ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #37967

Introducing Cybersecurity in a Discrete Structures Course Through a Visualization-based Plug-and-Play Cryptography Module

Jyothirmai Kothakapu

Ahmad Y Javaid (Dr.)

Ahmad Y. Javaid received his B.Tech. (Hons.) Degree in Computer Engineering from Aligarh Muslim University, India in 2008. He received his Ph.D. degree from The University of Toledo in 2015 along with the prestigious University Fellowship Award. Previously, he worked for two years as a Scientist Fellow in the Ministry of Science & Technology, Government of India. He joined the EECS Department as an Assistant Professor in Fall 2015 and is the founding director of the Paul A. Hotmer Cybersecurity and Teaming Research (CSTAR) lab. Currently, he is an Associate Professor in the same department. His research expertise focuses on application of computational intelligence to various computing domains including but not limited to education, cybersecurity, healthcare, human-machine teaming, and digital forensics. His projects have been funded by various agencies including the NSF (National Science Foundation), AFRL (Air Force Research Lab), NASA-JPL, Department of Energy, and the State of Ohio.

Quamar Niyaz

Quamar Niyaz received the B.S. and M.S. degrees in computer science and engineering from Aligarh Muslim University, in 2009 and 2013, respectively, and the Ph.D. degree from The University of Toledo, in 2017. He has been an Assistant Professor in computer engineering with the ECE Department, Purdue University Northwest, since 2017. He has published papers in the areas of computer and networks security, applied machine learning, and cybersecurity education. His research has been sponsored by the National Science Foundation.

Charlene M Czerniak

Introducing Cybersecurity in a Discrete Structures Course Through a Visualization-based Plug-and-Play Cryptography Module

1. Abstract

With the advancement in technology and the rapid increase in Internet usage through smart devices, users are increasingly exposed to cyber-crimes. Due to the limited training on cybersecurity and cyber-safe practices, young adults are especially an easy target for these cybercrimes. It is also well-known that there is a need to enhance organizations' cybersecurity capabilities while spreading cybersecurity awareness among the masses. To the former cause, degree programs have been established throughout the US to train the workforce; however, they have proved insufficient. Therefore, we propose developing and integrating plug-and-play modules for CS/CSE undergraduate courses at various levels to develop a security mindset among these students and inculcate interest in a cybersecurity career. Irrespective of what domain of CS/CSE the students decide to pursue as a career, these modules would attempt to teach cybersecurity throughout an existing CS/CSE program. This paper presents one such module in the form of a visualization tool that describes cryptography and its basics for a sophomore discrete mathematics course. Specifically, the tool demonstrates the mathematical foundations of cryptography, the implementation of the RSA algorithm, and a real-world scenario to showcase the utility of encryption. Related results demonstrating the efficacy of the tool are presented.

2. Introduction

In recent years, the advancement of technology has led to people spending more time on the Internet. Even though there are benefits of using the Internet, such as online transactions and knowledge sharing, mishaps always happen. As more people depend on online services, they become more exposed to these cyber-attacks. Due to the global COVID-19 pandemic, we have seen a record-breaking number of data breaches and cyber-crimes, mainly targeting individuals, corporate industries, and government organizations. On average, every minute $2.9 million is lost to a cybercrime [1], and every 32 seconds, a hacker targets a user over the Internet [2]. According to the Identity Theft Resource Center, a total of 163 million identities were exposed in 2020 [3], and around 790k Internet crime complaints were received by the Internet Crime Complaint Center (IC3) [4].

Cybercrimes are on the rise, and it can be safely assumed that they will only worsen as technology penetration increases and the human resources available to combat these crimes stay relatively stagnant. The significant cybersecurity workforce shortage throughout the world is well-known [5]. According to (ISC)2's 2020 Cybersecurity Workforce Study, there will be a need for 3.12 million cybersecurity professionals by 2021 due to the national cybersecurity skill gap in the US [6]. There have been several attempts to address this shortage in the long term by creating cybersecurity education degree programs [7, 8, 9]. However, there is an increasing need to educate individuals at various levels, including high schools, colleges, and universities. Creating new degree programs is not always feasible or accessible at the university level. Therefore, incorporating security-related concepts in the existing computer science (CS) or computer science and engineering (CSE) curriculum might be a viable and sustainable solution so that students can start considering security as a prerequisite before designing any system. It will also encourage students to pursue their careers in the cybersecurity field by reducing the cybersecurity workforce gap [10]. Nonetheless, students will develop a cybersecurity mindset and get trained in this area

throughout their undergraduate degree program. Hence, cybersecurity practices would become a new norm in all CS/CSE-related areas.

