ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE

Paper ID #38273

Engaging Children in Cryptology and Cybersecurity Learning and Career Awareness

Pavlo Antonenko

Zhen Xu

Do Hyong Koh

Christine Wusylko (University of Florida)

Kara Dawson

Swarup Bhunia

Amber Benedict

Amber Benedict is an assistant professor at Mary Lou Fulton Teachers College. Her work focuses on inclusive and collaborative instruction, and supporting general and special education teachers who work with students who struggle to read. In addition, she studies teacher instructional quality and supporting teams of teachers in effective instruction.Amber has published articles in Exceptionality, Learning Disabilities Quarterly, Teaching Exceptional Children,andIntervention School and Clinic. She is committed to collaborative grant writing and is the co-principal investigator of literacy projects funded by the National Science Foundation and the U.S. Department of Education, Institute of Education Sciences. A former special education teacher, Amber has taught in Iowa, Arizona, and Florida, and was a post-doctoral associate at Collaboration for Effective Educator Development, Accountability and Reform (CEEDAR Center) and clinical assistant professor within the College of Education at University of Florida.

Engaging Children in Cryptology and Cybersecurity Learning and Career Awareness

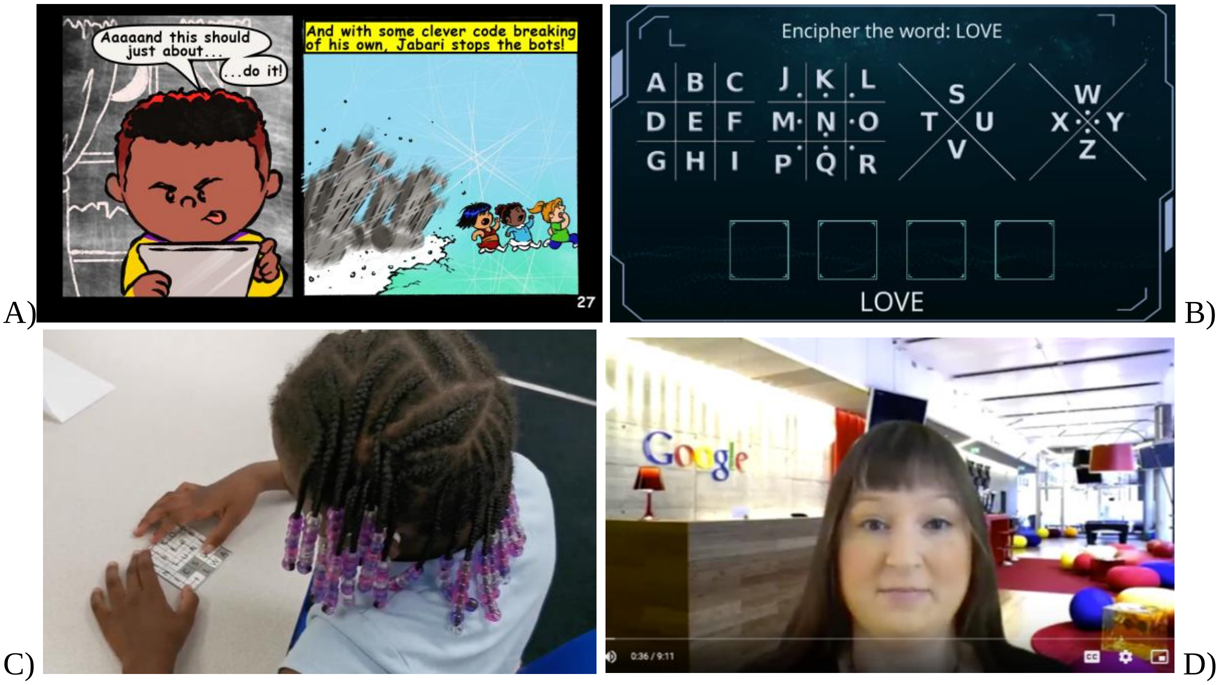
Introduction

Cryptology, the art of making and breaking codes (Stephenson, 2012), has been used to in secret communications for centuries. Nowadays, cryptology serves as the backbone of cybersecurity to protect the information security of the nation, businesses, and individuals (Parr & Penzl, 2010). However, cybercrime is one of the most challenging issues today, and cyberattacks have affected the operations of governments, businesses, and individuals (Interpol, 2020). People are impacted by cyberattacks in various ways. For example, Colonial Pipeline, the U.S. largest fuel supply operation, was forced to go offline due to a cyberattack, which in turn caused severe shot-term gas shortage in multiple states and impacted millions of people's everyday lives (Krauss et al., 2021). Technology companies have been largely investing into cybersecurity monetarily and technically (Rosenbaum, 2021). Following the Colonial Pipeline cyberattack, the White House issued an executive order to prioritize the security of technology across the country (White House, 2021). However, the country experiences a severe shortage of qualified cybersecurity professionals, due to a lack of graduates with STEM degrees (Crumpler & Lewis, 2019). Furthermore, the STEM workforce shortage is partly caused by persistent underrepresentation of women and ethnic minorities in STEM education and careers (Ambrose, 2019). For instance, women currently represent only 18% of the cybersecurity workforce and less than 12% of cybersecurity professionals are African American (U.S. Bureau of Labor Statistics, 2021). In 2017, the National Initiative for Cybersecurity Education (NICE) Workforce Framework was established with the aim to promote a network and ecosystem of cybersecurity education, training, and workforce development (Newhouse, et al., 2017). The 2011 White House executive order also instructed to initiate pilot programs to educate the public on the security capacity of software and Internet of things (IoT; the White House, 2021). Even though many efforts are being made to develop the cybersecurity workforce, little has been done to reach out to younger audiences and engage students in elementary grades, which is when children start to participate in activities in the cyberworld and begin to develop disciplinary preferences and career aspirations (Trans, 2018).

