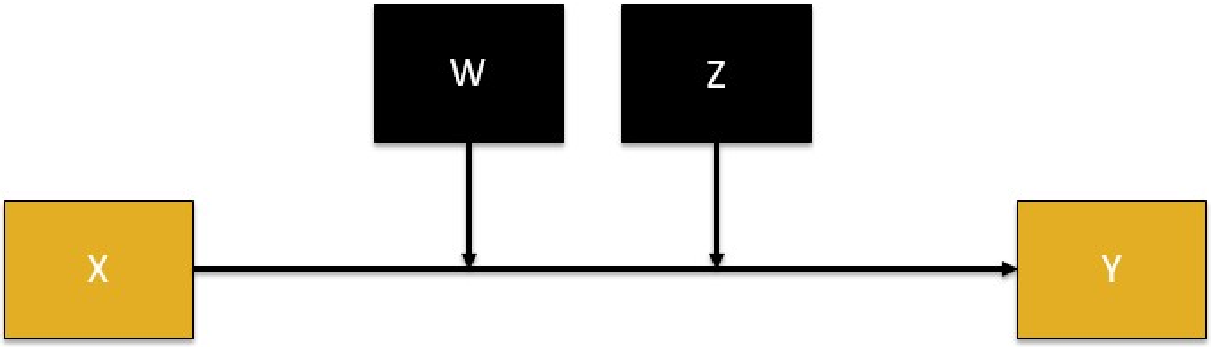
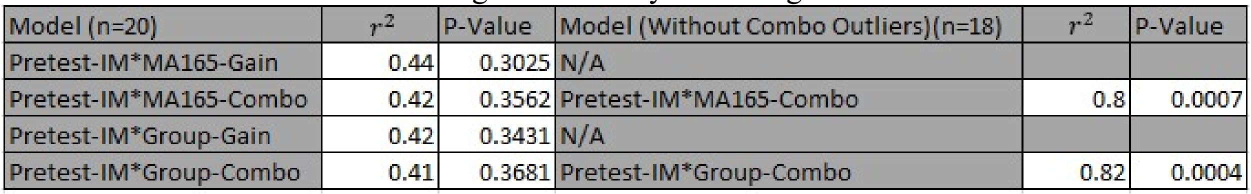


Figure 7: The Additive Moderation Relationship with two Moderating Variables (W and Z)

Results of additive moderator modeling are shown in Table 12.

Table 12: Results of Regression Analysis Testing Additive Moderation



Model (n=20)	r^2	P-Value	Model (Without Combo Outliers)(n=18)	r^2	P-Value
Pretest-IM*MA165-Gain	0.44	0.3025	N/A		
Pretest-IM*MA165-Combo	0.42	0.3562	Pretest-IM*MA165-Combo	0.8	0.0007
Pretest-IM*Group-Gain	0.42	0.3431	N/A		
Pretest-IM*Group-Combo	0.41	0.3681	Pretest-IM*Group-Combo	0.82	0.0004

Among these models, statistics describing the Pretest-Combo (without outliers) relationship, moderated by the "IM" and "Group" variables, stands out. The model of this relationship is both highly explanatory and significant (r^2=.82, p=.0004).

A moderated mediation model, in which the mediation of the relationship between the explanatory and response variables by is moderated by another variable, was also tested as a potential descriptor of the relationship between the “Pretest” and “Gain” or “Combo”. Figure 8 illustrates a generic model of moderated mediation of relationships.

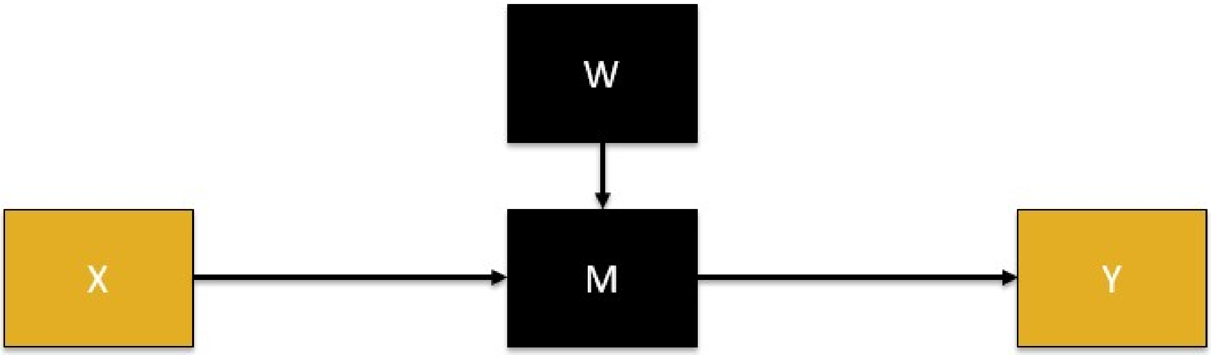


Figure 8: The Moderated Mediation Relationship (W as moderator, Z as mediator)

Modeling the Pretest-Gain relationship while using “IM” and “Group” as moderating and mediating variables (in either configuration) produced a model that was neither explanatory or significant (r^2=.08, p=.69) and in which the interactions between the “IM” and “Group” variables were also not significant. Models that used the “Combo” variable without outliers produced results that were also not significant (r^2=.32, p=.19) and in which the interaction of “IM” and “Group” were not significant.

Results of the various regression analyses presented in this sub-section support the alternative hypothesis that the effect of prior knowledge of mathematics on cryptography learning in this study is statistically significant. Prior knowledge of mathematics, with instructional method, moderates the relationship between subjects’ pretest scores of cryptography knowledge and learning gain as illustrated in Figure 9 below.

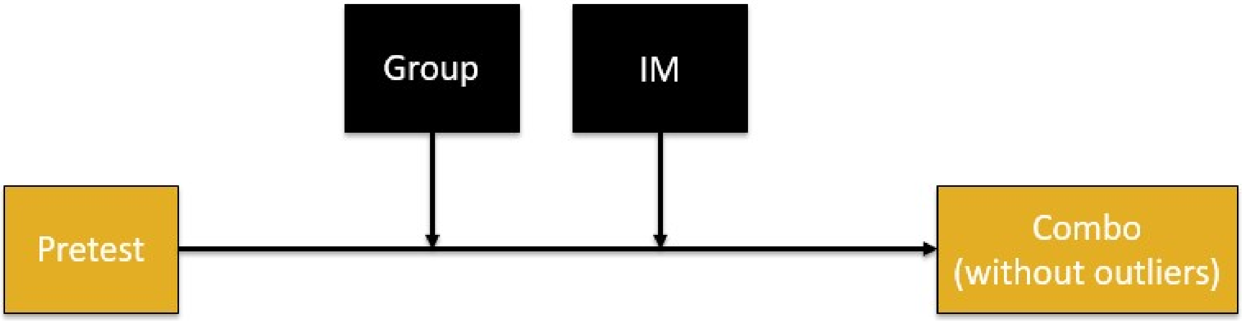


Figure 9: The linear relationship among pretest scores, prior knowledge of mathematics, instructional order, and learning gain (r^2=.82, p=.0004)

Further analysis of the additive moderation relationship model in Figure 9 quantify the influences of the moderating effects of the Group and IM variables on the relationship between subjects' pretest scores and learning gain as measured by the Combo variable without outliers. While neither the Group – Pretest nor the IM – Pretest interactions were significant at $\propto = .05$ individually, the IM – Pretest interaction was far more significant (p=.08) than the Group – Pretest interaction (p=.36). In terms of explanatory power, the IM-Pretest relationship contributed 6% ($r^2_{IM-Pretest} = .05$); the Group-Pretest contributed 1.2% ($r^2_{Group-Prete} \quad = .01$). These results suggest that the direct relationship between prior knowledge of cryptography is mostly responsible for learning gain generated by cryptography instruction, but that subjects who instructional support for representational understanding prior to representational fluency and had a stronger background in mathematics gained more knowledge of cryptography through instruction. Subjects who received instructional support for representational fluency first or had weaker math backgrounds learned less from cryptography instruction.

Assumptions

The primary assumption made in the design of this research was that subjects' prior knowledge of mathematics would not influence the results of the study. Demonstrated knowledge of calculus was a prerequisite for entry into this (and other) university's cryptography courses for computer science majors; this assumption is opposite of that practice. This research addressed two aspects of the impacts of prior mathematics knowledge on the study's results. First, the analysis tested whether or not a deeper treatment of the required calculus as indicated by successful completion of MA165 and/or MA166 influenced cryptography learning differently than a shallower one as indicated by completion of MA161 and/or MA162. Second, the study investigated whether more math taken within the university's course structure had an effect on cryptography learning. The regression models in which subjects' successfully completed prior university math courses and the Group variable were regressed against learning gain and the Combo variable were, in part, attempts to better understand what math and how much math is important to cryptography learning. The statistical tests detailed in sub-section 2.2.6.3 further analyzed potential mediating and moderating of subjects' prior knowledge of mathematics. Though this research was performed under the assumption that prior mathematics knowledge would not influence cryptography learning due to the relative homogeneity of mathematics knowledge among these subjects, this assumption was statistically tested in several ways during data analysis.

This research also assumed that subjects provided their best efforts to answer accurately questions asked of them. Though limits of subjects' attention spans were considered during the design of study instruments, any external factor that may have caused a subject to not give full effort during questioning may have a significant impact on study results due to the study's small sample size.

Limitations

Analysis of learning gain was most significantly limited in this study by the low statistical power of the analysis that resulted from the small sample size. Despite the use of multiple techniques by the researcher to recruit subjects for this study prior to and at the beginning of the semester in which the study took place, only 27 students expressed interest in participating. Of the 27, only 20 completed all of the study's activities from pretest to fMRI scan. Based on the difference in average learning gain between the treatment groups of 4%, the 20-subject sample size produced a power of only 15%. A power of 80% would have required a sample size of 192 subjects. The post-hoc analysis of the collected data was performed to compensate for the low power of the data analysis as designed.

Sub-optimal validation and standardization of the pre and posttest evaluation instruments placed further limitations on the analysis of learning gain. Because no standard, validated evaluation instrument exists for cryptography concepts, the pretest and posttest in this study used questions that had achieved a discrimination score greater than 0.667 in the researcher's prior research of cryptography learning. The discrimination criterion placed on the previously used questions produced only 24 of the 50 questions used on the pre and posttests. The 26 remaining questions needed for the tests were gathered from other, open sources and were vetted by a cryptography professor at the university, but no data about the difficulty or discrimination of these items was available. As a result of sub-optimal item validation, the pretest and posttest testing instruments were limited in their ability to measure the concepts being tested. Construct validity is discussed further in the following "Construct Validity" section.

Delimitations

The number of cryptography topics instructed was delimited to five and the total instructional time was delimited to approximately five hours in order to allow sufficient time for the development, implementation, and analysis of test instruments and instructional material. Because the study's author chose to instruct the selected topics outside of the subjects' required coursework, limiting the number of instructed topics to five was also the an attempt to maximize the quality of data collected given time constraints placed on subjects by their university coursework. Finally, selecting a small number of topics for investigation also allowed for an increased number of questions per topic, which facilitated a more granular analysis of topical knowledge. The choice to conduct this study outside of the university's regular course structure led to limitations on the amount of material covered in the study in order to maximize the quality of the collected data.

The potential impacts on results of delimiting instruction to such a small selection of topics and duration of instruction were potentially significant. Because subjects had no prior formal experience with the field of cryptography, topics were selected that first introduced key concepts in cryptography before those topics were discussed in greater depth. Providing introductory material further reduced the amount of time spent on the instruction of topics in greater depth. The learning results presented may have reflected only information about how the order of RU and RF instruction influences learning of introductory cryptography material among new cryptography learners. Results describing learning among these subjects of more in-depth cryptography knowledge may have been obscured by results produced by introductory material instructed in this study and, given time constraints on this study, these learning results were not reflective of the depth of instructional coverage given in a semester-long cryptography course.

Validity

Internal Validity

Limitations to the breadth and depth of the cryptography instruction provided as part of this study, the lack of a standard, valid body of knowledge and learner assessment instruments, and the lack of a control group most impactfully threatened the internal validity of learning results from this study. These threats to internal validity challenged both the study's construct and content validity. The following two sub-sections discuss how these three vulnerabilities impacted construct and content validity of cryptography learning in this study, and attempts to moderate their effects.

Construct validity

The primary threat to content in this study is the limited breadth and depth of the cryptography addressed. Five hours of instruction focused on five topics, as was delivered in this study, is not a representative sample of the full corpus of conceptual cryptography knowledge. The impact of the limitation imposed on this study by the lack of breadth is apparent when considering the prerequisite knowledge needed to learn Kerckhoff's Principle versus that needed to learn why and under what conditions certain problems are hard (and, therefore, suitable for use in cryptography. Students can gain accurate and precise understanding of Kerckhoff's Principle without mathematics or computing, gaining a similar understanding of the principles that make algorithms suitable for cryptography require some understanding of mathematics and computing. While efforts were made to bring topics requiring diverse sets prerequisite knowledge into the study, efforts were not taken to ensure that the selected topics were representative of the whole cryptography body of knowledge. Similarly, cryptography concepts explored at different levels of depth may also be best suited to instruction presented in different representational forms. If, for example, evidence supports that aspects of cryptography learning are dependent on an in-depth understanding of Chinese Remainder Theorem, the ability to perform the associated mathematical calculations will likely be required. A complete understanding of how order of instructional support for RU and RF affects cryptography learning and of the model of how this population learns cryptography requires a broader and more in-depth investigation of the body of cryptography knowledge.