Cybersecurity is a highly hands-on field, and it is crucial to train and motivate students through real-world, practical hands-on experiments using various tools and techniques. In addition, students must learn the development of cyber-secure applications and strategies and understand safe online behavior. Using such teaching tools and mechanisms in various courses can be accomplished at multiple levels of undergraduate education without turning the existing course delivery method and schedule upside-down. With this motivation, we propose using interactive, hands-on modules that can be easily incorporated or integrated into existing courses offered in CS/CSE programs. Using these modules, students can quickly learn topic-specific cyber-safe practices in several CS/CSE domains and develop a security mindset so that security doesn't come as an afterthought. Several of these modules may use user–friendly graphical interactions and various scenarios to teach undergraduate students about cybersecurity. As these are plug-and-play modules, instructors may use them without modifying the existing course delivery and schedule. This paper discusses a Unity-based interactive cryptography module developed for a Discrete Structure course. This tool helps students understand the number-theoretical foundations of the RSA algorithm, the implementation of the RSA algorithm, and a real-world scenario to showcase the utility of this encryption technique. Such frameworks have proved to work for the younger high school student population. This also motivated us to undertake this work and test its efficacy for an undergraduate student population [11].

The rest of the paper is organized as follows. In Section 3, we present a summary of the related works of cybersecurity education. Section 4 discusses the application design of the visualization framework. Section 5 discusses the cryptography basics and RSA Algorithm visualization implementation using Unity 3D. Section 6, evaluates and analyzes the survey results of 42 students. Finally, we conclude the paper in Section 7.

3. Related Work

Research indicates that students recall only 10% of what they read, 20% of what they hear, and 50% of what they remember if someone does something while explaining it to them, but they can remember over 90% if they practice by themselves while learning [12]. The students in high school and college can have greater cognition if provided with an opportunity to actively participate in classroom activities that use their critical thinking and problem-solving skills [12]. As a result, there is a crucial need for innovative and creative teaching methodologies in the cybersecurity field to increase students' interest. Many cybersecurity education programs like CTF (Capture the Flag) competitions [13], Game-based learning methods [14] [15], and hands-on practice-oriented learning methods [16] have been implemented in the last few years to fill the skill gap between the future workforce and the constantly increasing demand for cybersecurity experts

Due to the COVID-19 pandemic, many educational institutes have begun to offer online education. As a result, smartphones and tablets as content-delivery platforms have increased rapidly. However, delivering online courses in an interactive-based visualization format that allows students to participate actively is challenging [17]. The most well-known game, 'CyberCIEGE' is one of the interactive visualization-based cybersecurity games [18]. It consists of a 3D office environment where the players act as IT decision-makers for small businesses. There will be several scenario-based challenges where the players must make security-related decisions that they may face in real life. The scenarios are designed based on the concepts of encryption, patches, and

DMZ. The CyberCIEGE game has been implemented in several security courses also. The Kennesaw State University has conducted a survey of security games built on Unity 3D and Unreal Engine for cybersecurity education and training. These interactive visualization-based games cover concepts related to Security Awareness, Cryptography, Secure Software Engineering, Network, and Web security. This survey is beneficial as lecturers can choose a fair game from the catalog to teach several cybersecurity concepts [14].

A group created a CTF tournament for undergraduate students to learn security concepts in a competitive environment. The CTF tournament is designed so that it covers all the security-related topics from the syllabus. This inspired instructors to design and develop new challenges and students enjoyed solving them to reinforce their skills [19]. Furthermore, by incorporating serious games into learning, we introduce the concept of interaction-based visualization into our framework, which actively engages students in learning security concepts. The developed tool will assist students in learning each topic through interactive visualization-based simulations. Besides, the tool includes quizzes after each topic to assess the student's grasp of that topic.

4. Application Design

We analyzed various software engines like Unreal Engine, Maya, Cinema 4D, and Godot to design and develop the visualization framework. Most of these are complicated and expensive to use compared to Unity Engine. Unity enables developers to create applications for any platform without requiring significant code changes. Unity 3D offers several tools that make it easy for any developer to work on their projects. We have developed our visualization tool on Windows/Mac/Linux environment and currently working on its export to the Android platform to make it compatible with smartphones. Unity allows developers to create a plug-and-play (standalone) application that can be used anywhere without any need for additional software. Therefore, Unity is the ideal platform for developing the visualization tool [20].

We have designed the application so that it is simple to use and navigate for any user. We have created the main menu, which will contain a sub-menu and an assessment based on the topics discussed. Fig. 1 and 2 show the menus and sub-menus of the visualization tool. The framework is designed in three stages for the users – (i) Basics, (ii) Discussion about the topic using a real-world example, and (iii) 3) Interaction. Each stage will have an assessment based on the topics discussed. These assessments are important for the learners as they can evaluate what they are learning.

The *Basics* stage will consist of a brief discussion about the topic and some fundamentals related to it. To grab the user's attention, we have an animated character with some basic motions which will entertain users while learning about the topic. We can keep the user entertained and learning with a few interactions while explaining the concepts [21]. In the second stage, *Discussions*, we have provided a detailed explanation of the topics, and this is the stage where the user will get a complete understanding of the topic. We used different anime characters with varied animations for each section to keep users actively engaged in learning. Interaction is the final stage, where the user has to solve an interactive task based on the topics discussed in the preceding stages. For every stage, we have a quiz of 5 questions, which will allow users to assess what they are learning.

