CERIAS

The Center for Education and Research in Information Assurance and Security

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

Joseph Beckman (beckmanj@purdue.edu, Melissa Dark, Ph.D. – Primary Investigator

Problem

"…[a] 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 systems after an attack." (Evans and Reeder, 2010) and the difficult of building experts through education in complex mathematical concepts such as those underlying cryptography (Sims & Chi, 2011).

Goal

Cybersecurity experts with not only deep technical skills, but also the capabilities to recognize and respond to complex and emergent behavior, as well as a "security mindset", which includes mastery in using abstractions and principles, assessing risk and handling uncertainty, problem-solving, and reasoning; coupled with facility in adversarial thinking. This study focuses on the instruction of cryptography principles.

Research Questions

1. When cryptography instruction is delivered to students using instructional methods focused on representational understanding and representational fluency, does the order of use of these methods in instruction matter? That is, does learner expertise in the representational forms used in instruction support learning through translation among representational forms, does translation support expertise in representational forms, or neither?
2. Does prior knowledge of mathematics impact cryptography learning? If so, how?
3. Can processing cryptography concepts be measured in cognitive performance using fMRI and is cognitive processing of cryptographic concepts influenced by instructional method?

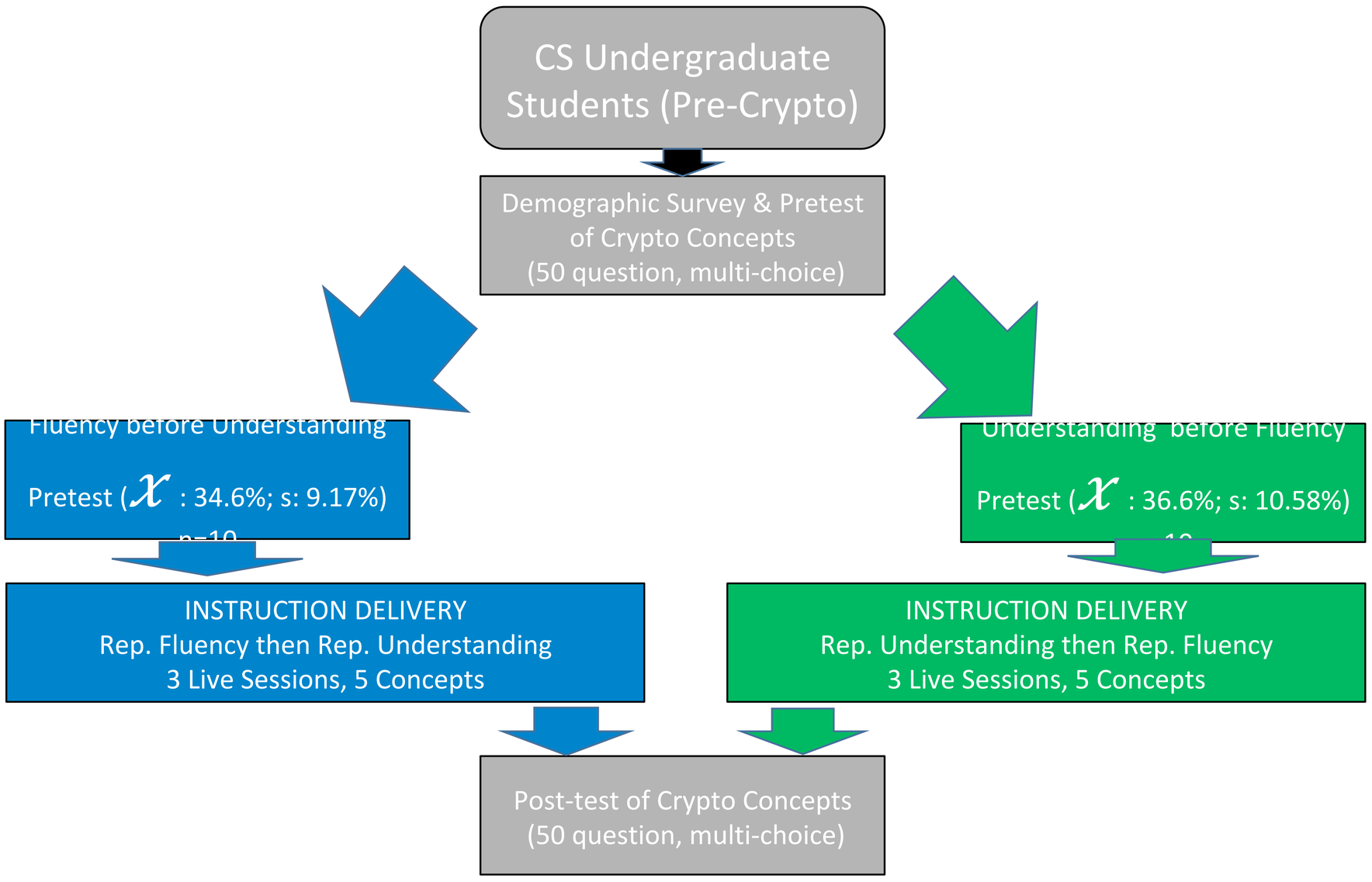
References

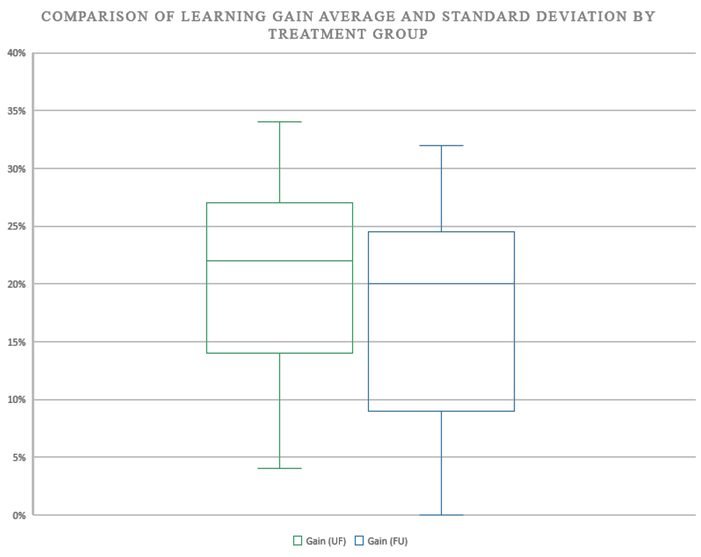
Lesh, R., Post, T., & Behr, M. (1987). Representations and translations among representations in mathematics learning and problem solving. Problems of representation in the teaching and learning of mathematics, 21, 33-40.

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

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.

Methods and Results





IM	Mean	Confidence Level Mean (95%)		Std Dev	Confidence Level Std Dev (95%)	
		Low	High		Low	High
FU	8.50	4.71	12.29	5.30	3.64	9.67
UF	10.50	7.40	13.60	4.33	2.98	7.90
Diff Pooled (FU-UF)	-2.00	-6.56	2.54	4.84	7.15	3.59

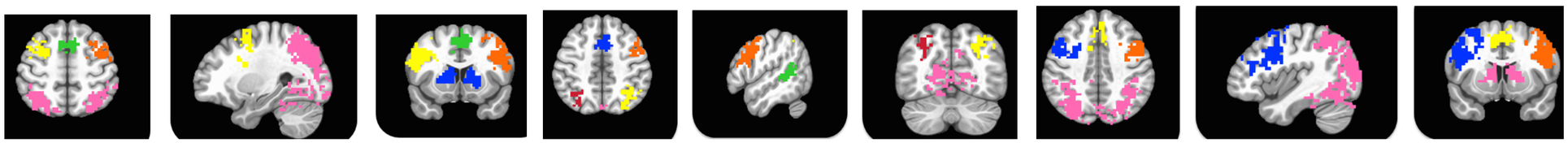
Summary of Stepwise Selection

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

	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

	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

	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



PURDUE UNIVERSITY Discovery Park

CERIAS®