Our project aims to address this issue by designing, developing, and testing a technology-enhanced cryptology and cybersecurity curriculum for 3rd- to 5th-graders, with a specific focus on girls and students from ethnic minority groups. The curriculum is designed to cultivate students' interest and career awareness in cryptology and cybersecurity issues, and increase their symbolic and morphological awareness, which is important in these and many other careers. This curriculum is designed to be used in afterschool environments, because schoolteachers may find it hard to implement this 20-hour curriculum due to the curricular and assessment pressures of public K-12 education, specifically in math and reading. There were also no existing national K-12 school standards for teaching and assessing for cryptology and cybersecurity when we started the project in 2019.

To make this curriculum engaging, supportive, and exciting for all students, we conceptualized, designed and implemented four interrelated components (Figure 1): (1) a web and Android app that includes games, puzzles, simulations, and tools for students to learn about the content and practice the skills; (2) a series of unplugged activities that reinforce the content and skills with the teachers' guidance and usually require small group collaboration; (3) a comic book that provides an engaging story with 4 near-peer characters (3 ethno-culturally diverse girls and a boy) with a unique context for problem solving and integration of digital and unplugged activities; and (4) role model videos in which gender and race-matched cryptology and cybersecurity researchers and professionals introduce their professions.

Figure 1. Curriculum components: A) an example comic book page; B) a screenshot of a digital activity; C) an example of an unplugged activity; D) a screenshot of a role model video.



Theoretical Framework

Educational design research (EDR), also often referred to as design-based research, develops theory-informed and evidence-based solutions to address real-world problems and develop knowledge to inform other researchers and practitioners who encounter similar problems (McKenny & Reeves, 2012; 2018). Given the goal of this project – that is, to design, develop, and test a technology-enhanced elementary level cryptology and cybersecurity afterschool curriculum, EDR was deemed by the team the most appropriate approach.

The design of solutions in EDR is guided by existing theories, and the research in return contributes to the development and elaboration of theories. In this project, the design and development of the curriculum used a blend of learning and design theories. For example, guided by the Zone of Proximal Development theory and the associated concept of instructional scaffolding (Vygotsky, 1978), we designed a variety of small group unplugged activities and teacher guided discussions, in which student peers and teachers serve as "the more knowledgeable others" in the social interaction (Vygotsky, 1978). In addition to this social scaffolding, material scaffolding (Reiser & Tabak, 2014) is also provided in our app, including elaborated instructions, visual cues, guided examples, sound feedback, audio narrations, animated instruction, and so on. We also drew on the notion of distributed scaffolding, which refers to scaffolding embedded at multiple time points during the learning process and in different components of the learning environment (Puntambekar & Kolodner, 2005). For example, we designed the digital activities and unplugged activities to complement to each other; key concepts are presented to students and then reinforced in different learning materials; and we designed materials and activities to engage students visually, spatially, auditorily, and kinesthetically.