5. Visualization-based Education Topics

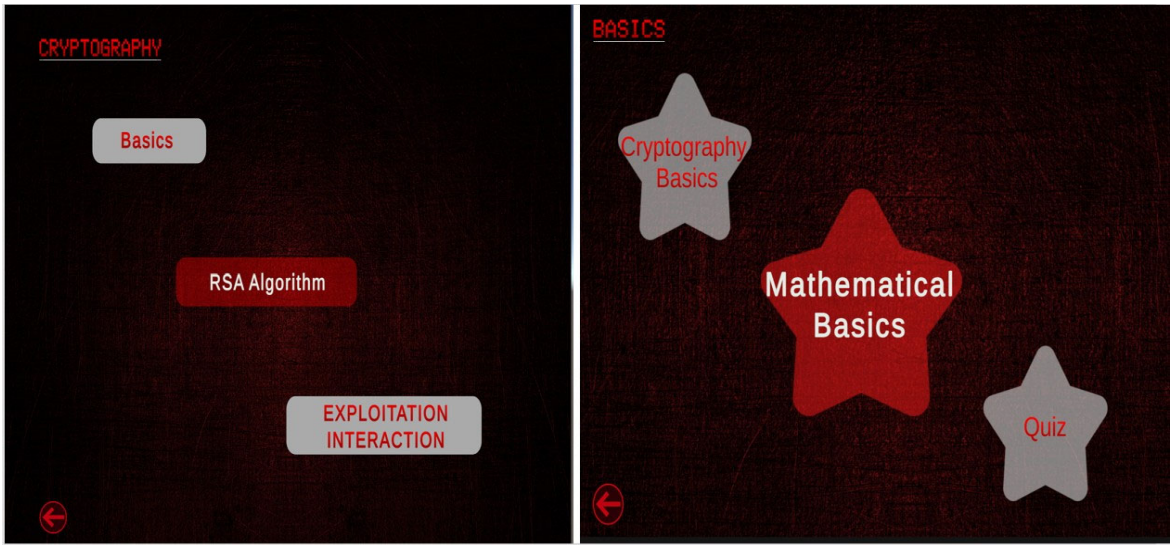

Fig. 1. Menu screens for topics and Basics section in the framework

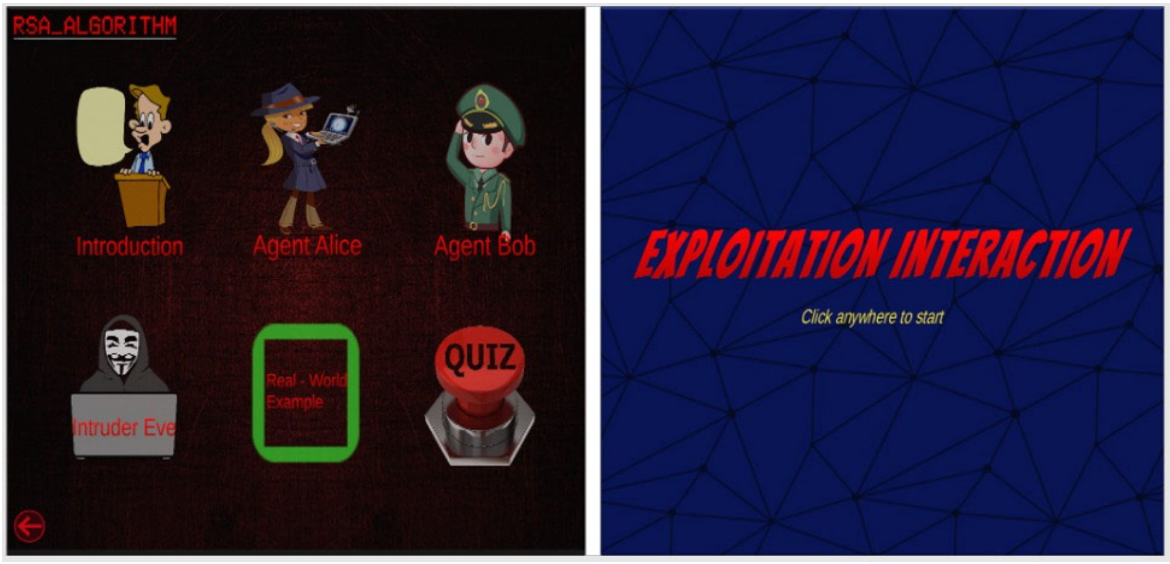

Fig. 2. Menu screens for RSA Algorithm section and Exploitation interaction section in the framework

The primary goals of this project are (i) to develop a security mindset at the undergraduate level, (ii) to introduce cyber-secure design and development practices from the early stages to minimize vulnerabilities during system design rather than the addition of security measures as an after-thought, and (iii) to inculcate interest among students in cybersecurity careers. We have developed an interactive visualization-based framework for undergraduate students to achieve these goals. The process of security topic selections is discussed in the following sections. To evaluate the framework's effectiveness, we conducted a pre- and post-survey before and after using the framework. The results of the surveys are discussed in Section 6.