Because cryptography does not have a standard, validated body of knowledge the ability to test the impact of order of instructional support for RU and RF across the discipline is limited. As described in Bloom (1956), a standardized body of knowledge is required in order to develop a comprehensive set of instruments for use in student assessment and standard learner assessments are vital to the evaluation of ability within a field. The lack of standard knowledge in cryptography not only constrains researchers' ability to test learning over the full scope of cryptography knowledge, it eliminates the possibility of using standardized, validated assessment tools of learners to gather data about the performance of constructs being tested. In this way, the lack of knowledge and assessment standards in cryptography is an impediment to construct validity, as well as content validity.

The ability to create an accurate model of the variables impacting cryptography learning among pre-cryptography was also constrained by this study's lack of a control group in which language and mathematical formulae were used to instruct cryptography concepts. A control group of this specific type would have allowed this study to explore other important aspects of cryptography learning, which could have produced a more robust model of cryptography learning in the studied population. Cryptography instruction in which language (written and spoken) and mathematical formulae are the primary representational forms used is common. Adding a control group using these instructional methods would have enabled a comparison among the UF, FU, and the common (control) groups that would have provided evidence of differences (or lack thereof) in learning gain between the treatment groups and the control group. Results of comparisons in learning gain among the three groups may have added evidence in support of the multiple additive moderator model, which was most explanatory and significant in this study, or guided a re-framing of the model resulting from this study's post-hoc analysis that may have resulted in a different, more explanatory and more significant model. Though this study's investigation of a statistical model of cryptography learning was post-hoc, the learning model construct would have been more effectively investigated if a control group as described had been present.

Content validity

Content validity of the pretest, instruction and posttest were threatened by the absence of standard evaluative instruments of cryptography knowledge that have been validated and are widely accepted in the field, similar to the Force & Motion Conceptual Evaluation used to measure learners' understanding of a class of physics concepts (Hill, 2015, p. 122). In lieu of a generally accepted instrument to measure knowledge of cryptography concepts, materials used for instruction and evaluation in this study incorporated material used for similar research on cryptography research. Posttest questions used in (Beckman, Bari, Chen, Dark, & Yang, 2017) were evaluated for discrimination between high and low scorers as part of the data analysis for that study. Discrimination was calculated by finding the top and bottom three scoring subjects (n=12) on the posttest given following instruction in that research, then dividing the number of the top three scorers who answered a question correctly by the number of the bottom three scorers who answered the question correctly. Questions from that study which were evaluated to have a discrimination value of ≥ 0.667 were considered for inclusion in the testing instruments used in this study. Question difficulty was not considered when excluding questions because of the assumed higher level of math background of these subjects versus those who participated in the previous study. Once questions from the previous study that meet the criterion were added to the testing instruments, the remainder of questions needed to achieve the desired 50 question threshold for the instruments were built from questions previously used in computer science programs to evaluate cryptography knowledge. If, in the view of the researcher, no questions were found that appropriately test concepts selected by the researcher for instruction, the researcher wrote questions to test the selected concepts. Posttest questions were modified from the pre-test to be equivalent forms of the pretest questions and the questions were re-ordered randomly. Once materials were built for this study, they were reviewed for accuracy of content and fidelity to the concepts taught by a tenured professor in the computer science department who possesses more than 30 years of experience in the practice and instruction of cryptography.

External Validity

The investigation of cryptography learning undertaken in this study was different from previous investigations of cryptography, which challenge the ability to generalize these results. This study was performed on undergraduate computer science majors in a large university in the Midwestern United States. Subjects participating in this study were between 18 and 20 years old, had passed courses in integral and differential calculus, and had not yet taken courses in cryptography at the university. Beckman, Dark, Kashyap, Wagstaff, & Yang (2017) studied a similar population, but compared the impact of instruction using Model Eliciting Activities (MEAs) on cryptography learning against a control group instructed using only symbolic representational forms (language and mathematical formulae). Methods used to evaluate subjects' performance were not comparable between Beckman, Dark, Kashyap, Wagstaff, & Yang, 2017 and this study. While it is likely that results from this study can be generalized to cryptography learners with the same academic background, such as subjects in Beckman, Dark, Kashyap, Wagstaff, & Yang (2017), no study has been performed that confirms the ability to generalize, and further generalizations are more tenuous.

Generalizations about the impacts of instructional methods on cryptography learning among students with more diverse math backgrounds would extend the contribution of this work, but are not yet supported by evidence. Though Beckman, Bari, Chen, Dark, & Yang (2017) assessed learners using a pretest-posttest format similar to the assessment performed of learners in this study and focused on subjects assumed to have a less rigorous mathematics background, that study did not gather demographic data on its subject and focused on different topics of instruction. Because it lacked a control group and because the instructional treatment was different than the treatment used in this study, Beckman, Bari, Chen, Dark, & Yang (2017) does not provide additional evidence related to learning hypotheses investigated in this study. Because demographic data was not collected, Beckman, Bari, Chen, Dark, & Yang (2017) cannot be used to further analyze the influence of prior mathematical knowledge on cryptography learning. In order to support generalization about cryptography learning beyond those with similar academic backgrounds, additional studies would be required.

THE STUDY OF COGNITIVE PROCESSING OF CRYPTOGRAPHY CONCEPTS USING FMRI

Literature Review

Cognitive Neuroscience in Support of Educational Goals

Jean Piaget theorized that learning, though a distinct process from development of the brain nonetheless changed specific brain structures as mental models were formed and modified (Piaget, 1964, p. 186). Yet, as Piaget and his contemporaries theorized, they were unable to gather empirical data about the physical impacts of learning on the brain. The tools that made observation of active cognitive process possible did not exist. In the past two decades, new tools and techniques have been developed that allow researchers to view the living human brain safely and to observe and capture changes to the brain as it works (Blakemore, Dahl, Frith, & Pine, 2011, p. 4). Researchers have begun to use tools such as electroencephalography, magnetic resonance imaging (MRI), and event-related potentials (ERP) to make observations of the brain in real time that were impossible prior to the advent of these technologies (Blakemore, Dahl, Frith, & Pine, 2011, p. 4). Real-time, non-invasive observation of the operation of the human brain has opened a new avenue of research that attempts to link biological processes in the brain to cognitive development (Blakemore, Dahl, Frith, & Pine, 2011, p. 3), which has evolved into the discipline of “cognitive developmental neuroscience” (Blakemore, Dahl, Frith, & Pine, 2011, p. 3). Practitioners of cognitive developmental neuroscience have sought to use the new observational tools of the discipline to better understand basic cognitive skills, such as the execution of executive functioning, and academic learning questions such as time dependencies of learning and instructional methods (Blakemore, Dahl, Frith, & Pine, 2011).

One of the basic questions of cognitive processing that remains under investigation is where in the brain cognitive processing occurs for various human functions. Modularist (or Fodorian) theories of cognitive processing posit that specific human functions activate specific areas in the brain to process information related to those activities (Barrett & Kurzban, 2006). Other researchers, such as Panksepp and Panksepp (2000), have argued that the human brain develops specialized areas of activation as a result of various experiences – a far more flexible interpretation of brain development than the modularist approach (Panksepp & Panksepp, 2000). Modularists have pointed to research on such topics as visual processing, especially visual processing of images of faces, as evidence of the modular nature of the brain (Barrett & Kurzban, 2006, p. 632). Proponents of a more flexible model of cognitive processing in the human brain have noted that studies in which the results supported a high degree of modularism also used very tightly controlled conditions or highly specialized functions (such as language) (Barrett & Kurzban, 2006, p. 631; Panksepp & Panksepp, 2000, p. 111). Despite considerable use of fMRI in brain research in recent years, the extent to which modularist (and more flexible) models of cognitive processing describe observed brain activity has remained hotly debated. As described in forthcoming sections of this document, studies of cognitive processing of mathematics have located areas of common activation among subjects, but the corpus of research involving cryptography has not developed sufficiently to make similar comparisons that might find common areas of activation in cryptography processing.

While cognitive developmental neuroscientists' investigations of learning questions has progressed, scientists have questioned some of the assumptions used and conclusions made, as well as the power of brain imaging tools used during attempts to bridge neuroscience and human learning. John Bruer (1997) took particular issue with early cognitive developmental neuroscientific investigations of childhood learning, buttressed using Bruner's theories, which concluded that children should receive early education because humans have a peak number of neurons in early childhood (Bruer, 1997, p. 5). Bruer pointed out that the knowledge about synaptogenesis used to support claims about the importance of early childhood education, which drove early childhood educational policy in the United States during the mid-1990's, were based on neuronal counts in monkeys and cats (Bruer, 1997, p. 5). The non-human research bases of synaptogenesis and neuronal pruning led to Bruer's recommendation to filter neuroscientific discoveries through cognitive psychology, rather than making direct claims about human learning based on neuroscientific research (Bruer, 1997, p. 11). Bruer (1997) also cautioned that synaptic changes in occur milliseconds and in ten-thousandths of a millimeter, where tools such as fMRI process in seconds and millimeters (p. 11). Though skeptical of attempts to connect neuroscience and human learning and education directly, Bruer presented a path through cognitive psychology by which weaknesses in assumptions and measurement were moderated and contributions to human learning and education were able to be made.

fMRI in Cognitive Neuroscientific Investigations of Learning and Education

Magnetic Resonance Imaging (MRI) has become a popular tool in cognitive processing research because it has been able to observe brain activity (Raichle & & Mintun, 2006, p. 451; Kwong, et al., 1992): non-invasively, over time, and safely in a wide age range of subjects including children. MRI has been considered safer than x-ray or CAT scanning technology because MRI does not expose its subject to potentially dangerous radiation. Unlike x-ray or CAT scanning machines, MRI machines create images of areas in the body by inducing a magnetic field that excites hydrogen atoms in bone and tissue exposed to the magnetic field (Kwong, et al., 1992, p. 5675). MRI derives its ability to track blood flow from iron in hemoglobin, which carries oxygen to the brain. Hemoglobin, when oxidized, is repelled by MRI's magnetic field. When de-oxidized, blood hemoglobin is weakly attracted to the MRI's magnetic field, which impairs the MRI's emitted signal. Signals from the MRI machine are analyzed by computer software and, when high concentrations of oxygenated blood are found in an area of the brain, software identifies that area as active (Raichle & & Mintun, 2006, p. 453). Because MRI is able to track blood flow in the brain over time, non-invasively, and safely in a wide age range of subjects, it found wide use in research, including educational research (Raichle & & Mintun, 2006, p. 451; Kwong, et al., 1992).

Functional Magnetic Resonance Imaging (fMRI) is a combination of tool and techniques that has facilitated observations of the human brain while subjects performed activities. FMRI uses a magnetic field to map brain activation in a subject over time by measuring changes in blood flow to the brain's regions and structures (Logothetis, Pauls, Augath, Trinath, & Oeltermann, 2001), but measures these changes while subjects are performing activities. The ability to monitor brain activity safely and non-invasively while subjects perform tasks has facilitated threads of research that investigated learning and brain development theorized to be impactful to learning. FMRI research has been used to investigate the impacts of sets of knowledge on the ability to perform sets of skills (Cantlon, Brannon, Carter, & Pelphrey, 2006; Clements-Stephens, et al., 2012), to investigate developmental differences on learning (Barde, Yeatman, Lee, Glover, & Feldman, 2012), and to investigate the comparative efficacy of instructional interventions (Szűcs & Goswami, 2007; Thomas, Wilson, Corballis, Lim, & Yoon, 2010; Beckman, et al., 2017; Beckman, Bari, Chen, Dark, & Yang, 2017). Despite the limitations of measuring cognitive processing using fMRI including: the cost of equipment, laboratory-style setting, and the potential for a lack of commonality in brain areas activated during complex tasks, fMRI has been used to better understand how basic mathematical functions are processed in the brain, to explore if differences exist between cognitive processing of basic mathematical functions in experts and novices, and to investigate how translating basic mathematical concepts among different representational forms impacts cognitive processing.

fMRI and the Measure of Cognitive Processing in Math Learning

(Szucs and Goswami (2007) argue that measurements of cognitive processing are useful in conjunction with behavioral measures to understand how mental models form and develop in order to better inform researchers on the effectiveness of instructional interventions (Szucs & Goswami, p. 114). Cantlon, Brannon, Carter, and Pelphrey (2006), for example, used fMRI to measure how the concept of magnitude was processed in the brains of 4-year-old children and adults. The study focuses on whether children who have not mastered symbolic numerical concepts of magnitude process non-numerical representations of magnitude similarly to adults, who are familiar with symbolic numbering (Cantlon, Brannon, Carter, & Pelphrey, 2006, p. 845). Because both young children and adults are more accurate in comparing small ratios than large ones and that condition remains true regardless of development, the authors selected comparison of ratios as the stimulus condition. Eight children and 12 adults were first presented with a crosshair and instructed to press a joystick button when the crosshair turned red. This activity served as a baseline for cognitive processing during a mechanical task for each individual. Each subject was then presented with a series of 238 images at 1.2 second intervals, which remained on screen for .3 seconds. Images in the series, on occasion, differed from the other images in the series in the shape of the stimulus items on the images, or number of the items presented on an image. The images were counterbalanced for quantity. When images contained a number of elements that differed from the standard, the ratio of that difference was always 2:1.

