International Conference
The Future of Education

Enhancing Cryptography Education Using Collaborative Visual Programming

Sherif Abdelhamid, Sarah Patterson, Blain Patterson

Virginia Military Institute, United States of America[1]

Abstract

Cryptography is the science of securing sensitive information and ensuring that only the intended recipients can access and process the encrypted data. Internet shopping, online payments, and social networking websites have become increasingly popular with the advancement of the internet. However, hackers are getting more skilled than before to exploit existing vulnerabilities and attack these websites. Due to this, it has become increasingly important to introduce the science of cryptography to future generations, at a younger age, in straightforward and more engaging ways [1]. Students need to acquire multidisciplinary skills in mathematics, information theory, and software programming to achieve this goal. In addition, students have to receive formal training in software testing and big data analysis. These requirements might create a barrier for non-computer science students and domain scientists to develop novel encryption algorithms or enhance existing ones. Existing studies in cryptography education focus on how to break down complex mathematical concepts into simpler forms, but few studies have examined the programming challenges during algorithm implementation. As a response, we implemented a web-based programming learning tool called vizLab. The tool will help students bridge the gap between cryptography's mathematical foundations and computing by using a visual approach to programming. Students will learn to construct data cryptography algorithms with minimal programming experience, using graphical icons representing the language's essential elements. vizLab can execute the students' block-based algorithms online; also, it can translate them into a high-level programming language (Python). Additionally, vizLab can store the completed blocks within an online cloud database. Students can share the constructed blocks with peers working on the same projects. Finally, students can integrate vizLab with learning management systems (LMS) to share their work with their instructors for assessment.

Keywords: *Cryptography education, block-based programming, collaborative e-learning*

1. Introduction

1.1 Background and challenges

Developing new encryption algorithms, or enhancing existing ones, requires students to master various skills in addition to formal training in software testing and big data analysis. Future generations might find these requirements a barrier to learning about cryptography [2]. In cryptography education, studies usually focus on how to simplify complex mathematical concepts, but few examine the programming challenges involved with implementation [3]. Furthermore, learning to program encryption algorithms requires that learners think in an organized and procedural way about the problems they are attempting to solve [4]. Programming needs problem-solving skills and is also dependent on various cognitive controls and styles of learners. In fact, field independence, logical reasoning, and direction-following skills were highly correlated with programming skills among college students [5]. Finally, one of the key requirements for learning programming is also the ability to understand and use variables, understand the dynamic nature of the values of variables, the degree of complexity in using variables, and the level of reasoning required [6].

1.2 Research Goal and Contributions

The ability to alleviate the extrinsic cognitive overhead reflects the learners' capacity to master computer programming and becomes the main gauge for their ability to develop novel encryption algorithms or enhance existing ones, which is the primary research goal of vizLab. vizLab aims to make students focus on the core cryptography concepts and programming skills with minimal extrinsic cognitive load. Our research contributions can be summarized as follows: (1) building vizLab that helps students use a visual approach to develop cryptography algorithms and (2) conducting a bibliographic analysis to explore and understand the research landscapes related to cryptography education.

2. Related Work

2.1 Literature Review

Researchers have taken different approaches to find out the most effective method of teaching security and cryptography. One option is to build security concepts into existing courses by adding the appropriate lessons to existing computer science courses [7,8]. Another alternative is creating separate security coursework or programs and concentrations [9]. Students can be motivated and engaged in the learning process by implementing active learning techniques, which can also be applied to cryptography curriculums [10,16]. Researchers studied the use of open-source software for cryptography education [11], and they found that the students' responses to the introduction of these systems have been positive. Another team of researchers used real-world scenarios illustrated by animation videos to demonstrate some well-known cryptographic protocols. Results showed that over 88% of the students found that the proposed platform increased their understanding speed [12]. In another research work [13], students were asked to create short videos presenting day-to-day cryptography topics. Results showed that 80% of students evaluated the experience as positive (agree or strongly agree). Researchers have used another group of tools called interactive classroom visualization (ICV) tools as an active learning technique [14]. ICV has been used for teaching security concepts in introductory computer classes and security-specific courses such as Cryptography and Information Warfare [15]. Another research work [3] proposed a cryptography-aware intelligent tutoring system that helps students detect crypto API misuse violations in secure applications.

