Enhancing Cryptography Education Using Collaborative Visual Programming

Sherif Abdelhamid, Sarah Patterson, Blain Patterson

Virginia Military Institute

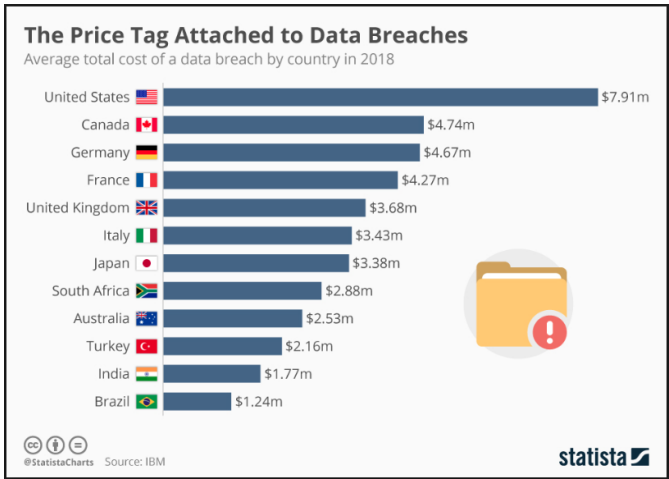
abdelhamidse@vmi.edu, pattersonse@vmi.edu, pattersonba@vmi.edu

Overview

- 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.
- Protection of data has become increasingly more important than before.

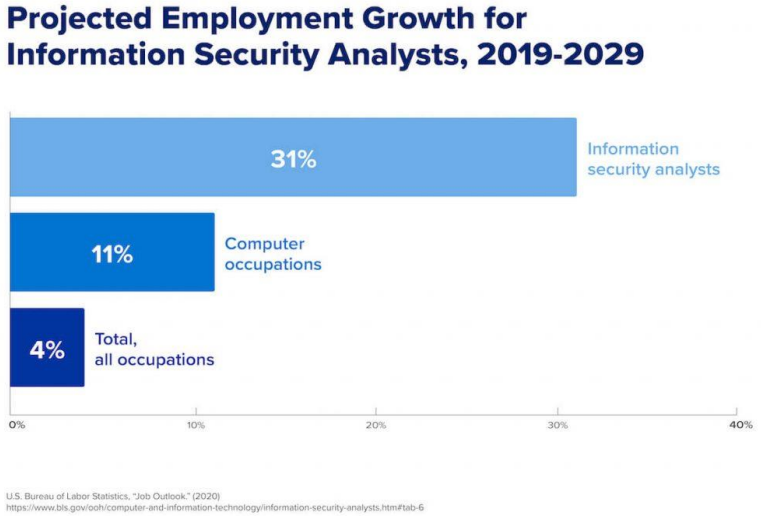
Problem

- Hackers are **getting more skilled** than before to exploit existing vulnerabilities and attack these websites.
- According to the Identity Theft Resource Center's (ITRC) data breach analysis, **there were 1,291 data breaches through September 2021**. This number indicates a **17% increase** in data breaches in comparison to breaches in 2020, which was 1,108.



Solution

- It is important to introduce the science of cryptography to future generations, at a younger age, in straightforward and more engaging ways.