Qin, Silk, Stenger, Fissell, Good, and Anderson (2004) measured the change of the brain activation patterns as children learn algebra equation solving. In this study, the authors sought understanding of the cognitive patterns of activation as simple equations are solved, again comparing children to adults. The study examined ten pre-algebra student volunteers in sixth through eighth grade and compared fMRI data against fMRI analysis from a study of college students performing the same algebra tasks by asking children to solve equations that involved 0, 1, or two mathematical steps without borrowing operations (Qin, et al., 2004). Children were given an fMRI scan on the first and fifth (final) days of the experiment. In the intervening days, the subjects practiced performing the experimental task outside of the fMRI machine (p. 5686). Based on results from the two scans, the researchers used a preliminary analysis to determine what areas of the brain should become the focus of their analysis, and built a predictive statistical model for the conditions based on that model. FMRI functional runs consisted of eight blocks, which began with a crosshair prompt displayed for 1.2 seconds, an equation for subjects to solve and answer within 12 seconds, followed by an 8.4 second display of a final prompt (p. 5686). The experiment found that both children and adults activated similar brain regions when solving these simple algebraic equations (p. 5687).

Thomas, Wilson, Corballis, Lim, and Yoon (2010) compares cognitive processing of simple mathematical functions in undergraduate and graduate university students in order to determine: what parts of the brain perform this processing, if the involved regions differ based on the representation used to present the question, whether translating these functions from graphs to algebra or from algebra to graphs used different areas of the brain for processing, or whether the active brain areas strictly represented the processing of functions (p. 610). The researchers placed subjects in the fMRI machine, performed an anatomical scan in order to later map brain activity to brain region, then performed four functional scan runs of ten scan blocks, each consisting 6 trials (p. 611). Trials consisted of pairs of images. Images represented linear or simple quadratic functions and were paired as two graphs, two equations, or a graph and an equation and their presentation was counterbalanced (p. 611). Subjects were tasked with deciding in 3.5 seconds whether or not both images represented the same function (p. 610). The experiment resulted in significant findings. First, that there were no significant differences in the cognitive processing of functions between the undergraduate and graduate students or based on representation. Further, and most important in this context, translation between representations (graph-algebra and algebra-graph) used the same brain areas during processing, but to a significantly greater extent than when subjects did not have to translate between representations (p. 614). Unfortunately, no descriptive statistics were given of this aspect of the result, but Figure 4 illustrates the result (Thomas, Wilson, Corballis, Lim, & Yoon, 2010, p. 611).

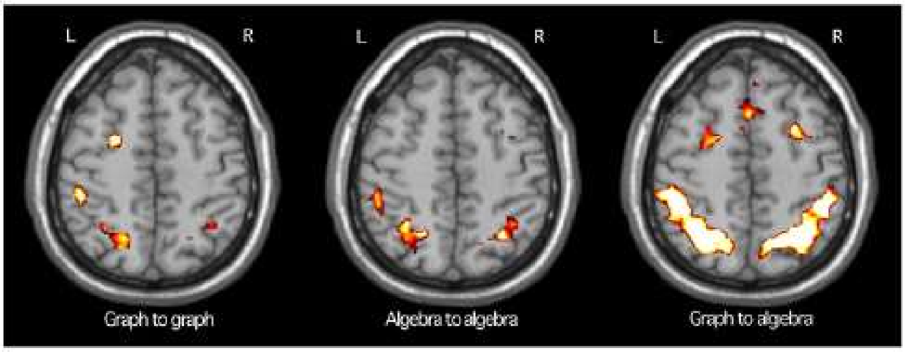


Figure 4: Brain Activation when Processing Functions

When considering the use of fMRI as a measure of metal models and representational fluency in cryptography, the experiments discussed in this section provide guidance for study design. FMRI studies use short trials and have simple, defined tasks. Thomas, Wilson, Corballis, Lim, and Yoon (2010) asked subjects to make a simple, but quick, comparison of two representations, while Cantlon, Brannon, Carter, and Pelphrey (2006) and Qin, Silk, Stenger, Fissell, Good, and Anderson (2004) asked subjects to solve simple equations. Comparisons made in fMRI experiments in mathematics often seek common areas of activation among groups of different ages or experiences in order to establish baseline activations for future research in support of learning higher-level concepts (Szűcs & Goswami, 2007, p. 123; Thomas, Wilson, Corballis, Lim, & Yoon, 2010, p. 617; Qin, et al., 2004, p. 5691). As a discipline highly dependent on conceptual understanding of mathematics, the field of cryptography can both consume data from fMRI studies of mathematics in order to better understand how learning of critical mathematics concepts takes place, and use fMRI as a tool to study questions such as: how experts and novices process aspects of cryptography problems, how different instructional methods impact processing of cryptography concepts, or examine potential cognitive processing linkages between concepts.

Initial work using fMRI to analyze how learners process cryptography concepts in the brain is detailed in Beckman, Bari, Chen, Dark, and Yang (2017). This descriptive study found significant activation in the right inferior frontal and left medial frontal lobes and the left interior frontal lobe of the brain when subjects attempted to solve cryptography problems presented using mathematical formulae. The right inferior frontal and left medial frontal lobes are associated with executive processing, or reasoning. The left interior frontal lobe of the brain is associated with representing numbers (Beckman, Bari, Chen, Dark, & Yang, 2017, p. 6). While the activation in executive processing areas of the brain during problem solving activities when the problems were represented in math provide evidence for a difference between cryptography processing and the cognitive processing of simple mathematics, no executive area brain activation was noted during problem solving activities where the problems were represented in pictorial or English language text forms (p. 6). The results of fMRI scans during cryptography problem solving in mathematical versus pictorial or language presentations provide evidence in support of the hypothesis that cognitive processing of cryptography depends solely on the representation in which the problem is presented (p. 8). This study did not investigate how instruction in representational fluency and instruction in representational understanding together influence cryptography learning.

Methodology

Research Question

The cognitive processing aspect of this research, based on existing literature, investigated as research question 1 (RQ1) where in the brain cryptography concepts were processed and whether learners processed cryptography concepts differently in the brain if those learners received cryptography instruction focused on representational fluency first, rather than representational understanding compared against activation patterns when instruction focused on representational understanding before representational fluency (RQ2).

Variable Operationalization

The cognitive processing component of this research used two different analyses of the “Areas of Cognitive Processing”   to investigate where in the brain cryptography concepts are processed, as RQ1, and whether the different instructional method treatments delivered as part of this study, “Instructional Method”, produced different activation in learners’ brains when learners are asked to solve cryptography problems under fMRI (RQ2). “Areas of Cognitive Processing” was defined as the regions and structures in subjects’ brains that received statistically significant (α=0.05) additional blood flow compared to a resting state control image during processing of cryptography concepts under fMRI. So, for each question asked of each subject, snapshots of blood flow patterns in the subject’s brain were collected twice each second during a 9-second response period after the question was presented. The snapshots of data collected during the response period were averaged together and compared against the average of blood flow patterns taken during a 15-second resting state, which preceded questions about each cryptography topic. Measurements of areas of cognitive used to support investigation of RQ1 averaged activation patterns of all twenty of the study’s participants by each of the three representational forms in which cryptography questions were presented during scanning. Investigation of RQ2 compared averages of brain activation patterns for the ten subjects in each instructional condition.

Population and Subject Selection

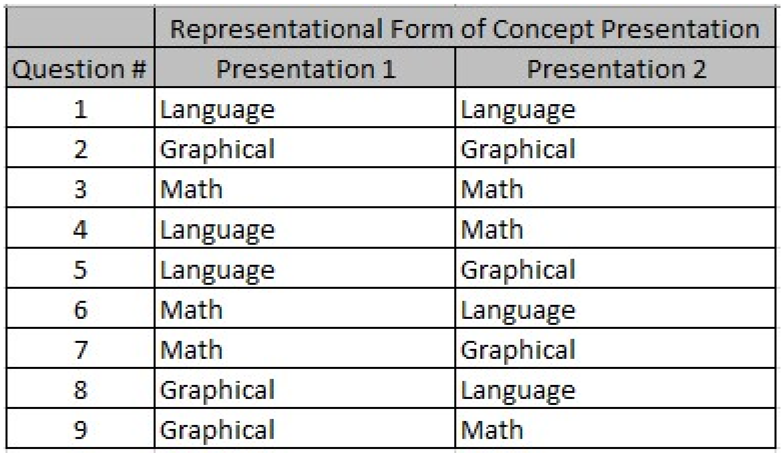
The investigation of cognitive processing of cryptography discussed in this section studied the same population and used the subject selection process, previously described in the “Population and Subject Selection” in section two.

Study Design and Procedure

This study’s investigation of cognitive processing of cryptography concepts used fMRI scans of subjects’ brains, subsequent to all classroom instruction in cryptography, to measure their brain activity as they responded to cryptography questions. Subjects were asked to complete a second attestation of their fitness for an fMRI scan and were given a safety briefing before completing one, one-hour fMRI scanning session.

The fMRI scanning protocol used in this study was based upon the protocol used in Thomas, Wilson, Corballis, Lim, and Yoon (2010), which investigated similar research questions in mathematics, and in Beckman, Bari, Chen, Dark, and Yang (2017), which investigated similar research questions in a different population of cryptography learners. Cryptography questions were presented to subjects under fMRI in functional runs by topic. Each of the five topics instructed during the three classroom sessions became an individual functional run of questions presented during the fMRI scan. Each functional run presented questions using the same number of presentations in graphical, language, and mathematical representational forms presented in the same order by representational form. Functional runs contained nine questions. The presentation of each question first asked subjects to focus on a black crosshair (+) pattern on a white background for 15 seconds. Brain activity during this period became the resting state brain activity for the subject when analyzing brain activity changes during cognitive processing of this question. Following the crosshair pattern, subjects were shown: a representation of a cryptography concept from the topic of the functional run for 9 seconds, a blank white slide for two seconds, and a second representation of a cryptography concept for 9 seconds. Finally, subjects were shown a second blank white slide for 9 seconds during which they had been instructed to respond to the question, “Do the two conceptual representations presented represent the same cryptography concept?” Table 22 below shows the order in which each of the three representational forms used in this study were presented in questions within the functional runs.

Table 13: Order of presentation of representational forms in questioning during fMRI functional Runs



	Representational Form of Concept Presentation	
Question #	Presentation 1	Presentation 2
1	Language	Language
2	Graphical	Graphical
3	Math	Math
4	Language	Math
5	Language	Graphical
6	Math	Language
7	Math	Graphical
8	Graphical	Language
9	Graphical	Math

Results

Blood oxygen data gathered from subjects' brains during fMRI show which of the brain's Broadmann areas were active while subjects answered cryptography questions. Initial analysis of fMRI data focused on RQ1. Resting state and active state activation of individual voxels, one millimeter square areas of the brain, from all twenty subjects were gathered for each of the three representations in which questions were presented: mathematical, language, and graphical, then compared using t-tests of the two sets of activations. Areas of activation shown in the upcoming figures and noted in the associated tables are defined as significant because the change in blood oxygen level between subjects' resting state brain activity, determined by having subjects stare at a crosshair pattern for one minute, and subjects' brain activation when responding to questions produced a p-value <0.05. Additionally, clusters of voxels that generated statistically significant values at $\alpha=0.05$ had to be within a group of at least 100 adjacent, significant voxels, which is denoted in upcoming tables as "Cluster Size". Figure 10 presents a pictorial representation the brain areas active when cryptography questions were presented using a mathematical representational form, while Table 14 lists the areas shown as active in Figure 1 and briefly describe the functions of those areas. Figure 11 and Table 15 display results for activation noted when questions were presented using language representation. Figure 12 and Table 16 display results for questions displayed in graphical format.