The design of the comic book was guided by the anchored instruction framework (Cognition and Technology Group at Vanderbilt, 1990). This technology-centered learning approach posits that providing students a story-driven "macrocontext" triggers and sustains students' engagement. A comic book was not originally in the our plans but we needed an engaging way to tie integrate various unplugged and digital activities and help children connect with the content we were developing. We created a story about three friends (Akila, Bai and Carly) who get sucked into the cyberworld after finding Akila’s Nana’s West African curio in the attic. The story is told through the perspective of Akila, and learners help the three friends and Akila’s little brother, Jabari, crack codes, solve puzzles, and learn the history of code making and breaking (i.e., cryptology) to help the girls escape. To find a way home, the children need to learn and apply various codes, ciphers, and knowledge of computer networks and cybersecurity to solve a variety of problems and puzzles. The comic book characters travel through space and time, meet relevant people in the history (e.g., Alan Turing), and experience historical events. Students in afterschool programs help the comic book characters solve problems and, ultimately, get out of the cyberworld. The comic book weaves the unplugged and digital activities together and the seamless experience of learning in various modalities and using different media is designed to immerse students in a state of flow (Csíkszentmihályi et al., 2021).

EDR values the participation and perspectives of multiple stakeholders such as practitioners, content experts, community members, and researchers from multiple relevant disciplines, etc. In this project, our research and development team consists of experts in educational technology, electrical and computer engineering, special education, cybersecurity, and STEM education. The team also includes 8 afterschool teacher leaders and administrators from five partner afterschool programs, as well as a post-doctoral researcher and graduate students with expertise in computer science, software development, graphic design, and educational measurement. A professional visual artist, an African American illustrator from our local community, contributed to the design of the story and development of the comic book. Additionally, our (mostly female) advisors from other research universities, cybersecurity research institutes, a cybersecurity industry partner (Raytheon), a national museum (National Cryptology Museum), and technology company (Google) provided valuable resources, feedback, and suggestions, and offered to serve as cryptology and cybersecurity role models in our project.

EDR develops solutions in multiple iterations, which means the solutions and products evolve throughout multiple cycles of design, development, and testing. In addition to observing afterschool educators and soliciting their feedback during the design and development phases, our curriculum went through two major pilot implementations in Fall 2020 and Spring 2021. Using qualitative and quantitative methods, we examined the feasibility, usability, and efficacy of the curriculum, and made careful modifications to all curricular components based on the results of these pilot implementations as part of our EDR.

The theoretical and practical implications generated from EDR should be grounded in empirical data collected in authentic learning settings (McKenny & Reeves, 2018). In Fall 2021, our curriculum was implemented nationally with 17 teachers and 232 elementary students in 16 afterschool programs. In this paper, we report results from this national implementation of our curriculum. Specifically, we address the following research questions:

(1) How does the curriculum impact students' learning of cryptology and cybersecurity?
(2) How does the curriculum impact students' identity and careers awareness in cryptology and cybersecurity?

Method

Participants

In Fall 2021, our curriculum was implemented in 16 afterschool classrooms across Southeastern U.S. Two hundred thirty-two elementary students and 17 teachers in urban, rural, and suburban afterschool programs participated in the implementation and research. These unique programs serve students from many underrepresented groups and communities - some programs serve only girls, others - only African American students, one program focused on students with learning disabilities, and two more – on supporting students and families who came to the United States as refugees. Participants' demographic information is provided in Table 1. It should be noted that 70% of our elementary student participants were girls and 72% identified as non-Caucasian (57% African American).

Table 1. Participant demographics

		N	%
Sex	Girls	163	70.26
	Boys	55	23.71
	I'd rather not say	5	2.16
Race	American Indian or Alaska Native	14	6.03
	Asian	6	2.59
	Black/African American	132	56.90
	Hispanic/LatinX	9	3.88
	Native Hawaiian or Other Pacific Islander	4	1.72
	White	53	22.84
	Other/ I'd rather not say	5	2.16
Age	8 years old	45	20.18
	9 years old	91	40.81
	10 years old	57	25.56
	11 years old	25	11.21
	12 years old	3	1.35

13 years old	1	0.45
I'd rather not say	1	0.44

Measures and data sources

We employed mixed research methods to obtain a more comprehensive understanding of students' learning of cryptology and cybersecurity as well as career awareness in learning this curriculum. Students' learning of cryptology and cybersecurity was measured using a 13-item assessment created by the research team. This assessment measures students' understanding of the key concepts in this curriculum. The design of the assessment was guided by the framework of Standards for Educational and Psychological Testing (AERA, 2014). This assessment was used before and after the implementation of the curriculum in the pretest/posttest format.