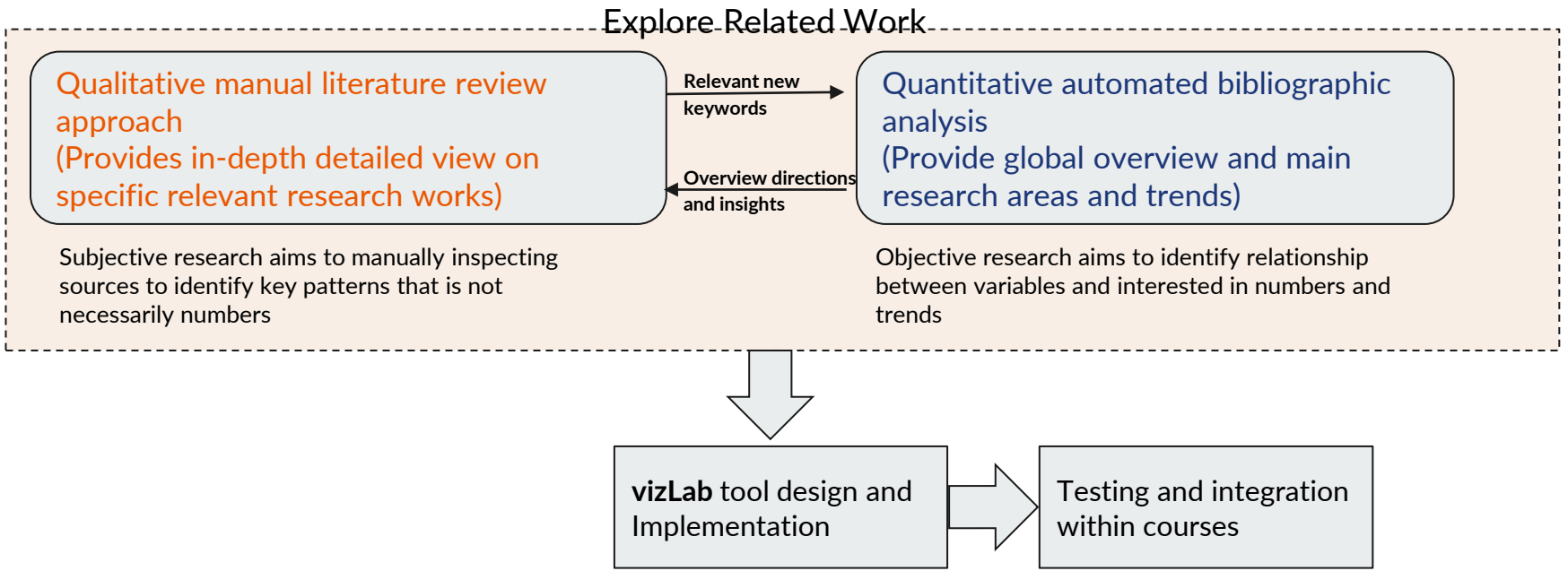


Challenges

- 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 engineering, testing and big data analysis.
- learners need to think in an organized and procedural way about the problems they are attempting to solve .

These requirements might create a barrier for students and scientists to develop and implement novel encryption algorithms or enhance existing ones.

Methodology



Literature Review

- Integrate security concepts into existing courses
- Create separate security coursework or programs and concentrations
- Implementing active learning techniques
- Use of real-world scenarios
- Algorithm illustration with animations
- Use of interactive visualizations
- Building intelligent tutoring systems

Bibliographic Analysis

- Conducted bibliometric analysis to identify research themes and explore the academic landscapes related to cryptography education.
- Collected ~10k publications from Crossref database, a not-for-profit association of publishers, including both commercial and not-for-profit organizations.
- From the retrieved publications, we key 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.

Bibliographic Analysis

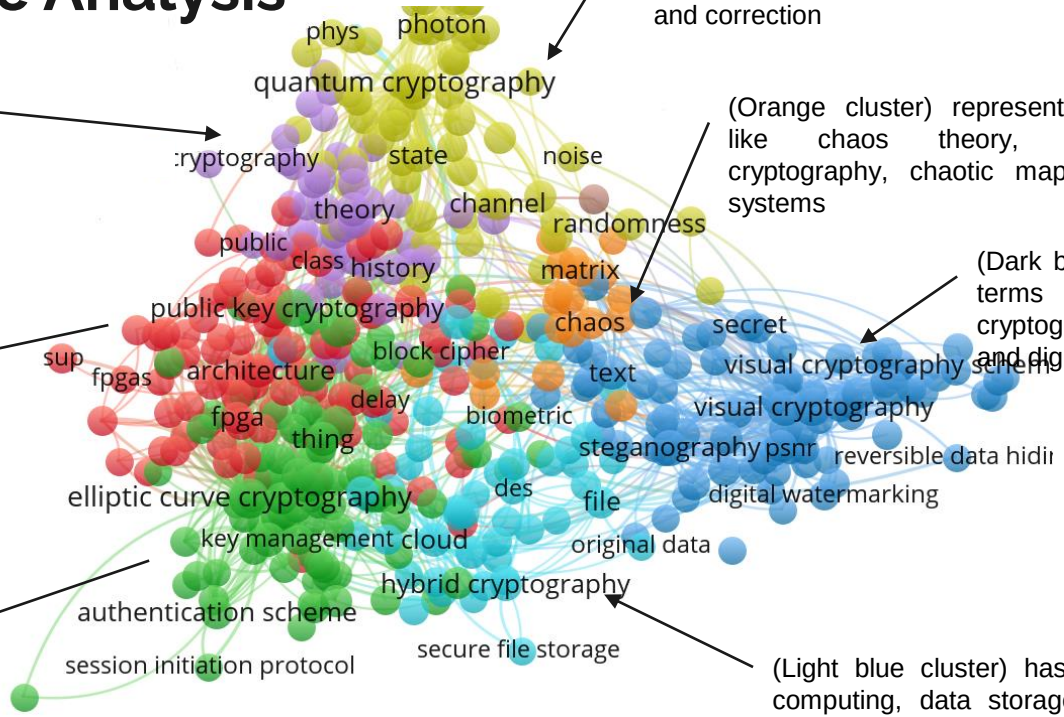
(Yellow cluster) is related to quantum cryptography, quantum physics, quantum mechanics, quantum communications, and error detection and correction