2.2 Bibliographic Analysis

Following the literature review, we conducted a bibliometric analysis to identify research themes and explore the academic landscapes related to cryptography education. We conducted a bibliometric mapping using Crossref, a not-for-profit association of publishers, including both commercial and not-for-profit organizations. We specifically aimed to study the major research themes related to cryptography. From the retrieved publications (relevant to our topic of interest), we extracted terms (with minimum occurrences of ten) from the abstract and title, resulting in 468 keywords. Based on the co-occurrences of the terms within the same title or abstract, we constructed the term co-occurrence network, which consists of 14937 edges/links and 468 nodes. Each node represents a term, and each edge represents a co-occurrence relationship. Finally, we applied a network clustering algorithm, which identified seven main research clusters. The clusters can illustrate different research themes or directions relevant to cryptography. Cluster 1 (in red) contains key terms related to public-key cryptography, hardware, FPGA, and energy consumption. Cluster 2 (in green) represents research works related to elliptic curve cryptography, wireless sensor networks, smart grids, and vehicular ad hoc networks. Another cluster, number 3 (in dark blue), contains key terms related to visual cryptography, steganography, and digital watermarking. Cluster 4 (in yellow) is related to quantum cryptography, quantum physics, quantum mechanics, quantum communications, and error detection and correction. Our research work on cryptography education fits well within cluster 5 (purple color). Cluster 5 consists of key terms like students, courses, and teaching cryptography. Cluster 6 (in light blue) has terms related to cloud computing, data storage, secure data transfer, data privacy, and management. Finally, topics like chaos theory, chaotic cryptography, chaotic maps, and systems are found with cluster 7 (in orange color).

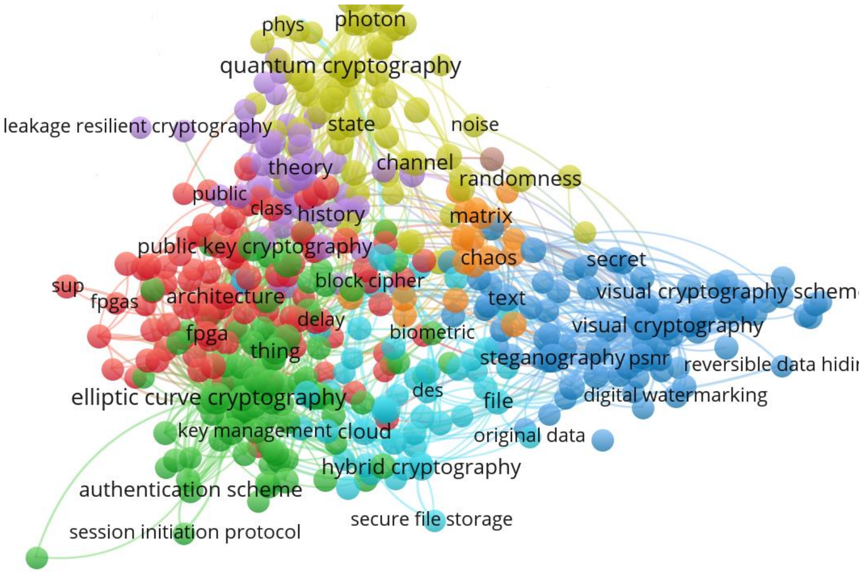
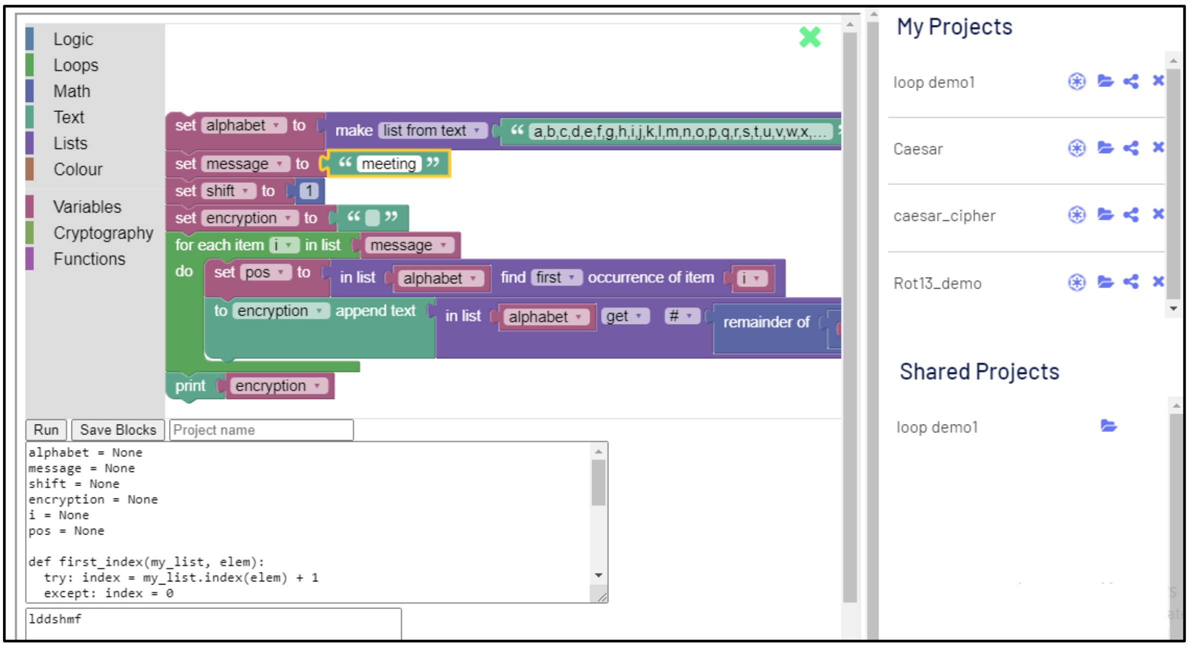