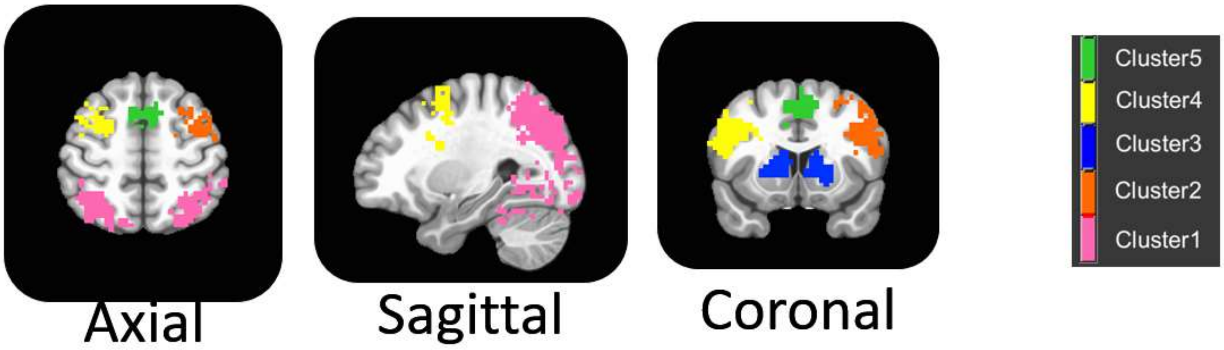


Figure 10: fMRI Brain Image Activation: Math Presentation vs. Baseline (n=20)

Table 14: Broadmann Areas of Brain Activation: Math Presentation vs. Baseline (n=20)

	Gyrus	Broadmann Area	Function
Cluster 1	Precuneus	4	Primary Motor and Visual Processing
Cluster 2	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 3	Cuneus	17	Visual Processing
Cluster 4	Right Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 5	Medial Frontal Gyrus	46	Executive/Abstract Processing

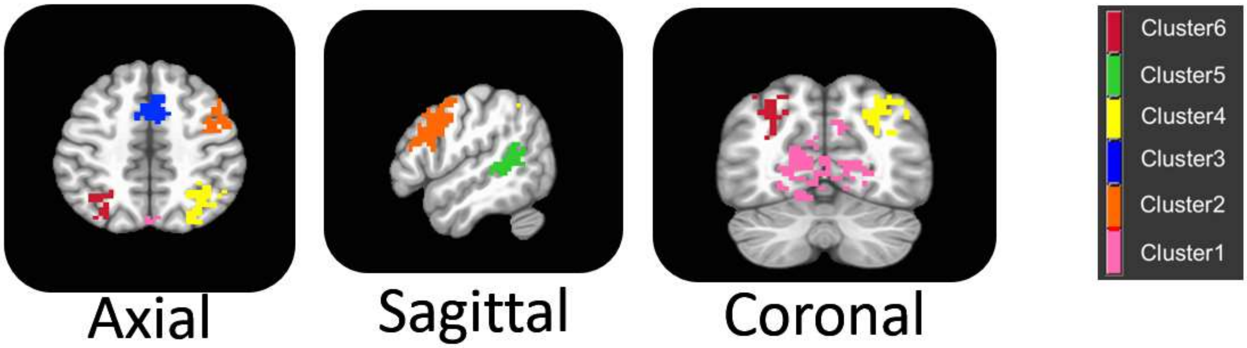
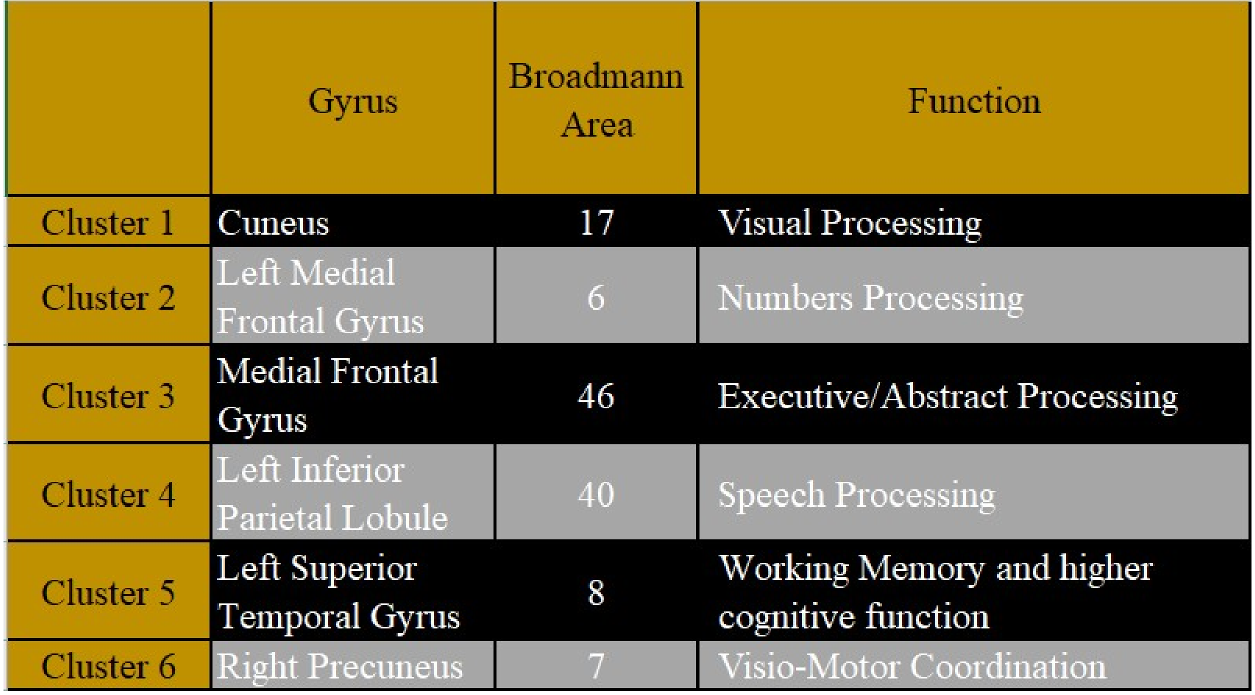


Figure 11: fMRI Brain Image Activation: Language Presentation vs. Baseline (n=20)

Table 15: Broadmann Areas of Brain Activation: Language Presentation vs. Baseline (n=20)



	Gyrus	Broadmann Area	Function
Cluster 1	Cuneus	17	Visual Processing
Cluster 2	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 3	Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 4	Left Inferior Parietal Lobule	40	Speech Processing
Cluster 5	Left Superior Temporal Gyrus	8	Working Memory and higher cognitive function
Cluster 6	Right Precuneus	7	Visio-Motor Coordination

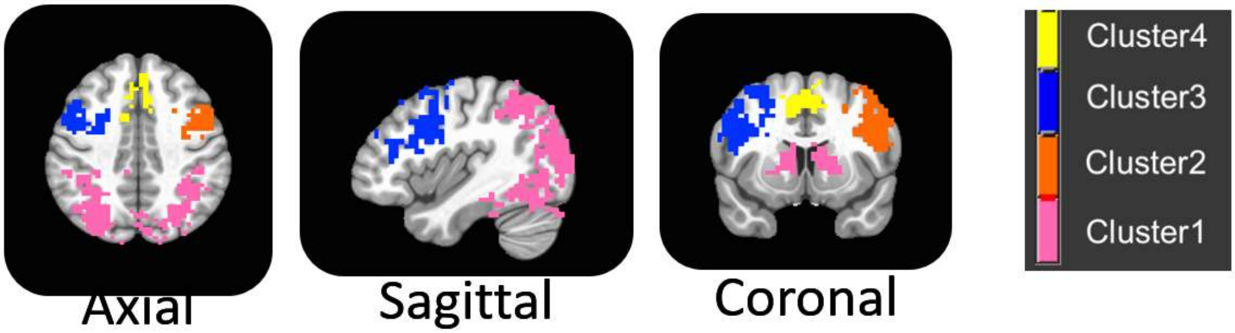
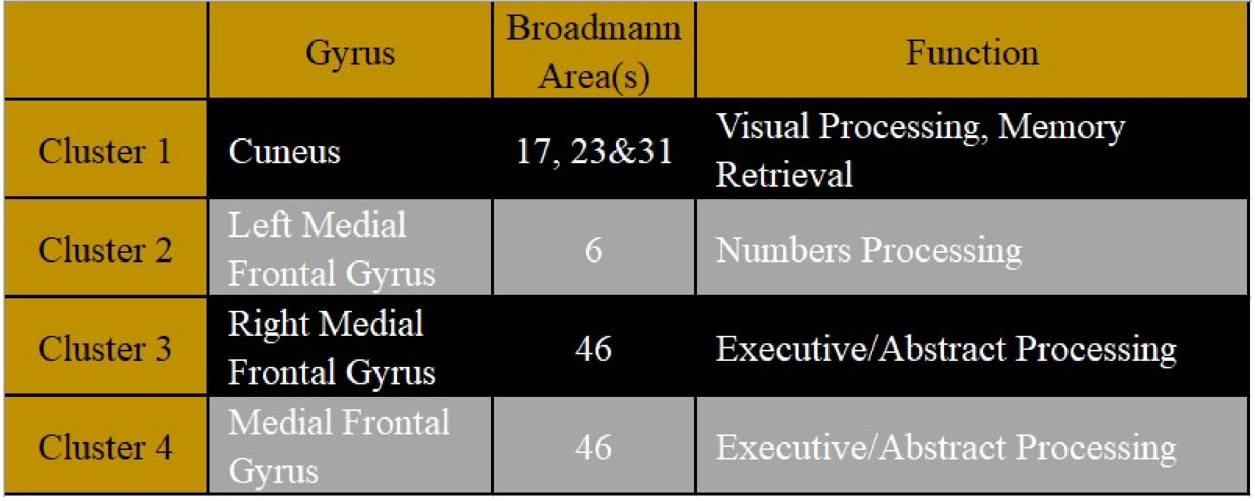


Figure 12: fMRI Brain Image Activation: Graphical Presentation vs. Baseline (n=20)

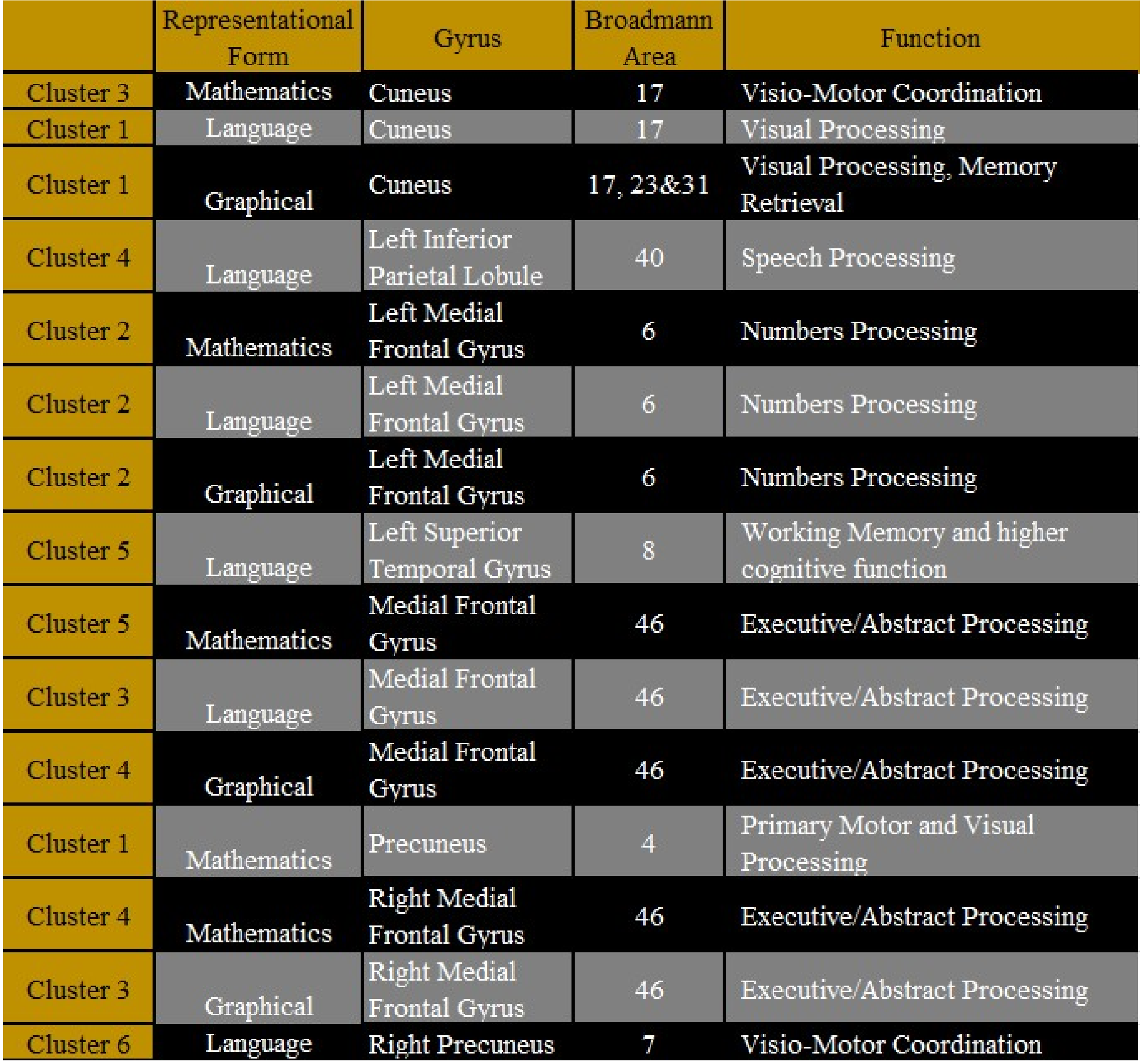
Table 16: Broadmann Areas of Brain Activation: Graphical Presentation vs. Baseline (n=20)



	Gyrus	Broadmann Area(s)	Function
Cluster 1	Cuneus	17, 23&31	Visual Processing, Memory Retrieval
Cluster 2	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 3	Right Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 4	Medial Frontal Gyrus	46	Executive/Abstract Processing

In order to format data for potential inference, clusters of brain activation were compared among the three representational forms by building a table of common areas of activation and creating the brain images associated with these comparisons. Table 16 highlights clusters of common activation by displaying activation by representational form, sorting, and labeling active clusters.