Even though there is a wide range of topics in the cybersecurity domain, we have selected cryptography for our visualization framework development. In cryptography, we focused on RSA Algorithm. We choose RSA Algorithm because it perfectly aligns with the mathematical concepts

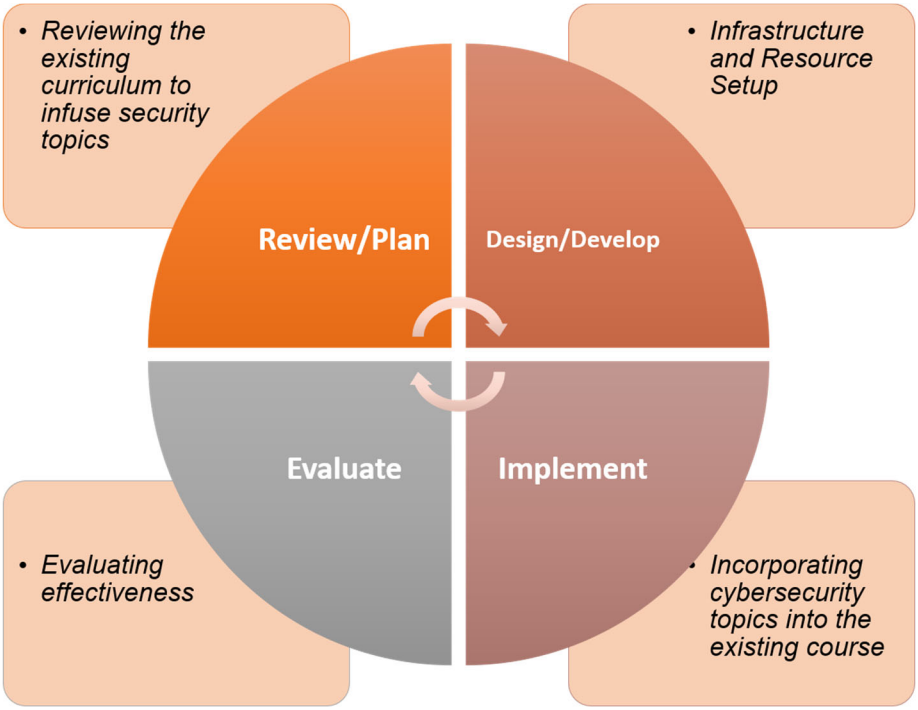

Fig. 3. Methodology used for the research

of the Discrete Structure course offered at various universities. The methodology used for this research is shown in Fig. 3.

5.1. RSA Algorithm Visualization

The RSA algorithm is a public key (asymmetric) cryptosystem that is based on Number theory and uses a block cipher system [22]. It uses two different keys to encrypt and decrypt the data. The algorithm's security is based on large numbers prime factorization, which is a well-known mathematical issue with no viable solution [23]. For the RSA algorithm visualization, we have considered the following questions:

- What is the RSA algorithm, and how does it work?
- How to make the RSA algorithm process easy to explain?
- How to visualize the implementation of the RSA Algorithm?

The above questions are answered in the developed framework. In the initial stage, we introduce the fundamentals of cryptography and its mathematical concepts. In the next stage, a detailed explanation of the RSA algorithm is provided, and in the last stage, we have an interaction module based on the RSA algorithm.

5.1.1. Cryptography Basics

For the introduction stage of RSA algorithm module visualization, we considered cryptography basics and mathematical basics related to Number theory. In the cryptography basics section, we explain basic terms like encryption, decryption, cryptography, and symmetric and asymmetric cryptography algorithms. In the mathematical basics section, we explain the fundamentals of

Modular Arithmetic, Euler's theorem, and Euler's totient functions. Fig. 4 shows the animated characters used in describing cryptography and fundamental mathematical illustrations.

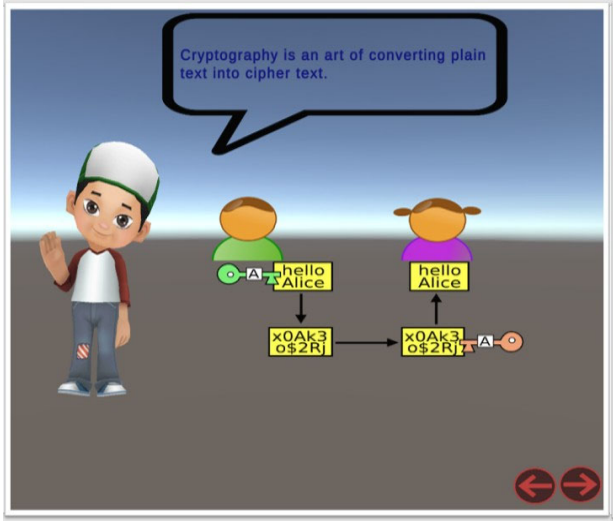

Fig. 4a. Cryptography Basics visualization

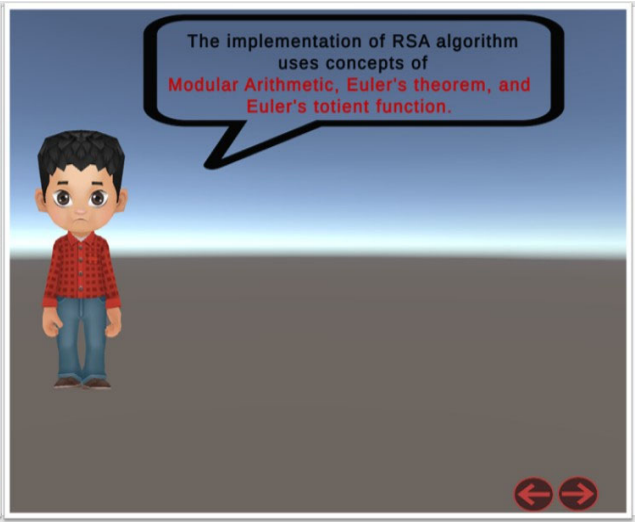

Fig. 4b. Mathematical Basics visualization

5.1.2. RSA Algorithm Module

For RSA algorithm visualization, we have six sub-sections in the framework. Each subsection is designed so that students can quickly learn about the usage and application of the RSA Algorithm. The description and functionality of each subsection are listed below:

- Introduction

Objective: The basic concepts related to the RSA Algorithm are shown in the illustration.

Explanation: The RSA algorithm's background information is covered in this section. We discuss the use of private and public keys in encrypting and decrypting the data.

- Agent Alice

Objective: Encrypting the messages using the RSA Algorithm.

Explanation: We used a story-driven visualization in the framework to make things more interesting. We have considered two soldiers, Agent Alice and Agent Bob, who work in the military. Agent Alice works as an undercover agent and is trying to send important information to Agent Bob. Here we show the process of how Agent Alice uses the RSA algorithm to encrypt the message. An example is shown in Fig. 5a.

- Agent Bob

Objective: Decrypting the messages using the RSA algorithm.

Explanation: The illustration shows a detailed systematic process of how Agent Bob decrypts the message using his private key. An example is shown in Fig. 5b.

- Intruder Eve

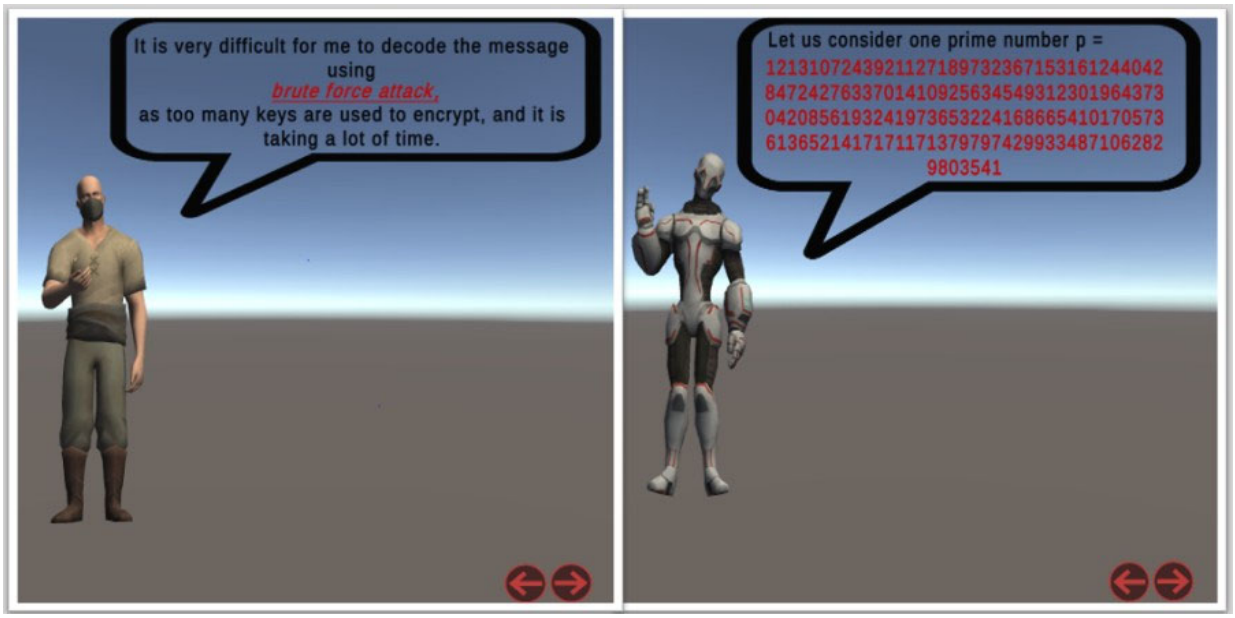

Fig. 5. Learning Modules, 5a. Agent Alice (left), 5b. Agent Bob (right)

Objective: Discusses the attacks that can be used for exploiting the RSA algorithm.

Explanation: While Agent Alice sends an encrypted message to Agent Bob, Agent Eve who is an intruder gets suspicious and tries to decode the message using various attacks like Brute force attack, Dictionary attack, Frequency analysis attacks. The process involved in using these attacks is also explained in the visualization framework. Fig 6a shows an example.

- Real-World Example

Objective: It demonstrates the working of the RSA Algorithm by using a real-life scenario.

Explanation: The illustration shows how hard it is to decode the RSA Algorithm if we use two large prime numbers for encrypting the message. It will also provide an example of how large prime numbers are employed in real-world scenarios. Fig 6b shows an example.

- Quiz

Objective: To evaluate the knowledge gained by the learners.

Explanation: The quiz consists of 5 multiple-choice questions. The questions are framed based on the information provided in the tool. The learners can take the quiz to evaluate their understanding of topics discussed in the previous sections of the framework.