Fig. 1. The term co-occurrence network where each node represents a term, and each edge means a co-occurrence relationship. Nodes within the same cluster are assigned the same color.

Based on the related work review, we found that few studies have considered the programming challenges during cryptography algorithm implementation. Most of the studies focus on providing means to simplify the understanding of complex math concepts and algorithms but with little attention to the software development aspect. As a response, in this work, we implemented vizLab to provide an effective way for students to implement novel encryption algorithms or enhance existing ones. The bibliographic analysis revealed the significant themes within cryptography research. However, we found that the amount of research related to education is relatively small compared to other research directions. The findings from the bibliographic analysis are consistent with the related work discussion.

3. System Overview

vizLab is an independent online tool, part of CyEd cyberinfrastructure. vizLab uses the visual programming language (Blockly), where graphical icons represent the language's essential elements. The graphical icons can be selected, copied, and moved around in a workspace, and students can create various programming elements, including (e.g., action sequence, decision, iteration, and functions). Students can build the cryptography algorithms from scratch or use built-in visual blocks for each algorithm. The example in fig. 2. illustrates how students can create Caesar cipher from scratch. Additionally, students can store the created blocks in the database and can be retrieved later from the menu on the right. Students can share and collaborate with peers on various projects allowing them to build new algorithms on top of existing ones. Students can submit their code to a learning management system (e.g., Canvas) for evaluation and grading by instructors.


Logic
Loops
Math
Text
Lists
Colour
Variables
Cryptography
Functions
set alphabet to make list from text “ a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,...
set message to “ meeting ”
set shift to 1
set encryption to “ ”
for each item i in list message
do set pos to in list alphabet find first occurrence of item i
to encryption append text in list alphabet get # remainder of
print encryption
Run
Save Blocks
Project name
My Projects
loop demo1
Caesar
caesar_cipher
Rot13_demo
Shared Projects
loop demo1

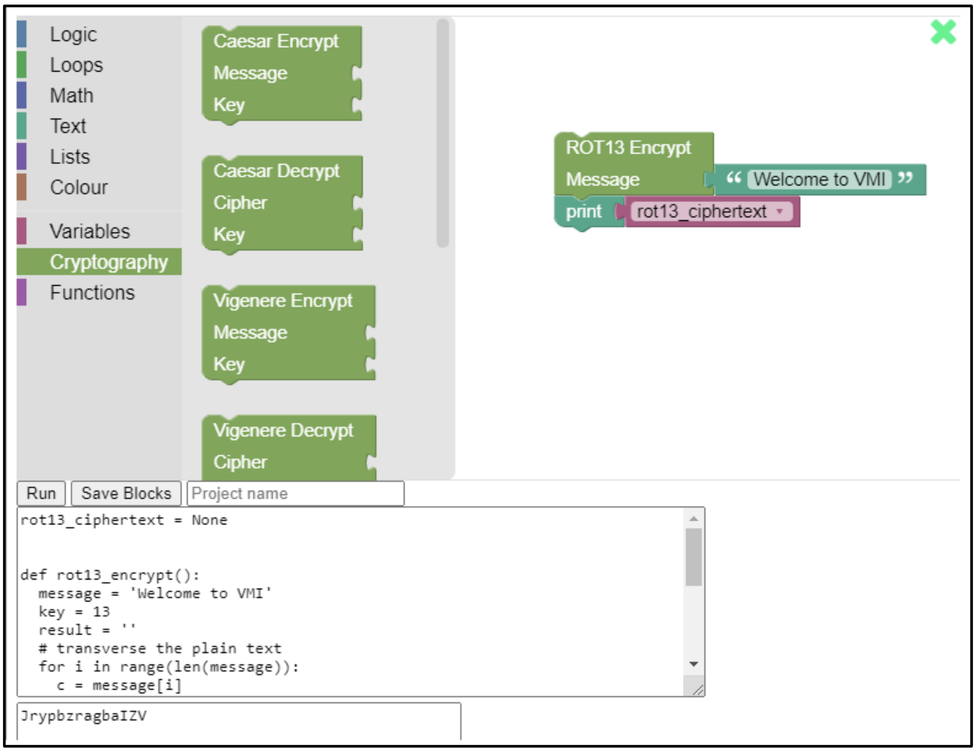
```
alphabet = None
message = None
shift = None
encryption = None
i = None
pos = None

def first_index(my_list, elem):
  try: index = my_list.index(elem) + 1
  except: index = 0
```

```
lddshmf
```

Fig. 2. Block-based learning of programming languages using VizLab.