Table 17: Broadmann Areas of brain activation sorted by Gyrus



	Representational Form	Gyrus	Broadmann Area	Function
Cluster 3	Mathematics	Cuneus	17	Visio-Motor Coordination
Cluster 1	Language	Cuneus	17	Visual Processing
Cluster 1	Graphical	Cuneus	17, 23&31	Visual Processing, Memory Retrieval
Cluster 4	Language	Left Inferior Parietal Lobule	40	Speech Processing
Cluster 2	Mathematics	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 2	Language	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 2	Graphical	Left Medial Frontal Gyrus	6	Numbers Processing
Cluster 5	Language	Left Superior Temporal Gyrus	8	Working Memory and higher cognitive function
Cluster 5	Mathematics	Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 3	Language	Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 4	Graphical	Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 1	Mathematics	Precuneus	4	Primary Motor and Visual Processing
Cluster 4	Mathematics	Right Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 3	Graphical	Right Medial Frontal Gyrus	46	Executive/Abstract Processing
Cluster 6	Language	Right Precuneus	7	Visio-Motor Coordination

The combination and grouping of active clusters in the Table 17 show that Broadmann Areas 17 (visual processing), 6 (numbers processing), and 46 (executive processing) were active as students processed cryptography questions in all three representational forms in which questions were presented during fMRI scans. Within Broadmann Area 46, the right medial frontal gyrus was also active during processing of questions presented mathematically and graphically, but not in language. Based on the analysis in support of RQ1 of brain activation patterns found during scanning, this study provides evidence of the use of Broadmann Areas 6 (numbers processing)

and 46 (executive processing) when processing cryptography concepts. Broadmann Area 17 is also recruited when cryptography questions are presented to subjects visually.
A secondary analysis compared brain activation data from the fMRI scans by instructional method in support of RQ2. In that analysis, brain activation data from the ten subjects who received cryptography instruction in the UF treatment group were compared to brain activation data from the ten subjects who received instruction in the FU treatment group. T-tests of activation levels by voxel between the two groups showed no statistically significantly differences at α=0.05 in brain activation using the same process described in the opening paragraph of this section.

Assumptions

The key assumption made during the cognitive processing component of the research was that subjects were thinking in ways during the scan that were consistent with the instructions presented. When subjects were instructed to rest and focus on the crosshair pattern, the analysis relied on subjects' having done so. Similarly, the analysis relies on subjects' having thought about the cryptography concepts presented to them. Throughout each subject's scan, discomfort resulting from the noise generated by the fMRI scan or from remaining still inside the machine during the scan challenged this assumption. Additionally, the assumption of focus on the task at hand was quite fragile for any particular question and for any particular subject because, to confound the result of a particular question, a subject needed only lose focus or become confused while asked to rest or asked to respond to the question. Because the sample size of this study was relatively small, the weight of data gathered from each question was relatively large.
Aspects of this component of the study were implemented to minimize the impacts when subjects' foci strayed. By using the same functional run design for each of the five cryptography topics, each subject received fifteen questions presented using each of the three representational forms investigated in this research. Activations by representational form were averaged across subjects to produce the grand average activation patterns presented as results. Subjects were also required to answer all questions during the scan, which made sure that the weight of responses were no greater than designed. The use of multiple questions per representation and delimiting the number of representational forms used in the study reduced the individual importance of data from any one activation pattern.

Limitations

Cost, both financial and in subjects' time, of administering fMRI scans was the primary limiting factors of this component of the research. Financial costs included the purchase of time to use the MRI machine and compensation for subjects. Accordingly, the number of subjects scanned during this study was limited to 20. Subjects' time spent under fMRI in this study was limited to approximately one hour. The number of questions presented during scanning and the presentation duration of each slide were designed to fit into a one-hour period in order to accommodate limits on subjects' willingness to endure the fMRI scan. Limits to the number of cryptography topics covered and the number of representational forms investigated were driven, in whole or in part, by the limitation on the amount of time subjects were expected to endure fMRI scanning.

Beyond its costs, the MRI machine itself and the resultant analysis limited the cognitive processing investigation in this research. There were limitations on both spatial and temporal resolution as noted in Bruer (1997). The rigidity in the delivery of fMRI scans and in the processing of scan data were also limiting factors in the analysis. Because subjects had to remain nearly still during the scan, questioning of their understanding of cryptography concepts was limited to those questions which could be answered using a handheld button box, which meant that the questions had to have distinct, multiple-choice responses. So, the nuances of subjects' responses that might have indicated a particular misconception that resulted may not have been captured. Following data collection, data from individual scans were transformed to match a standard template. This process accounted for the difference in head size among subjects. So, spatial resolution limitations noted by Bruer (1997) were potentially made more problematic by data transformations that manipulated the locations of brain areas used to create composite areas of brain activation shown in the figures above. While the scan and analysis procedures used in this research were standard for research using fMRI brain scans, limitations based on the requirements of the MRI machine may have impacted the accuracy and precision of the scans used in this research.

Delimitations

The number of representational forms in which cryptography instruction was delivered and in which test questions were asked was delimited to: graphical, language, and mathematical. Classroom instruction and test questions were presented only in these three representational forms in order to allow comparison between the fMRI results from this study with the fMRI results from previous work. As noted above, the length of pre and posttests was delimited to a total of 50 questions each in order to balance the number of data points from those tests with the limitation of subjects' attention spans.

Validity

Internal Validity

fMRI scan data was subjected to threats to internal validity both during the generation of fMRI data, and during data analysis. Internal validity of the fMRI scan data creation process relied on the scanning protocol in Thomas, Wilson, Corballis, Lim, and Yoon (2010), from which the scanning protocol used in this research was derived, to provide reliable measurement of time-dependent brain activity during cognitive processing of this subject matter, as well as the ability of the cryptography questions processed by subjects under fMRI to elicit appropriate cognitive processing activity. The scan protocol used in Thomas, Wilson, Corballis, Lim, and Yoon (2010) produced brain activation consistent with numeric processing found in several studies of algebraic and integral calculus problem solving (Wilson, Corballis, Lim, & Yoon, 2010, p. 615), which provided evidence in support of the internal validity of the scan protocol. The questions asked of subjects while under fMRI were new, so the internal validity of these questions used to create the fMRI responses in subjects was unclear. Though previously untested in research, the cryptography questions presented during fMRI were reviewed by the same process as the pre and posttest questions and the instructional modules. Though the scan protocol and questions presented to subjects under fMRI were both sources of threats to the internal validity of the fMRI data creation process, the novelty of the questions presented to subjects under fMRI was the largest threat to internal vulnerability of the fMRI scans because these questions are untested in fMRI research.

The primary source of threat to internal validity in the fMRI data analysis process originates from the normalization of each subject's brain to a common template size and shape. In order to analyze fMRI data for this study, which attempts to find common areas of brain activation across groups of subjects, individual points of activation on individual subject's brains must be averaged with points of activation found in other subjects. Because each subject's brain is a different size and shape, individual fMRI scan results need to be normalized in order to analyze these data from a group of subjects. The normalization process, described in more depth in Beckman, Bari, Chen, Dark, and Yang (2017), the process of normalization of individual fMRI scans involves the manipulation of individual results to fit a standard template brain. As a result of normalization, areas of activation found in individual scans may be stretched or compressed during transformation that may misrepresent the location of activation on the normalized template brain. Though these misrepresentations of brain activation caused by transformation onto the normalized template had less impact on the fMRI scan results when averaged with an increasing number of individual scan results, the error introduced by the normalization process emphasizes the importance of larger sample sizes when performing analysis of groups of fMRI scans.

External Validity

The cognitive processing component of this research identified areas of the brain that, when taken together, expected to generalize to fMRI scans of cryptography learners with similar backgrounds in mathematics. Areas of brain activation found in these results to have been active during cryptography processing corresponded to mathematics processing, others to interpretation of visual stimuli, and still others to executive processing. No individual area of the brain was found to be unique to cryptography processing and this study did not investigate the extent to which these combinations were distinctive to cryptography processing. The decision to use the same fMRI scan protocol in this research as was used in Beckman, Bari, Chen, Dark, and Yang (2017) was made in an attempt to investigate the extent to which the external validity of this study's results to cryptography learners beyond computer science students into adjacent, information security-related fields. Comparisons of activation patterns made between this study and Beckman, Bari, Chen, Dark, and Yang (2017), as summarized in tables 13-15 below, did not support generalization of results related to RQ1 to adjacent, information security-related disciplines.

Generalizations related to the impact of instructional method on active areas of cognitive processing of cryptography (RQ2) were made more difficult to support because of the absence of any noted impact. Several factors may have helped to cause a lack of difference in activation areas between the treatments studied. The instructional treatments used in this study may not have been sufficiently different to produce different activation patterns in the brain. The lack of significance of the t-test that compared learning gain results in the cryptography learning component of this research supports this possibility. However, as discussed in Section 3.1.2 Beckman, Bari, Chen, Dark, and Yang (2017) measured no significant difference in brain activation when topics instructed using MEA were compared against topics taught using only lecture with text and mathematical formulae. So, the possibility remains that instructional method does not change the locations in the brain where cryptography is processed across cryptography learners, but further research is required before the extent of external validity of this result can understood.

DISCUSSION

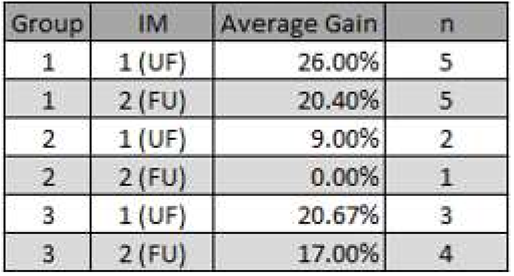
Discussion of Learning Results

Though a t-test comparing learning gain results did not provide evidence in support of the significance on learning of the order of instructional support for representational understanding or representational fluency, the small sample size of the study, the narrow scope of instruction provided, and the lack of a standard body of knowledge and learner assessment instruments may have negatively impacted these results. The low power ($\beta = .15$) derived from this sample size would have required a 25% difference in the average learning gain between the two treatment groups in order to generate significant results at $\propto = .05$. A 25% difference between the two treatment groups in average learning gain would have been an especially notable result to have been generated by the five hours of instruction on five cryptography topics taught in this study. If, for example, the FU treatment group averaged a 17% gain from pretest to posttest score as it did in this study, the UF group would have had to have gained 42% from pretest to posttest in order to generate a learning gain that would have been statistically significant in the designed t-test. Such a result would have been highly suspicious, especially in a study where the sample size was so small and the instruction so limited.

The lack of a standardized body of knowledge and standard assessment instrument also reduced the likelihood of finding a statistically significant result from the comparison of learning gain between the treatment groups in this study. Despite attempts to maximize the content validity of the testing instruments through statistical analysis of previously used questions and expert review, only 17 of the 50 questions in the posttest were described as having a difficulty score .5 ≥ x ≤ .7 and a discrimination score greater than .1 in post-hoc item analysis. While interpretation of what item discrimination and difficulty statistics indicate “good” questions is subjective, this analysis of the posttest items raises concerns that the ability to measure learning gain using pretest and posttest scores is limited. Because, in addition to the small number of participants and small amount of instruction performed in this study, only 17 posttest questions were found to be strong evaluators of the concepts instructed, the validity of conclusions based on the t-test comparing the study’s treatment groups was further weakened.

Statistics descriptive of learning gain also suggest that the results of the as-designed t-test may not accurately reflect the relationship between instructional methods tested in this study and learning gain. As shown in Tables 2 and 3 (page 31), the average learning gain in the UF group was 4% greater than the UF group. Also, the standard deviation in scores in the UF decreased by 1.01% from pretest to posttest whereas standard deviation increased 5.00% from pretest to posttest in the FU group. Higher average learning gain in the UF group may suggest that learners in that treatment group benefitted in their cryptography learning from in-depth treatments of individual representations and representational forms, specifically as they related to cryptography. The downward trend in standard deviation from pretest to posttest in the UF group suggests that the increase in cryptography learning resulted from the instruction, rather than individual aptitude or some other cause. Additionally, subjects in the UF group always increased their knowledge of cryptography, on average, more than subjects in the FU group regardless of their previous level of mathematics knowledge. When average learning gain by treatment was further separated by subjects' levels of prior mathematics experience used as categories in the "Group" variable, the following results were produced.

Table 18: Average Learning Gain by Prior Mathematics Knowledge (Group) and Instructional Method (IM)



Group	IM	Average Gain	n
1	1 (UF)	26.00%	5
1	2 (FU)	20.40%	5
2	1 (UF)	9.00%	2
2	2 (FU)	0.00%	1
3	1 (UF)	20.67%	3
3	2 (FU)	17.00%	4

As noted previously, the Group variable is a categorical variable separated as follows. Subjects categorized as "1" have taken or tested out of both MA165 and MA166, those in category "2" have tested out of or taken MA165 or MA166, those categorized as "3" have taken or tested out of neither MA165 nor MA166. The increased average learning gain by instructional method and consistently superior average learning gain by the UF treatment group across all levels of mathematics knowledge tested in this study suggest that the order of instructional support for representational understanding and representational fluency as operationalized by the IM variable may contribute significantly to learning gain in cryptography in a larger sample of subjects.