Engineering Identity Development Scale (EIDS; Capobianco et al., 2012) was adapted to assess the development of our participants' identity in cryptology and cybersecurity. EIDS was designed for and validated with pre-adolescent learners with Cronbach's alpha = 0.76. This 20-item instrument includes two subscales: (1) academic identity in engineering and (2) occupation identity in engineering. In this study, we adapted EIDS by changing the term "engineer" into "cryptologist" in the occupation identity subscale (and defining what the term means using age-appropriate language). The responses were recorded using a 3-point Likert scale from "Disagree" to "Agree." This instrument was also used in the pretest/posttest format.

Several researchers from the project team observed each implementation session in two afterschool programs. Guided by Fredricks and colleagues' (2004) theory of academic engagement, the observation protocol was developed and validated to focus on students' behavioral engagement, cognitive engagement, and emotional engagement as they participated in each individual learning activity. Field notes were used to record student and teacher actions and communications during curriculum implementation.

Finally, we conducted semi-structured interviews (Patton, 1990) with students in the two programs after the teachers finished implementing the curriculum. Eight students participated in the interviews. General questions about students' perceptions of the curriculum were asked, such as what they thought about the activities and what they felt they had learned. Students were also asked about their opinions about each curricular component: a) the comic book, b) unplugged activities, c) digital activities, and d) role models videos and discussions.

Data analysis

Quantitative data was analyzed using paired samples t-tests. The qualitative data was analyzed using thematic analysis (Braun & Clarke, 2012). We first converged data from both qualitative data sources. Then, we followed the six steps for conducting thematic analysis suggested by Braun and Clarke (2012) and generated themes reflecting students' learning and evolving awareness of cryptology and cybersecurity careers.

Results

Student learning of cryptology and cybersecurity

We used a paired samples t-test to compare the learning assessment scores from the pretest and the posttest. The result indicated a statistically significant difference between the mean scores on the pretest and posttest (M_{pre} = 5.51, SD_{pre} = 1.79, M_{post} = 7.46, $SD_{pos\ t}$= 2.39, t = 9.07, df = 143, $p < 0.001$). The effect size was large with Cohen's d = 0.76. Qualitative data served to further illuminate students' learning of cryptology and cybersecurity. In particular, the following themes emerged during our data analysis:

- Elementary students CAN successfully develop knowledge and skills in cryptology and cybersecurity.

We found that students were able to learn the knowledge and skills in cryptology and cybersecurity addressed in this curriculum. We observed that most students were able to recall and apply the key concepts they learned previously at the beginning of each session. In doing the small group unplugged activities, students actively collaborated with their peers to achieve learning goals and flexibly used the new vocabulary without prompts from the teacher. In doing individual digital activities, they were willing to share their knowledge and experience with peers and help each other. All of the interviewees were able to recall a variety of concepts from their afterschool sessions, which covered the majority of the content of this curriculum.

- Teacher scaffolding is critical to successful learning

Even though we designed a variety of material scaffolds in the digital activities and in the paper-based materials, we found that some students and student teams did not use the scaffolds. For example, some students did not listen to the audio narration of the comic book, or read the activity instructions carefully. However, the just-in-time social scaffolding provided by teachers (i.e., “more knowledgeable othhers”) successfully supported students in learning. The scaffolding included providing examples and analogies to explain and reinforce abstract knowledge, explicitly guiding students to compare and contrast concepts, etc.

Development of career awareness and identity in cryptology and cybersecurity

In our study, the EIDS instrument was used to measure students' careers awareness in cryptology and cybersecurity using the pretest and posttest format (Capobianco et al., 2012). We compared the pretest and posttest EIDS scores and its two subscales (academic idenitity and occupational identity) using paired samples t-tests. Results indicated no statistically significant difference between the mean total EIDS scores on the pretest and posttest. The difference between the pretest and posttest scores for the academic identity subscale was not statistically significant either. However, the difference in the scores on the occupational identity scale approached statistical significance (M_{pre} = 26.01, SD_{pre} = 4.99, M_{post} = 26.93, SD_{post} = 4.54, t = 1.78, df = 143, p = 0.08). Qualitative data also provided evidence suggesting students' improvement in cryptology and cybersecurity career awareness.

- Students demonstrated evolving awareness of the cryptology and cybersecurity-related professions that they never heard about before.

In the interview, students expressed that they had never heard about the profession of cryptologist and shared that they had known very little about the careers of a cybersecurity engineer or a cybersecurity analyst prior to the curriculum. Students told us that they gained some understanding about these professions, the skills that are needed, and how these professionals contribute to our country's national security from this curriculum. During class, students also repeatedly expressed their admiration for these professionals.

- Girls were inspired by female cryptology and cybersecurity role models.