Students can use the built-in cryptography library with ready-to-use blocks for various cryptography algorithms, see fig. 3. This feature is helpful for students who have no programming experience but are still interested in learning about various cryptography algorithms. vizLab is an extensible system because new blocks representing different cryptography algorithms will be added in the future by the community of researchers behind vizLab. One of the vizLab goals is to create a community of students, instructors, and cybersecurity researchers who can collaborate and continuously contribute to the tool.



```
rot13_ciphertext = None


def rot13_encrypt():
  message = 'Welcome to VMI'
  key = 13
  result = ''
  # transverse the plain text
  for i in range(len(message)):
    c = message[i]
```

```
JrypbzragbaIZV
```

Fig. 3. vizLab provides a ready-to-use library of cryptography blocks. For example, students here use the ROT13 block to encrypt an input message.

4. Conclusion and Future Work

In this research work, we presented vizLab, a web-based programming learning tool that helps students avoid the programming challenges during cryptography algorithm implementation. Our future work will involve integrating vizLab into an undergraduate course. In addition, we will collect and analyze data about students' conceptual understanding and their ability to construct cryptography algorithms using surveys and class observations.

Acknowledgment

This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit cyberinitiative.org.

References

1. McGettrick, A. Toward effective cybersecurity education. IEEE Security & Privacy, 11(6), 66-68 (2013).
2. Garera, S., & Vasconcelos, J. Challenges in teaching a graduate course in applied cryptography. ACM SIGCSE Bulletin, 41(2), 103-107 (2009.
3. Singleton, L., Zhao, R., Song, M., & Siy, H. CryptoTutor: Teaching Secure Coding Practices through Misuse Pattern Detection. 21st Annual Conference on Information Technology Education, 403-408 (2020).
4. Jonassen, David H. "Learning with technology: Using computers as cognitive tools." Handbook of research for educational communications and technology (1996).
5. Foreman, Kim Hyun-Deok. "Cognitive style, cognitive ability, and the acquisition of initial computer programming competence." (1988).
6. Nachmias, Rafi. "Variables--An Obstacle to Children Learning Computer Programming. Technical Report No. 8." (1986).
7. Petrova, Krassie, et al. "Embedding information security curricula in existing programmes." Proceedings of the 1st annual conference on Information security curriculum development. (2004).
8. Vaughn, Rayford B., David A. Dampier, and Merrill B. Warkentin. "Building an information security education program." Proceedings of the 1st annual conference on Information security curriculum development. (2004).
9. Azadegan, Shiva, et al. "An undergraduate track in computer security." Proceedings of the 8th Annual Conference on innovation and Technology in Computer Science Education. (2003).
10. Chickering, Arthur W., and Zelda F. Gamson. "Seven principles for good practice in undergraduate education." AAHE Bulletin 3 (1987).
11. McAndrew, Alasdair. "Teaching cryptography with open-source software." ACM SIGCSE Bulletin 40.1 325-329 (2008).
12. Younis, Younis A., et al. "Teaching Cryptography Using CYPHER (InteraCtive CrYPtograpHic Protocol TEaching and LeaRning)." Proceedings of the 6th International Conference on Engineering & MIS. (2020).
13. González-Tablas, Ana I., and Pablo Martín-González. "Student-Generated Videos for Promoting Better Attitudes Towards Cryptography." Proceedings of the 50th ACM Technical Symposium on Computer Science Education. (2019).
14. Schweitzer, Dino, and Wayne Brown. "Interactive visualization for the active learning classroom." Proceedings of the 38th SIGCSE technical symposium on Computer science education. (2007).
15. Schweitzer, Dino, and Wayne Brown. "Using visualization to teach security." Journal of Computing Sciences in Colleges 24.5 143-150 (2009).
16. Abdelhamid, Sherif, and Tristen Stower. Use of Online Educational Videos for Concept Oriented Peer-Based Learning. Filodiritto Editore, 11th International Conference New Perspectives in Science Education, pp. 155–160 (2022).