While the previously discussed challenges to internal validity apply to these descriptive statistics as they do to the t-test between treatment groups, these descriptive statistics suggest that the results of the t-test may have shown significance in a larger number of subjects despite the limitations of this study. If order of instructional support were to be found to be significant in a larger sample as suggested by more detailed descriptive analysis of this study's learning data, then the data would support the instruction of cryptography concepts by describing a concept in-depth in one representational form, and repeating that process for the concept in other representational forms. Instruction in which learners must achieve representational understanding within a specific knowledge domain and in each of the representational forms among which learners seek to translate supports instructional design theories posited by Ainsworth's (2006) DeFT Framework concerning the maximization of learning using multiple representations. The DeFT framework, which proposes a conceptual framework under which learning using multiple representational forms can be maximized, theorizes that learners should understand the representational forms from which they are learning at a general level, but should also understand how that representation applies in the context of the specific knowledge domain being studied (Ainsworth, 2006, p. 186). Building understanding of a representational form in context can build understanding in learners of how each representational form emphasizes and de-emphasizes properties of phenomena specific to the domain of study, which further facilitates learners' ability to translate among representational forms. Learners that are able to translate among representational forms within cryptography have deep conceptual knowledge of cryptography. Because the instruction and evaluations in this study were not designed to distinguish between instructional support for generalized understanding of representational forms versus support for domain-specific understanding of representational forms, these results provide no evidence regarding Ainsworth's claims regarding the importance of a generalized understanding of representational forms. The results of this study shown in Table 18 do provide evidence in support of Ainsworth's theory that prior domain-specific understanding of representational forms used in instruction is required if learners are to maximize benefits of learning from instruction using multiple representational forms. In the practice of instructing cryptography, these results imply that instructors should focus on teaching both the knowledge being represented and about the representational form used to represent the knowledge when instructing using multiple representational forms.

Examination of the effects of prior mathematical knowledge on cryptography learning did produce a statistically significant result. As shown in Figure 9, this analysis noted a direct effect of prior knowledge of cryptography, as represented by pretest score, on cryptography learning gain, as represented by the “Combo” variable without outlying observations, as well as moderation effects on learning gain produced indirectly by prior knowledge of mathematics and instructional method, the “Group” and “IM” variables, respectively. This model was both significant at α=.05 (p=.0004) and explanatory ($r^2 = .82$), but this study’s lack of a control group may have been an impactful limitation of this analysis.

The lack of a control group in this study prevented these results from adding to the understanding of how the use of multiple representations in cryptography instruction impacts cryptography learning compared to other instructional methods and how cryptography instruction and learning relates to the larger body of work in STEM education. Cryptography concepts are often expressed as mathematical formulae paired primarily with either spoken or written text descriptions to enhance learners’ understanding of the formulae during instruction. In these cases, learners are experiencing cryptography instruction that uses two different representations, math formulae and text, which are both symbolic representational forms. If this study had used a control group, such as one in which instruction was presented in a single representational form, results could have provided additional information about how the use of multiple representations, representational understanding, and representational fluency in cryptography instruction influenced learning when compared to instruction using a single representational form. Comparisons enabled by the addition of a control group as described would have informed a more complete mapping of cryptography learning to theories of learning and expertise tested in physics, chemistry, and engineering and would have provided further evidence against which learning theories could have been evaluated.

In terms of the additive moderation model found to be the most significant and explanatory in this study’s analysis of the relationship between prior knowledge of mathematics and learning gain, addition of a control group to this study may have facilitated a re-framing of variables and significance of a different model of relationships among them. Theories of STEM instruction using multiple representational forms, such as (Ainsworth, 2006; Lesh, Post, & Behr, 1987;

Kozma, Russell, Jones, Marx, & Davis, 1996), suggest that the control group in which only math formulae and language (text and spoken) were used would have experienced less learning gain, on average, than the UF or FU treatment groups tested in this study. If those theories held true under study, the model representing the relationships in this study would require re-framing. In the hypothetical case, an "Instruction" variable could be constructed to represent UF, FU, and control instructional methods as subdivisions. Within this framework, it is possible that regression analysis would have revealed a relationship between variables, dominant in its significance and explanatory power, in which "Instruction" mediated the relationship between prior cryptography knowledge and learning gain and "Instructional Method" (as operationalized in this study) moderated the mediation of the relationship.

Discussion of Cognitive Processing Results

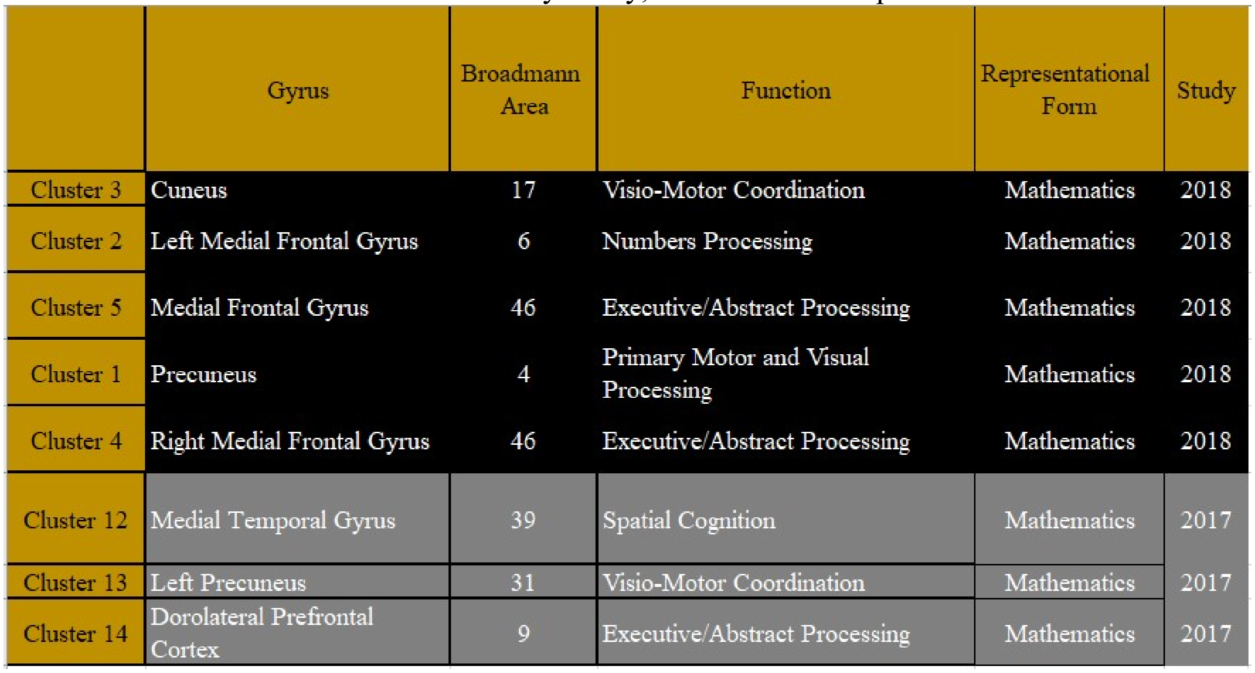
As noted in "Results" sub-section of the "fMRI Study of Cognitive Processing of Cryptography Concepts" section, analysis in support of RQ1 revealed common areas of brain activity among all 20 subjects during cognitive processing of cryptography problems. Activation of areas related to numbers processing, such as Broadmann Area 6, across subjects and representational forms is consistent with the prior research about cognitive processing of mathematics, the theoretical parent of cryptography, during fMRI scans (Thomas, Wilson, Corballis, Lim, & Yoon, 2010). Broadmann Area 17, used for visual processing, was consistently active throughout questioning during scans. Activation of Broadmann 17 is consistent with visual presentation of material during scanning. Broadmann Area 46, active during executive processing activities, was also active across representations during questioning under scan in this study. Activation during cognitive processing of cryptography of the left medial frontal gyrus, understood to be used for numbers processing, is consistent with previous research (Thomas, Wilson, Corballis, Lim, & Yoon, 2010; Chochon, Cohen, Moortele, & Dehaene, 2004; Kucian, et al., 2006; Pesenti, Thioux, Seron, & Volder, 2000). Activation noted in executive processing areas of the brain across subjects and representational forms is consistent with the expectation that the questions asked would require subjects to organize cryptography concepts in their minds and apply those concepts to the problems presented before responding.

Executive processing activation provides evidence in support of constructivist learning theories of Piaget and Bruner, which is a significant finding of this research. Consistent activation of this area of the brain provides suggests that subjects were attempting to make sense of the questions presented using the mental models each developed or revised during this study's classroom instruction. Questions presented during fMRI were conceptually consistent with material taught during classroom instruction, but were novel presentations in their detail of cryptography. According to Bruner, these representational forms instigated processing of these questions as new encounters with knowledge, as described by Piaget. Based on Piaget's theories, the brain then began to process these questions as new encounters with cryptography knowledge and attempted to integrate them into the subject's existing mental model. According to Broadmann's mapping of brain areas, integration became the job of Area 46. Results from this study, however, are not consistent with other studies of cognitive processing of mathematics and of cryptography.

Average brain activation patterns in this study were only partially consistent with activation patterns noted in Thomas, Wilson, Corballis, & Yoon (2010). Unlike that study, this study did not find a consistent pattern of activation of the intraparietal sulcus (IPS) based on questions presented in any representational form. Posterior superior parietal lobule (PSPL) activation was found only in analysis of responses to graphical representation, whereas Thomas, Wilson, Corballis, & Yoon (2010) found activation in the PSPL during analysis of activity stimulated through both mathematical and graphical representational forms. The most likely explanation for the inconsistencies between this study and Thomas, Wilson, Corballis, & Yoon (2010) is that the two works studied cognitive processing of different mathematical topics. Specifically, the study of applied mathematics in this study is in contrast in complexity of the problem to the study of basic mathematics in Thomas, Wilson, Corballis, & Yoon (2010) and, therefore, may explain significant differences in average brain activation patterns between these two studies. The act of applying conceptual knowledge to novel situations in this study was a different request of learners than recognizing translation of basic mathematical functions to the correct graph as required of subjects in Thomas, Wilson, Corballis, & Yoon (2010).

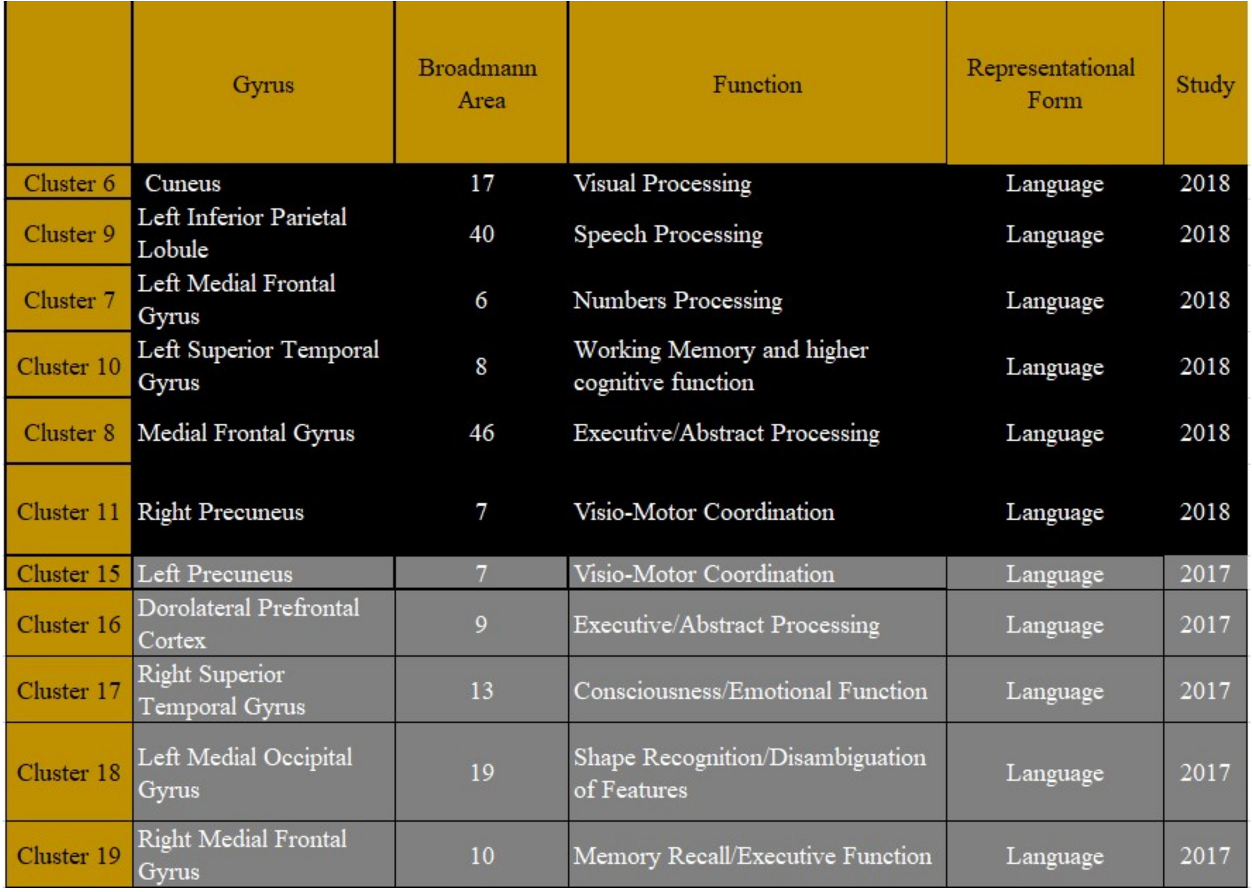
Areas of brain activation noted in this study were also inconsistent with the previous study of this research question that used the same scan protocol. Comparisons of brain activation in this study stimulated by mathematical and graphical representational forms, respectively, did not show any common areas of brain activation with the same activation patterns from Beckman, Bari, Chen, Dark, and Yang (2017). Questions presented in the language representational form in both Beckman, Bari, Chen, Dark, and Yang (2017) and this study produced a consistent pattern of activation in Broadmann Area 7, related to visio-motor coordination. A full accounting of similarities and differences in brain activation between this study and Beckman, Bari, Chen, Dark, and Yang (2017) are detailed in Tables 27-29 below.