5.1.3. Exploitation Interaction Module

We created an interactive exercise where users are provided with step-by-step instructions on how to encrypt and decrypt the messages. Then they must solve the problems based on their knowledge gained from the previous sections. This will provide an excellent hands-on experience to students where they can encrypt and decrypt the messages on their own using the RSA Algorithm. The

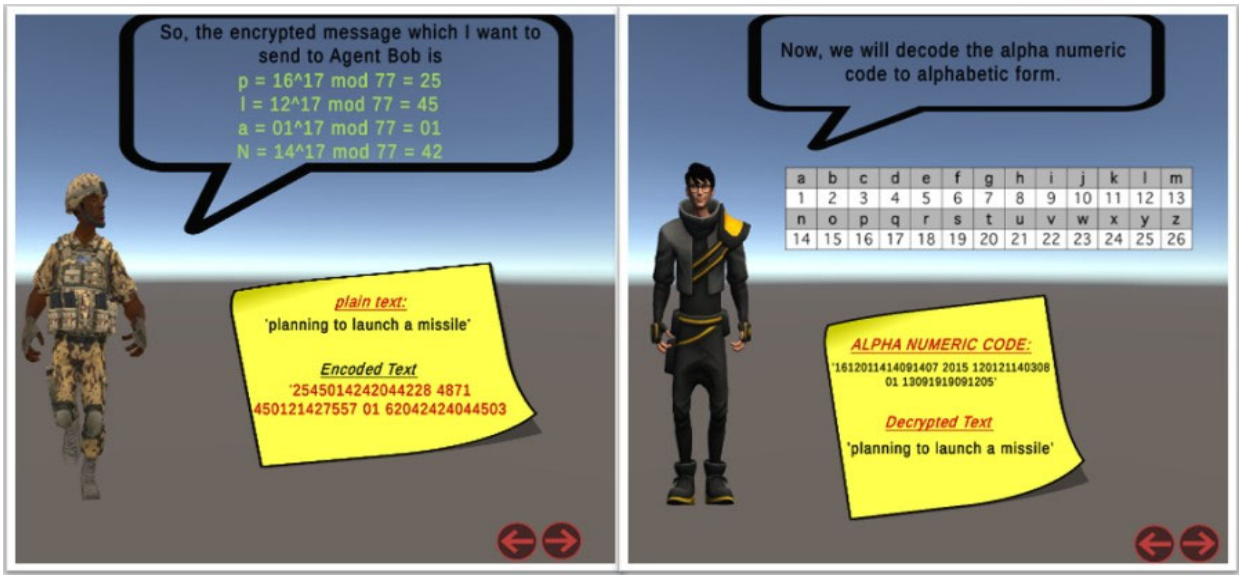

Fig. 6. Learning Modules: 6a. Intruder Eve (left), 6b. Real-world example (right)

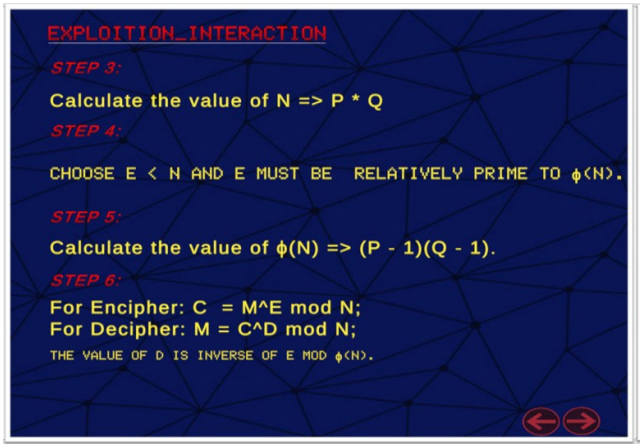

Fig. 7a. Exploitation Interaction modules, Instructions

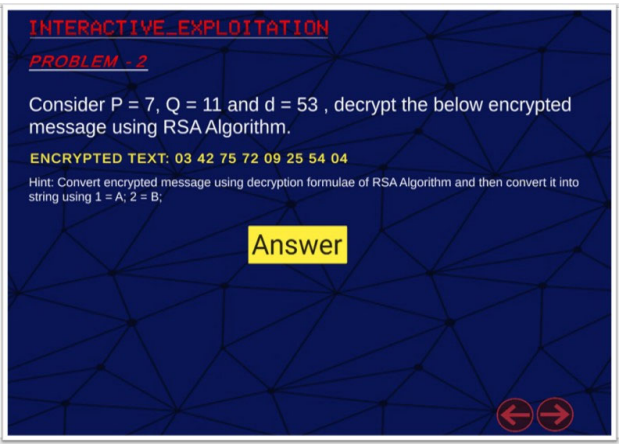

Fig. 7b. Exploitation Interaction modules, Exercise

interaction module consists of three exercises, one for decryption and two for encryption. Fig. 7 shows step-by-step instructions and how the exercises have been designed.