(Purple cluster) consists of key terms like students, courses, and teaching cryptography

(Orange cluster) represent topics like chaos theory, chaotic cryptography, chaotic maps, and systems

(Dark blue cluster) contains key terms related to visual cryptography, steganography, and digital watermarking

(Red cluster) contains key terms related to public-key cryptography, hardware, FPGA, and energy consumption.



(Green cluster) represent research relevant to elliptic curve cryptography, wireless sensor networks, smart grids, and vehicular ad hoc networks

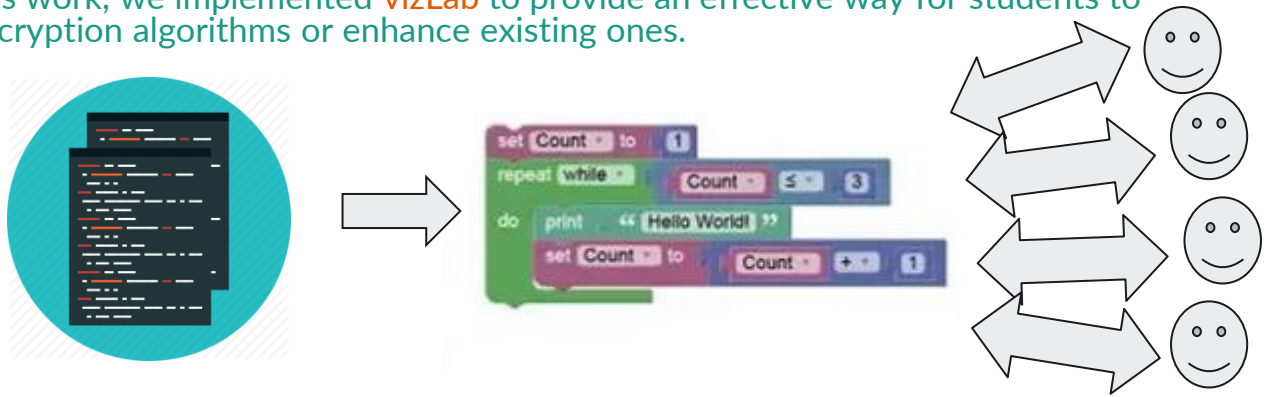
(Light blue cluster) has terms related to cloud computing, data storage, secure data transfer, data privacy, and management