We found that the female role models in particular inspired the girls who participated in the curriculum implementation. The girls were excited when they learned about female cryptologists during WWII (the WAVES program – Women Accepted for Volunteer Emergency Service) and female cybersecurity engineers. In the observation notes, multiple researchers wrote that girls said "wow!" "cool!" when they were introduced female cryptology and cybersecurity role models. In the interview, one female participant told us, "After hearing about this program [curriculum], and [WAVES ladies in] World War II, I felt really good about these women. I could maybe look up to them and say, wow, maybe that could be me one day."

Conclusion

In this study, we explored students' learning and development of an identity and cryptology and cybersecurity as well as career awareness in a 20-hour afterschool curriculum that introduces cryptology and cybersecurity to elementary-aged children. Our data suggest that children as young as 8-9 years old understand and can master cryptology and cybersecurity concepts and skills. Our participants' understanding of cryptology and cybersecurity concepts significantly improved as a result of participating in this curriculum. We also found that our curriculum allowed students to start developing an awareness of the related professions and occupational identity as a cryptologist. Girls were especially inspired by the female cryptology and cybersecurity role models integrated in our comic book story (Akila's Nana, a WWII WAVES cryptologist) and practicing female cybersecurity experts in our role model videos.

Acknowledgements

This material is based upon work supported by the National Science Foundation under DRL-ITEST Grant No. 1849768. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

Ambrose, M. (2019). *Panel warns US faces STEM workforce supply challenges*. American Institute of Physics. https://www.aip.org/fyi/2019/panel-warns-us-faces-stem-workforce-supply-challenges

American Educational Research Association, American Psychological Association, & National Council on Measurement in Education. (2014). *Standards for educational and psychological testing.* (2014th ed.). American Educational Research Association.

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 57–71). American Psychological Association. https://doi.org/10.1037/13620-004

Capobianco, B. M., French, B. F., & Diefes-Dux, H. A. (2012). Engineering identity development among pre-adolescent learners. *Journal of Engineering Education*, *101*(4), 698-716.

Cognition and Technology Group at Vanderbilt. (1990). Anchored instruction and its relationship to situated cognition. *Educational Researcher*, 2-10.

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity Workforce Gap. In *Center for Strategic and International Studies (CSIS)*. http://www.isaca.org/Knowledge-Center/

Csíkszentmihályi, M., Abuhamdeh, S., & Nakamura, J. (2021). *Flow*. Natur & Kultur Allmänlitteratur.

Fredricks, J. A., Blumenfeld, P. C., & Paris, A. H. (2004). School engagement: Potential of the concept, state of the evidence. Review of educational research, 74(1), 59-109.

Interpol. (2020). COVID-19 Cybercrime Analysis Report. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Krauss, C., Chokshi, N., & Sanger, D. (2021, May 12). Gas pipeline hack leads to panic buying in the southeast. *The New York Times*. https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html

McKenney, S., & Reeves, T. C. (2012). Conducting educational design research. In *Handbook of research on educational communications and technology*. Springer. http://dspace.ou.nl/handle/1820/4034

McKenney, S., & Reeves, T. C. (2018). *Conducting educational design research*. Routledge.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. In *NIST special publication 800-181*. https://doi.org/10.1201/b19962

Paar, C., & Penzl, J. (2010). *Understanding cryptography*. Springer.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Puntambekar, S., & Kolodner, J. L. (2005). Distributed scaffolding: Helping students learn science from design. *Journal of Research in Science Teaching*, *42*(2), 185–217. https://doi.org/10.1002/TEA.20048

Reiser, B. J., & Tabak, I. (2014). Scaffolding. In R. K. Sawyer (Ed.), *The Cambridge Handbook of the Learning Sciences, Second Edition* (pp. 44-62). Cambridge University Press. https://doi.org/10.1017/CBO9781139519526.005

Rosenbaum, E. (2021). *Microsoft has a $20 billion hacking plan, but cybersecurity has a big spending problem.* CNBC. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Stephenson, N. (2012). *Cryptonomicon*. Random House.

The White House. (2021). *Executive order on improving the nation's cybersecurity*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Tran, Y. (2018). Computer programming effects in elementary: Perceptions and career aspirations in STEM. *Technology, Knowledge, & Learning*, 23(2), 273-299.

U.S. Bureau of Labor Statistics. (2021a). Occupational Outlook Handbook: Information Security Analyst. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Vygotsky, L. (1978). Interaction between learning and development. In *Mind and society* (pp. 79–91). Harvard University Press.