6. Results and Analysis

The module presented in section IV has been given to sophomore students at our University who took the course “Discrete Structure” offered in Spring 2021. Since the University offered online classes due to the COVID-19 pandemic restrictions, we have given the developed module tool to students through blackboard and asked them to explore it. We also provided end-to-end documentation about how to access and navigate the tool. Our goal is to make students learn security concepts using a practice-oriented module with graphical interactions. To evaluate the impact of this visualized framework module, we have created pre and post-surveys to go along with the developed framework. First, we offered all the 42 students pre-surveys as class assignments, and then we provided them the developed framework to explore and then followed by post-surveys.

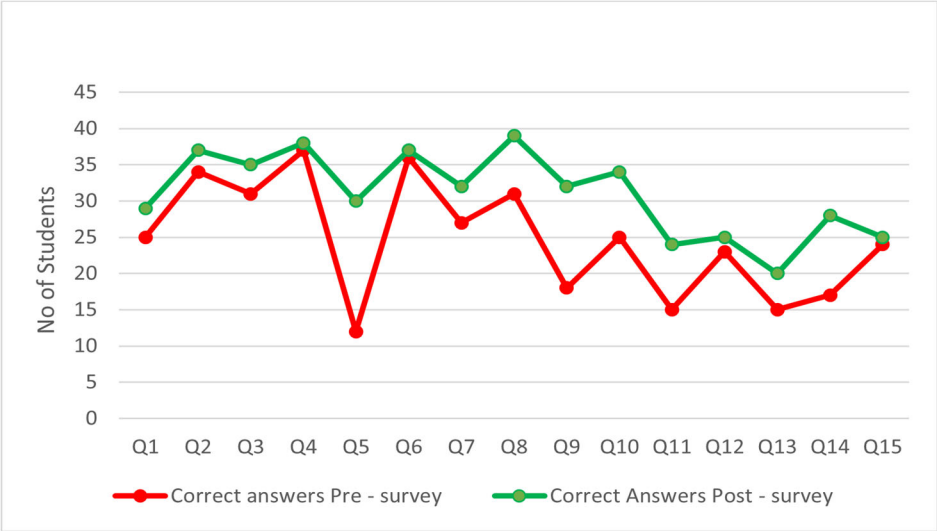

Fig. 10. pre and post survey results of the hands-on module

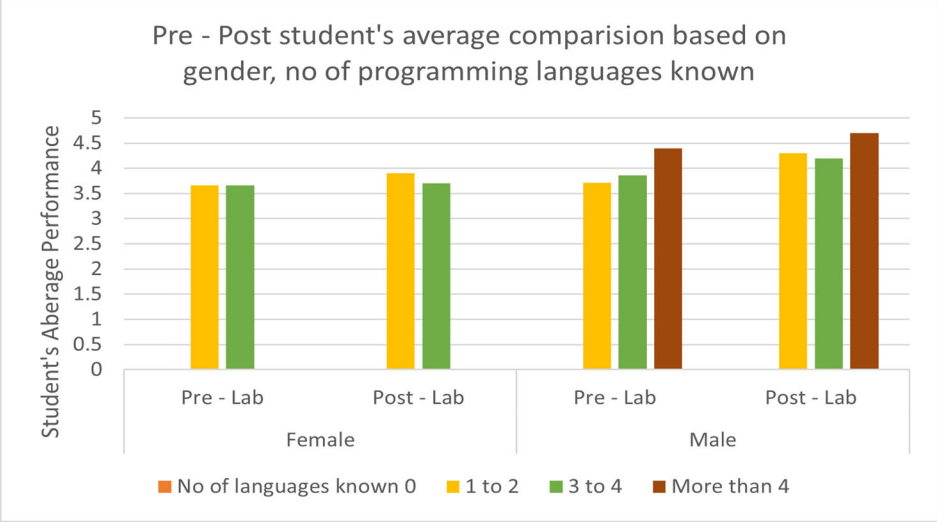

Fig. 11. Pre- and post-survey results of the hands-on module

We conducted a total of 4 surveys, 2 pre–surveys and 2 post-surveys based on general cybersecurity awareness and on the developed hands-on framework. The questions posed in the hands-on framework survey are presented in Table I. It should be noted that the questions in this set of 15 questions were multiple choice with only one correct answer. A graphical representation of the percent of correct and wrong answers given by students in the pre- and post-module-based survey is shown in Fig. 10. A positive outcome is observed from the results of the survey after using interactive visualization hands-on framework.

The student's general cybersecurity knowledge was also assessed using a 5- point Likert scale. The options were 5 (Strongly Agree), 4 (Agree), 3 (Neither Agree nor Disagree), 2 (Disagree), and 1 (Strongly Disagree). Depending on the questions, the answers were graded on a scale of 1 to 5, with 5 being the correct answer, 4 – partially correct answer, 3 – neither correct nor wrong answer, 2 – partially wrong answer, and 1 – wrong answer. The survey results have shown that interactive visualization-based learning has improved students' knowledge of cybersecurity principles and

motivated them to pursue their careers in the cybersecurity field. This second survey had 43 questions and consisted of 37 cybersecurity questions and 6 demographics-related questions. We have further analyzed the data based on gender and the number of programming languages known. The results are shown in Fig. 11. We have observed a positive impact on both genders even though males have more computer knowledge than females.