Outcome

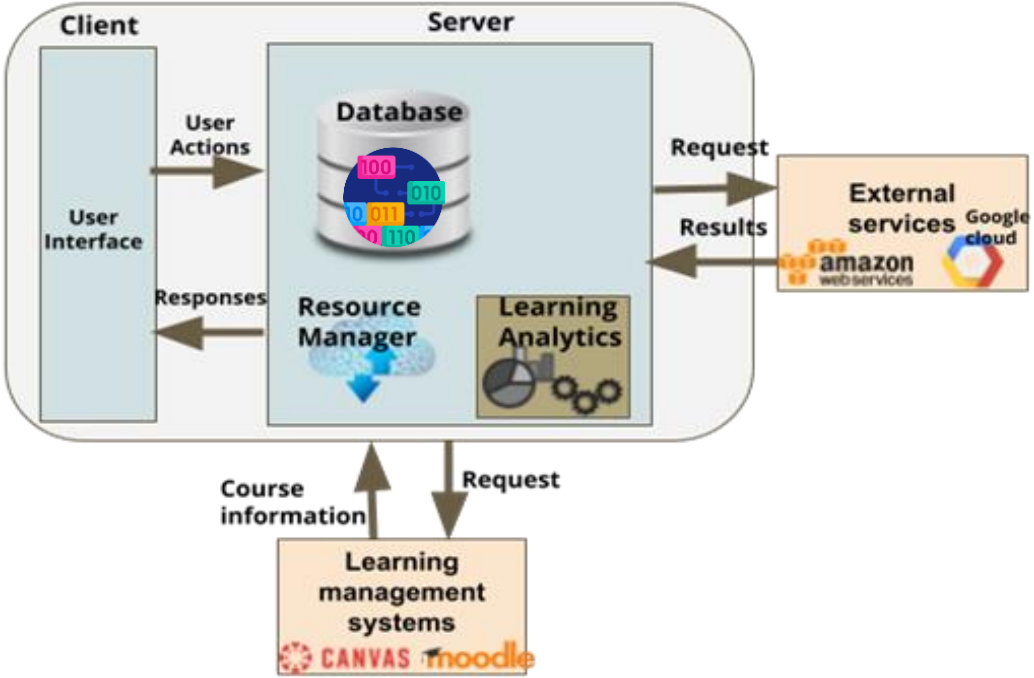
Few studies within cryptography education have considered the programming challenges during cryptography algorithm implementation.

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.

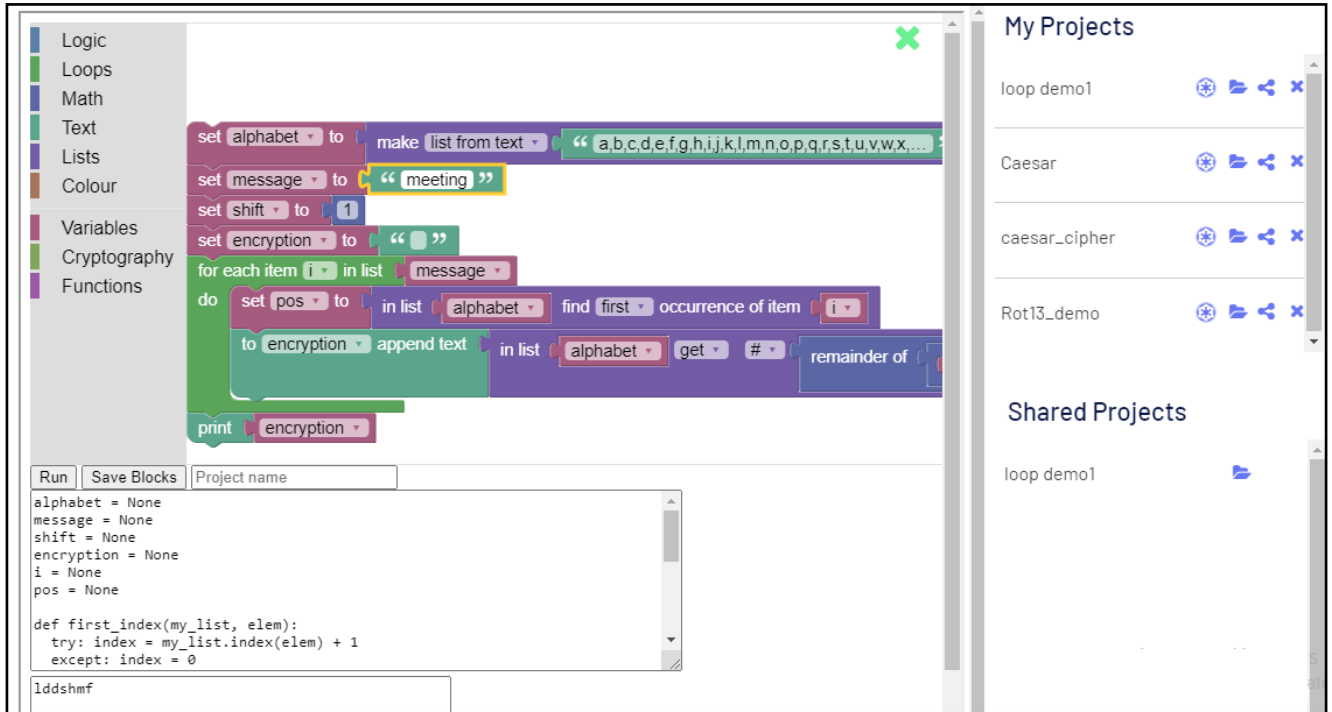
As a response, in this work, we implemented vizLab to provide an effective way for students to implement novel encryption algorithms or enhance existing ones.