Table 19: Active Areas by Study, Mathematical Representation



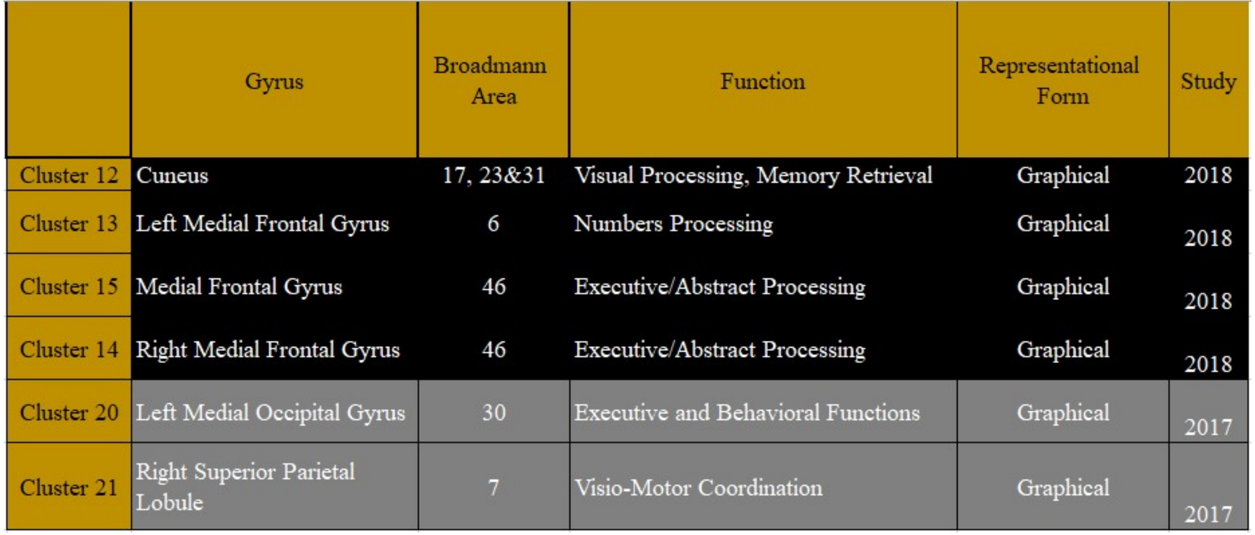
	Gyrus	Broadmann Area	Function	Representational Form	Study
Cluster 3	Cuneus	17	Visio-Motor Coordination	Mathematics	2018
Cluster 2	Left Medial Frontal Gyrus	6	Numbers Processing	Mathematics	2018
Cluster 5	Medial Frontal Gyrus	46	Executive/Abstract Processing	Mathematics	2018
Cluster 1	Precuneus	4	Primary Motor and Visual Processing	Mathematics	2018
Cluster 4	Right Medial Frontal Gyrus	46	Executive/Abstract Processing	Mathematics	2018
Cluster 12	Medial Temporal Gyrus	39	Spatial Cognition	Mathematics	2017
Cluster 13	Left Precuneus	31	Visio-Motor Coordination	Mathematics	2017
Cluster 14	Dorolateral Prefrontal Cortex	9	Executive/Abstract Processing	Mathematics	2017

Table 20: Active Areas by Study, Language Representation



	Gyrus	Broadmann Area	Function	Representational Form	Study
Cluster 6	Cuneus	17	Visual Processing	Language	2018
Cluster 9	Left Inferior Parietal Lobule	40	Speech Processing	Language	2018
Cluster 7	Left Medial Frontal Gyrus	6	Numbers Processing	Language	2018
Cluster 10	Left Superior Temporal Gyrus	8	Working Memory and higher cognitive function	Language	2018
Cluster 8	Medial Frontal Gyrus	46	Executive/Abstract Processing	Language	2018
Cluster 11	Right Precuneus	7	Visio-Motor Coordination	Language	2018
Cluster 15	Left Precuneus	7	Visio-Motor Coordination	Language	2017
Cluster 16	Dorolateral Prefrontal Cortex	9	Executive/Abstract Processing	Language	2017
Cluster 17	Right Superior Temporal Gyrus	13	Consciousness/Emotional Function	Language	2017
Cluster 18	Left Medial Occipital Gyrus	19	Shape Recognition/Disambiguation of Features	Language	2017
Cluster 19	Right Medial Frontal Gyrus	10	Memory Recall/Executive Function	Language	2017

Table 21: Active Areas by Study, Graphical Representation



	Gyrus	Broadmann Area	Function	Representational Form	Study
Cluster 12	Cuneus	17, 23&31	Visual Processing, Memory Retrieval	Graphical	2018
Cluster 13	Left Medial Frontal Gyrus	6	Numbers Processing	Graphical	2018
Cluster 15	Medial Frontal Gyrus	46	Executive/Abstract Processing	Graphical	2018
Cluster 14	Right Medial Frontal Gyrus	46	Executive/Abstract Processing	Graphical	2018
Cluster 20	Left Medial Occipital Gyrus	30	Executive and Behavioral Functions	Graphical	2017
Cluster 21	Right Superior Parietal Lobule	7	Visio-Motor Coordination	Graphical	2017

In tables 19-21, only this study and Beckman, Bari, Chen, Dark, and Yang (2017) are compared because both studies used the same fMRI scan protocol and domain knowledge, which eliminates one potentially confounding variables from the comparison. Several possible explanations for differences in brain activation under fMRI between this study and Beckman, Bari, Chen, Dark, and Yang (2017) remain. One assumed difference between the two studies that may account for divergent patterns of activation between them is the assumed difference in subjects' mathematical backgrounds. The spring 2017 work was performed using technology students, who likely had weaker backgrounds in mathematics compared to the computer science students in this study. No data on mathematical backgrounds of subjects was collected for the 2017 study, but the assumption is strong because mathematics requirements for entry into the University's computer science undergraduates include calculus, whereas no mathematics requirements are present for the course from which all 2017 subjects were drawn. Other differences between Beckman, Bari, Chen, Dark, and Yang (2017) and this study that may have complicated the comparison of brain activation data including: the use of different instructors by study, differences in the topics taught, and larger instructional groups in the 2017 study.

While common areas of brain activation were found during investigation of RQ1, the analysis comparing brain activation patterns between the UF and FU treatment groups found no significant differences in activation in support of RQ2. The negative result of this investigation may suggest that differences in instructional methods do not change where in the brain cryptography concepts are processed. If changes to instructional methods do not change the location of brain activity, then investigating the areas in which cryptography is processed in the brain has no role in evaluating instructional methods used to maximize cryptography learning. With that said, delimitations on instructional methods studied and on the aspects of cognitive processing studied may have severely impacted the results of this analysis of RQ2 and, consequently, the implications of these cognitive processing results for practice. Only two instructional methods were considered in this work. The two instructional methods differed only in order, not in content. It is possible, and perhaps likely, that a difference in cognitive processing of cryptography by treatment group was not observed because all subjects ultimately got the same instruction – just in a different order.

The possibility also exists that the treatment group did differ in how they processed cryptography as a result of the differences in instruction in this study, but those differences did not appear as differences in the location of activation. This study did not investigate changes in the connections among brain areas, commonly referred to as “white matter”, formed during cryptography instruction. By tracking changes in connections in subjects’ brains before and after cryptography instruction, then averaging those changes by instructional group, it is possible that effects on subjects’ brains attributable to differences in instructional method may have been illuminated. The negative result of the analysis comparing brain activation by instructional method produced no implications for the practice of instructing cryptography, but the analysis may have been negatively impacted by the lack of content variety in the instruction and lack of investigation of changes in white matter after instruction.

While the lack of a positive result in the investigation of RQ2 diminishes the practical implications of the cognitive processing component of this study, it provides fodder for modularists in theoretical debates about cognitive processing. This study has relied on a theoretical basis in which cognitive processing is modular by type of processing required – a functional specialization in the brain (Barrett & Kurzban, 2006, p. 630). Barrett & Kurzban (2006) summarizes modularist theories of cognition well, and refutes some of the arguments against). That is, when one must process visually, a particular area of the brain is activated. When one is manipulating numbers, a separate area of the brain becomes active. The lack of differentiation by instructional method of brain activation during cognitive processing supports modularist views of cognitive processing. Because learners in both treatment groups were performing the same function (solving conceptual cryptography problems), according to modularist theories, their patterns of brain activation should be the similar, even though subjects in the different treatment groups may have been solving the problems in different ways.

The cognitive processing component of this study contributes to research in cognitive processing by identifying areas of brain activation used by undergraduate computer science cryptography learners, to learning theory, and to cognitive theory. Results from the classroom learning component of this study are explainable using constructivist learning theories, but the results from the cognitive processing component lend further support to those results. As is true of the classroom learning results, the small sample size from which brain activation data was gathered provide little power, and consequently, little support of the conclusions presented. Rather, this study can serve as a beginning point for additional research in cryptography learning.

CONCLUSIONS AND FUTURE WORK

Cryptography Learning

Investigation of the influence of the order of instructional support for representational understanding and representational fluency produced inconsistent results. Apparent inconsistencies between the inferential and descriptive statistical analyses of this study's learning data suggest that the primary task of future work should be to recruit a larger group of participants. Work focused on comparing the efficacy of different instructional methods on computer science (CS) students (or those with a similar background in mathematics) against the efficacy of those methods on other subjects of differing mathematical backgrounds could add to our understanding of the role of instructional methods in cryptography learning and increase its sample size through diversity. Research that continues to focus on the efficacy of different instructional methods among subjects may benefit in recruitment by: not including an fMRI component to the study, expanding the study across educational institutions, or running the study over the course of multiple academic terms, although each solution comes with its own challenges in terms of both administration and internal validity.

In addition to increasing the number of participants in the study, future investigations of the impacts of instructional methods and/or mathematics background on cryptography learning would be well served to broaden and deepen the topics of instruction. The five cryptography topics that were the subjects of instruction in this study should not be considered to be representative of all topics in cryptography in terms of how instructional method or math background applies to them. The greater number of cryptography topics taught during future studies, the better our understanding will be of the factors influencing cryptography learning by topic and in general. One way to address this issue is to teach multiple sections of cryptography to subjects in parallel and using different instructional methods by section. Because such an arrangement would be quite taxing on an individual instructor, rotation of multiple instructors through the sections by topic should be considered.

Future studies of cryptography learning and instruction should include a control group in which subjects are instructed using language and mathematical formulae – a symbolic representation only group. While larger groups of subjects may provide greater insights into the questions investigated in this study, this study did not address the comparative impact of instruction using a single representation versus instruction using multiple representational forms on cryptography learning. As in engineering (Moore, Miller, Lesh, Stohlmann, & Kim, 2013), chemistry (Kozma, Russell, Jones, Marx, & Davis, 1996), and physics, (Hill, 2015), one justification for the use of multi-representational instruction is its demonstrated ability to increase conceptual learning in a domain compared to instruction using single representational forms. Studying the comparative impacts on learning of single versus multi-representational instruction is important to a full understanding of the impacts of different instructional methods on cryptography learning.

Finally, future studies of cryptography learning would benefit from a standard, validated body of knowledge accompanied by vetted learner assessment instruments. Unfortunately, the lack of a standard body of knowledge and learner assessments is a challenge that can only be overcome over time and through the work of experts in the field of cryptography and instruction. Until this problem is fully addressed, research on cryptography learning will continue to struggle to gain a full understanding of how various learners most effectively learn cryptography and what learners need to know to fully benefit from cryptography instruction.