Table 1. Survey Questions

Q1	What kind of cipher is a Caesar Cipher?
Q2	Encryption is when you get ciphertext and turn it into plaintext
Q3	What is needed to read encrypted messages?
Q4	What is Cryptography used for?
Q5	In RSA Algorithm, we select 2 random large numbers 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
Q6	What text is the scrambled and unreadable output of encryption?
Q7	In which type of encryption is the same key used to encrypt and decrypt data?
Q8	Which of the following asymmetric cryptography algorithms is most commonly used?
Q9	In the RSA algorithm, (n) = ? in terms of p and q.
Q10	RSA is named after the researchers (a, b, c) who proposed it?
Q11	Bob received an encrypted message sent to him from Alice. Which key should he use to decrypt the message?
Q12	Using p=3, q=13, d=7 in the RSA Algorithm, what is the value of Plaintext for a Cipher Text 8?
Q13	For p = 11 and q = 17 and choose e = 7. Apply RSA algorithm where PT message = 88 and thus find the CT?
Q14	For RSA Algorithm to work, the value of 'P' must be less than what value?
Q15	How can you break an encrypted code into plain understandable text without knowing the shift?

7. Conclusion

As the number of people using the Internet keeps rising, users must be aware of the cyber-attacks they may face while browsing the websites. The main goal of this project is to spread cyber-awareness by developing a security mindset among the students at the undergraduate level. In this paper, we have developed an interactive plug-and-play framework with hands-on experience using real-world scenarios for the Discrete Structure course offered at our University. This interactive module will increase the student's interest in learning cybersecurity principles. This approach will benefit the future workforce as students build expertise in the cybersecurity field. The module is well received by students, as indicated by post-survey results. Based on the student's feedback, we plan to enhance further and create a mobile-compatible version of the framework.

References

1. Morgan Steve. Cybercrime to cost the world $10.5 trillion annually by 2025, Nov 2020.
2. Lazic Marija. Hackers attack every 39 seconds, January 2021.
3. Identity theft resource center sees data compromises drop 33 percent in the first half of 2020, Jul 2020.
4. FBI releases the internet crime complaint center 2020 internet crime report, including covid-19 scam statistics, Mar 2021.
5. Rebecca Vogel. Closing the cybersecurity skills gap. Salus Journal, 4(2):32–46, 2016.
6. Cybersecurity professionals stand up to a pandemic, 2021.
7. Djedjiga Mouheb, Sohail Abbas, and Madjid Merabti. Cybersecurity curriculum design: A survey. In Transactions on Edutainment XV, pages 93–107. Springer, 2019.
8. Melissa Dark and Jelena Mirkovic. Evaluation theory and practice applied to cybersecurity education. IEEE Security & Privacy, 13(2):75–80, 2015.
9. Trudy Howles, Carol Romanowski, Sumita Mishra, and Rajendra K Raj. A holistic, modular approach to infuse cybersecurity into undergraduate computing degree programs. In Annual Symposium On Information Assurance (ASIA), Albany, NY, pages 7–8. Citeseer, 2011.
10. William Crumpler and James A Lewis. The cybersecurity workforce gap. JSTOR, 2019.

11. Laxmi M Podila, Jyothi P Bandreddi, Javier I Campos, Quamar Niyaz, Xiaoli Yang, Anastasia Trekles, Charlene Czerniak, and Ahmad Y Javaid. Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students. In 2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), pages 303–310. IEEE, 2020.
12. [12] Michael Findley. The relationship between student learning styles and motivation during educational video gameplay. IJOPCD, 1:63–73, 07 2011.
13. C Li and R Kulkarni. Cybersecurity education through gamification. In American Society for Engineering Education 123rd Annual conference and exposition, 2016.
14. Winston Anthony Hill Jr, Mesafint Fanuel, Xiaohong Yuan, Jinghua Zhang, and Sajad Sajad. A survey of serious games for cybersecurity education and training. 2020.
15. Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Game-based cybersecurity training for high school students. pages 68–73, 02 2018.
16. Brent Wilson. Teaching security defense through web-based hacking at the undergraduate level. 2017.
17. Markus Krause and Joseph Williams. A playful game-changer: Fostering student retention in online education with social gamification. 03 2015.
18. C.E. Irvine, M.F. Thompson, and K. Allen. Cybercrime: gaming for information assurance. IEEE Security Privacy, 3(3):61–64, 2005.
19. Hugo Gonzalez, Rafael Llamas-Contreras, and Omar Montano. Using a CTF tournament for reinforcing learned skills in cybersecurity course. Research in Computing Science, 148:133–141, 12 2019.
20. Unity. (2020) Unity scenes. [Online]. Available: https://docs.unity3d.com/Manual/CreatingScenes.html
21. Lorena Blasco-Arcas, Isabel Buil, Blanca Hernandez-Ortega, and F Javier Sese. Using clickers in class. the role of interactivity, active collaborative learning, and engagement in learning performance. Computers & Education, 62:102–110, 2013.
22. RSA (cryptosystem), Jul 2021.
23. Xin Zhou and Xiaofei Tang. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th International Forum on Strategic Technology, volume 2, pages 1118–1121, 2011