System Overview

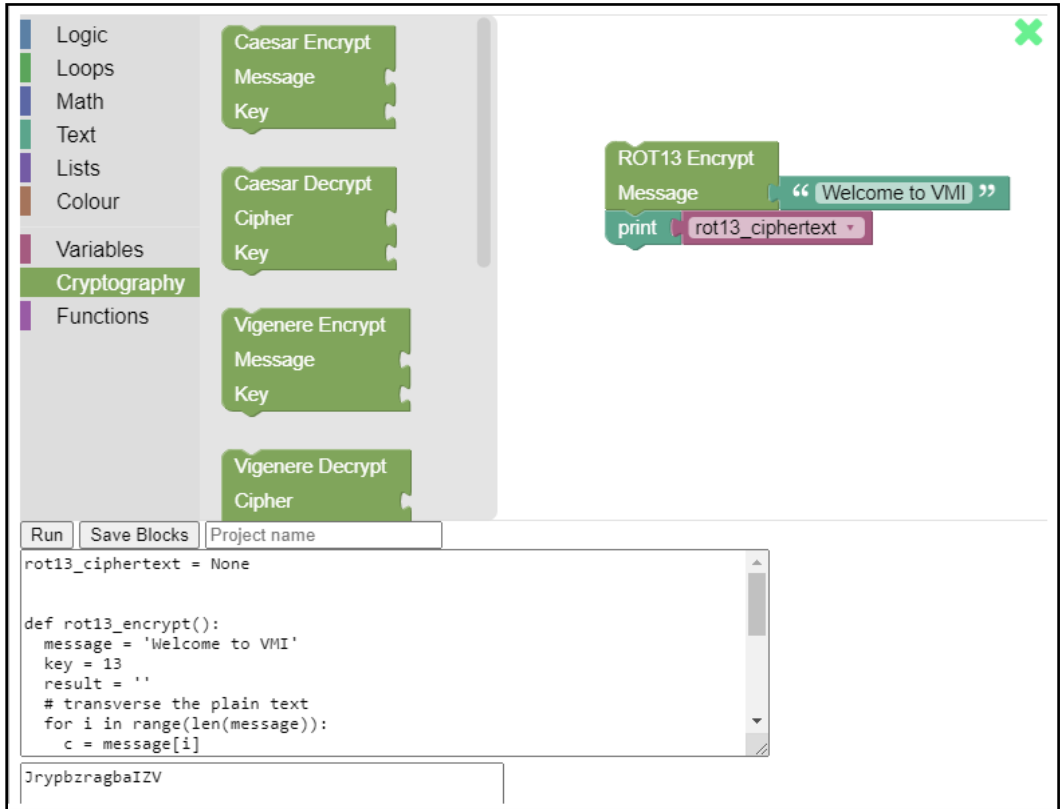


System Overview



System Overview

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



Conclusion

In this research work, we presented **vizLab**, a web-based programming learning tool that helps students avoid the programming challenges during cryptography algorithm implementation. vizLab promotes collaborative learning and engagement.

Our future work will involve integrating vizLab into an undergraduate course(s).

In addition, we will collect and analyze data about students' conceptual understanding and their ability to construct cryptography algorithms using surveys and more class observations.

Questions Please...