Cognitive Processing of Cryptography

This study of cognitive processing of cryptography did not produce results that can be directly applied to cryptography instruction, but did shed light on additional areas of research that could impact cryptography instruction. In particular, the negative finding related to RQ2 and findings in RQ1 are only partially consistent across representational forms, topics, and among similar studies. Those inconsistencies mean that further experimental investigation of cognitive theories are required in order to gain a more complete understanding of how cryptography concepts are processed in the brain during problem solving. Further study of the comparative impacts of instructional methods on cognitive processing of cryptography, as in RQ1, could provide valuable insights by comparing cognitive processing in different instructional methods than were tested in this study and by comparing activation patterns among populations. Comparing activation patterns between those who received instruction in multiple representational forms against those who received instruction using one representational form may produce different results than the comparison of activation in this study that used two multi-form instructional methods. Comparisons of brain activation among subjects with different backgrounds in mathematical (or other) education may also shed light into what factors related to learning influence patterns of cognitive processing activity. Future analysis of cognitive processing activity should also investigate changes in white matter over the course of study. White matter changes would illustrate how the brain has changed over the course of study and, in combination with these data about where in the brain cryptography concepts are processed, could provide insight into how cryptography instruction in its various forms changes the brain in subjects across populations. A more complete understanding of how cryptography instruction changes the brain could provide the insights and spur the implications for practice sought in this study.

Further study of cryptography processing in the brain would also provide data that would further inform debates in cognitive theory. Future studies should study cognitive processing of cryptography in ways that test tenets of modularist, network, and hybrid theories of cognitive processing while also attempting to gain practically applicable insights into how instruction can be made better through analysis of cognitive processes. This study provided some support for a modularist view of cognitive processing. Cognitive processing of cryptography was found to activate specific areas of the brain as discussed in results from RQ2, but this support was limited. To an extent, activation patterns were a function of the representation in which the information was presented during questioning, as noted in these results. Based on comparisons of activation patterns between this study and Beckman, Bari, Chen, Dark, and Yang (2017), depth of mathematics education may impact activation patterns. Many other factors that may influence where in the brain cryptography concepts are processed remain uninvestigated. The simultaneous investigation of cognitive theory and instruction presents the possibility of finding aspects of cognitive processing that is both impactful to instruction and informative to cognitive theory. Such findings could be generalizable, potentially, to any number of subjects, instructional methods, or types of students.

As it relates to instruction in cryptography in particular, future research in cognitive processing should broaden to the use of other measurement tools, preferably in tandem. For example, the strong spatial resolution of fMRI could be combined with the excellent temporal resolution and (relative) lack of physical constraints on subjects provided by electro-encephalography to produce a rich data set in a study of the impacts of activity during instruction. Again, studies should be designed and their results analyzed both for applicability in the classroom and as a test of cognitive theory. By continuing this thread of research using different designs and tools, it may be possible to find insights into learning that are unique to the study of cognitive processing.

REFERENCES

Ainsworth, S. (2006). A conceptual framework for considering learning with multiple. *Learning and Instruction*, 183-198.

Anderson, L. W., Krathwohl, D. R., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., & Wittrock, M. (2001). *A taxonomy for learning, teaching and assessing: A revision of Bloom's taxonomy.* New York: Longman Publishing.

Barde, L. H., Yeatman, J. D., Lee, E. S., Glover, G., & Feldman, H. M. (2012). Differences in neural activation between preterm and full term born adolescents on a sentence comprehension task: implications for educational accommodations. *Developmental cognitive neuroscience*, S114-S128.

Barrett, H. C., & Kurzban, R. (2006). Modularity in cognition: framing the debate. *Psychological review, 113*(3), 628.

Barron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology, 51*(6), 1173-1182.

Beckman, J., Bari, S., Chen, Y., Dark, M., & Yang, B. (2017). The Impacts of Representational Fluency on Cognitive Processing of Cryptography Concepts. *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2017)* (pp. 59-67). USENIX Association.

Beckman, J., Dark, M., Kashyap, P., Wagstaff, S., Yang, B., & Chen, Y. (2017). Cognitive Processing of Cryptography Concepts: An fMRI Study. *ASEE Annual Conference and Exposition.* Colombus, Ohio: American Society for Engineering Education.

Biggs, J. B., & Collis, K. F. (2014). Evaluating the quality of learning: The SOLO taxonomy (Structure of the Observed Learning Outcome). *Academic Press*.

Blakemore, Dahl, Frith, & Pine. (2011). Developmental Cognitive Neuroscience. *Developmental Cognitive Neuroscience, 1*, 3-6.

Blakemore, S. J., & Bunge, S. A. (2012). At the Nexus of Neuroscience and Education. *Developmental cognitive neuroscience*, S1-S5.

Bloom, B. S. (1956). Taxonomy of educational objectives. Vol. 1: Cognitive domain. (pp. 20-24). New York: McKay.

Boyer, C. B. (1959). *The History of the Calculus and Its Conceptual Development: (The Concepts of the Calculus).* Dover.

Bressoud, D. M., Carlson, M. P., Mesa, V., & Rasmussen, C. (2013). The calculus student: insights from the Mathematical Association of America national study. *International Journal of Mathematical Education in Science and Technology, 44*(5), 685-698.

Bruer, J. (1997). Education and the Brain: A Bridge Too Far. *Educational Researcher, 26*(8), 4-16.

Bruner, J. S. (1964). The course of cognitive growth. *American Psychologist*, 1.

Cantlon, J. F., Brannon, E. M., Carter, E. J., & Pelphrey, K. A. (2006). Functional imaging of numerical processing in adults and 4-y-old children. *PLoS biology, 4*(5), 125.

Chadha, R., Delaune, S., & Kremer, S. (2009). Epistemic logic for the applied pi calculus. *Formal Techniques for Distributed Systems*, 182-197.

Chi, M. T., Glaser, R., & Farr, M. J. (1988). *The nature of expertise.* Hillsdale, NJ: Lawrence Erlbaum Associates.

Chi, M., Feltovich, P. J., & Glaser, R. (1981). Categorization and representation of physics problems by experts and novices. *Cognitive science, 5*(2), 121-152.

Chochon, F., Cohen, L., Moortele, P. V., & Dehaene, S. (2004). The change of the brain activation patterns as children learn algebra equation solving. *Proceedings of the National Academy of Sciences, 101*(15), 5686–5691.

Clements-Stephens, A. M., Materek, A. D., Eason, S. H., Scarborough, H. S., Pugh, K. R., Rimrodt, S., & Cutting, L. E. (2012). Neural circuitry associated with two different approaches to novel word learning. *Developmental cognitive neuroscience*, S99-S113.

Dark, M., & Manigault, C. (2006). Model eliciting activity for problem solving in information assurance. *Proceedings of the IA Symposium at SUNY Albany.* Albany, NY.

Delice, A., & Kertil, M. (2015). Investigating the representational fluency of pre-service mathematics teachers in a modelling process. *International journal of science and mathematics education*, 631-656.

Evans, K., & Reeder, F. (2010). *A Human Capital Crisis in Cybersecurity: Technical Proficiency.* CSIS.

Hayes, A. F. (2013). *Introduction to Mediation, Moderation, and Conditional Process Analysis : A Regression-based Approach.* Guilford.

Hill, M. J. (2015). *Scientific representational fluency: defining, diagnosing, and developing.* ISC2. (2018). *ISC2 Global Information Security Workforce Study, 2018.* ISC2.

Kaput, J., Noss, R., & Hoyles, C. (2002). Developing new notations for a learnable mathematics in the computational era. *Handbook of international research in mathematics education*, 51-75.

Kozma, R. B., & Russell, J. (1997). Multimedia and understanding: Expert and novice responses to different representations of chemical phenomena. *Journal of research in science teaching, 34*(9), 949-968.

Kozma, R. B., Russell, J., Jones, T., Marx, N., & Davis, J. (1996). The use of multiple, linked representations to facilitate science understanding. *Based on presentations at the NATO Symposium on International Perspectives on the Psychological Foundations of Technology-Based Learning Environments.* Crete: Lawrence Erlbaum Associates, Inc.

Kozma, R., Chin, E., Russell, J., & Marx, N. (2000). The roles of representations and tools in the chemistry laboratory and their implications for chemistry learning. *The Journal of the Learning Sciences*, 105-143.

Kucian, K., Loenneker, T., Dietrich, T., Dosch, M., Martin, E., & Von Aster, M. (2006). Impaired neural networks for approximate calculation in dyscalculic children: a functional MRI study. *Behavioral and Brain Functions, 2*(1), 31.

Kwong, K. K., Belliveau, J. W., Chesler, D. A., Goldberg, I. E., Weisskoff, R. M., Poncelet, B. P., . . . Rosen, B. R. (1992). Dynamic magnetic resonance imaging of human brain activity. *Proceedings of the National Academy of Sciences, 89*(12), 5675-5679.

Leinhardt, G., Zaslavsky, O., & Stein, M. K. (1990). Functions, graphs, and graphing: Tasks, learning, and teaching. *Review of educational research*, 1-64.

Lesh, R., & Doerr, H. M. (2003). *Beyond constructivism: Models and modeling perspectives on mathematics problem solving, learning, and teaching.* Routledge.

Lesh, R., & Lehrer, R. (2003). Models and modeling perspectives on the development of students and teachers. *Mathematical thinking and learning*, 109-129.

Lesh, R., Post, T. R., & & Behr, M. (1987). Representations and translations among representations in mathematics learning and problem solving. In L. Erlbaum, *Problems of representations in the teaching and learning of mathematics.*

Logothetis, N. K., Pauls, J., Augath, M., Trinath, T., & Oeltermann, A. (2001). Neurophysiological investigation of the basis of the fMRI signal. *Nature, 412*(6843), 150.

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014). Toward Curricular Guidelines for Cybersecurity. *Proceedings of the 45th Annual Technical Symposium on Computer Science Education* (pp. 81-82). Atlanta: ACM.

Moore, T. J., Miller, R. L., Lesh, R. A., Stohlmann, M. S., & Kim, Y. R. (2013). Modeling in engineering: The role of representational fluency in students' conceptual understanding. *Journal of Engineering Education*, 141-178.

Muller, D., Judd, C. M., & Yzerbyt, V. Y. (2005). When moderation is mediated and mediation is moderated. *Journal of personality and social psychology, 89*(6), 856.

Nakashima, E. (2017, January 12). Russian government hackers penetrated DNC, stole opposition research on Trump. *The Washington Post*.

O'Neill, G., & Murphy, F. (2010). Guide to taxonomies of learning.

Panksepp, J., & Panksepp, J. B. (2000). The seven sins of evolutionary psychology. *Evolution and cognition, 6*(2), 108-131.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, 76-79.

Pesenti, M., Thioux, M., Seron, X., & Volder, A. D. (2000). Neuroanatomical substrates of Arabic number processing, numerical comparison, and simple addition: A PET study. *Journal of cognitive neuroscience, 12*(3), 461-479.

Piaget, J. (1964). Part I: Cognitive development in children: Piaget development and learning. *Journal of research in science teaching, 2*(3), 176-186.

Pierce, A. O. (2016). *Exploring the Cybersecurity Hiring Gap.*

Qin, Y., Carter, C. S., Silk, E. M., Stenger, V. A., Fissell, K., Goode, A., & Anderson, J. R. (2004). The change of the brain activation patterns as children learn algebra equation solving. *Proceedings of the National Academy of Sciences, 15*(101), 5686-5691.

Raichle, M. E., & & Mintun, M. A. (2006). Brain work and brain imaging. *Annu. Rev. Neurosci.*(29), 449-476.

Rau, M., Scheines, R., Aleven, V., & Rummel, N. (2013). Does Representational Understanding Enhance Fluency-Or Vice Versa? Searching for Mediation Models. *Educational Data Mining*.

Ristenpart, T., & Yilek, S. (2010). When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. *NDSS* (pp. 121-128). The Network and Distributed System Security Symposium.

Rittle-Johnson, B. (2006). Promoting transfer: Effects of self-explanation and direct instruction. *Child development, 77*(1), 1-15.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 conference on Information technology education*, 113-122.

Schembari, N. P. (2007). 'Hands-On Crypto': Experiential Learning in Cryptography. *Proceedings of the 11th Colloquium for Information Systems Security Education* (pp. 7-13). Boston: CISSE.

Schneider, F. (2013). Cybersecurity Educaiton in Universities. *IEEE Security & Privacy, 11*(4), 3-4.

Simms, X., & Chi, H. (2011). Enhancing cryptography education via visualization tools. *Proceedings of the 49th Annual Southeast Regional Conference* (pp. 344-245). ACM.

Suby, M., & Dickson, F. (2015). *The 2015 (ISC) 2 Global Information Security Workforce Study.* (ISC) 2.

Szűcs, D., & Goswami, U. (2007). Educational neuroscience: Defining a new discipline for the study of mental representations. *Mind, Brain, and Education, 1*(3), 114-127.

Tavakoli, A. S., Jackson, K., Moneyham, L., & Birmingham, A. (2009). Examining Mediator and Moderator Effect Using Rural Women HIV Study. *SAS Global Forum.*

Temkin, A. (2007). Teaching Cryptography to Continuing Education Students. *Fifth World Conference on Information Security Education* (pp. 121-128). Boston: Springer.

Thomas, M., Wilson, A., Corballis, M., Lim, V., & Yoon, C. (2010). Evidence from cognitive neuroscience for the role of graphical and algebraic representations in understanding function. *Mathematics Education, 6*(42), 607-619.

Tytler, R., Prain, V., & Peterson, S. (2007). Representational issues in students learning about evaporation. *Research in Science Education*, 313-331.

United States Office of Personnel Management. (2015). *Cybersecurity Incidents.* Washington, D.C.: United States Office of Personnel Management.