The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #41434

A Novel Scavenger Hunt Activity for Increasing Student Engagement in Cryptography Coursework

Dr. Heena Rathore, Texas State University
Dr. Henry Griffith, San Antonio College

A Novel Scavenger Hunt Activity for Increasing Student Engagement in Cryptography Coursework

Heena Rathore
heena.rathore@txstate.edu
Computer Science Department
Texas State University

Henry Griffith
hgriffith5@alamo.edu
Department of Math and Engineering
San Antonio College

Abstract

As the realm of cybersecurity grows increasingly critical, imparting the knowledge of computer system security particularly cryptography to students is paramount. This paper presents an innovative approach to this endeavor through the integration of scavenger hunt, uniquely tailored to transcend the boundaries of traditional teaching. Unlike conventional methods which are predominantly introduced during high school or incorporate a single intricate puzzle for participants to solve, this paper emphasizes practical application over theory, improving the way students grasp complex concepts and retain them. In this work, students collaborated in groups to engage in an "Capture the Flag" style scavenger hunt, conducted through the platform of Google Earth. Throughout the activity, they were actively encouraged to leverage a wide array of online tools, encompassing resources such as usage of large language models such as ChatGPT and various others, to collaboratively solve the questions. During the exercise, students encountered encrypted messages at various stages and to progress in the activity had to apply cryptographic principles to decipher these messages. The proposed practical application of cryptography involved tasks like decrypting codes, solving puzzles, or using ciphers to reveal clues led them closer to the final challenge. By introducing scavenger hunt at the intersection of computer system security education, we open a gateway to experiential learning that is engaging, interactive, and fun. This approach was also compared with a research-centric group project that delved into establishing secure methods for cyber-physical systems. The study indicates that a majority of students (77.4%) viewed the Capture the Flag Scavenger Hunt as a highly valuable learning experience.

1 Introduction

Studying computer security is crucial in today's interconnected digital landscape to safeguard sensitive information, preserve privacy, and ensure the reliable functioning of computer systems[1]. An undergraduate (UG) course in computer security typically includes topics such as network security, operating system security, cryptography, software security[2]. Cryptography, a fundamental pillar

of computer system security, plays a pivotal role by providing techniques to secure data through encryption and decryption processes[3]. It enables secure communication, authentication, and data integrity verification, thwarting unauthorized access, data breaches, and cyberattacks. Mastery of cryptography empowers professionals to design robust security protocols and build resilient systems that can withstand the evolving challenges of the digital age[4].

Math is highly integral to cryptography, as it provides the theoretical foundations for understanding the complexity and security of cryptographic algorithms [5],[6]. Concepts from number theory, abstract algebra, probability, and computational complexity form the basis of cryptographic methods[7]. While the mathematical underpinnings can pose challenges for some students, they are essential for grasping the intricacies of cryptographic algorithms and ensuring their effectiveness. Students may struggle with the mathematical aspects, but a solid understanding of these foundations is critical for developing secure and reliable cryptographic systems. Facilitating the motivation and enthusiasm for students lacking technical expertise and engagement to study poses a significant challenge to educators.

Recently, gamification has emerged as a promising approach to incentivize students by integrating various game-based techniques into educational modules. In this regard, capture the flag (CTF) competitions[9] have been found to be an effective means of introducing students to diverse technical concepts inherent in the conventional computer science curriculum[8]. By making cryptography fun and engaging[10], we can help students develop a deeper understanding and appreciation for this important field of study. Having CTF activity can foster continuity in skill development, emphasizing how increased engagement could motivate students to devote the additional time necessary to develop requisite math skills, thereby enhancing continuity in their learning journey.

This paper describes recent efforts to integrate a scavenger hunt activity within the Computer System Security course at Texas State University during the Spring and Fall 2023 semester. Computer security course is required for all UG CS majors, and is also taken by a significant number of graduate students under a cross-listed course. A group-based experiential learning experience was utilized and compared with semester long group projects. For experiential learning, students had to compete with each other to solve several cryptographic challenges. Details regarding the logistics of the implementations and lessons learned for future implementations are described herein.

2 Related Work

There are multiple avenues for integrating experiential learning into the curriculum, one of which is fostering group collaboration among students. While various studies have highlighted the significance of group projects[11],[12] a more specific and less explored approach involves incorporating activities like CTF challenges and scavenger hunts. It was found in one study[23] that students' self-confidence would improve through participation in a CTF activity as compared to techniques in a controlled environment. It bolstered students' confidence in executing, recognizing, and defending against attacks[23]. The CTF participation enhances practical skills, separating knowledge-based and skill-based CTF exercises could yield improved outcomes. In this section, we delve into existing research that explores and incorporates active learning through scavenger hunt-style activities, shedding light on their effectiveness in promoting teamwork and collaboration within educational settings.

Cryptography, the practice of sending secretive messages, is a dynamically evolving field explored by mathematicians and computer scientists. This discipline holds increasing significance in contemporary society, with applications encompassing Internet security, diplomatic confidentiality, and historical contexts. In this respect, Idaho National Laborartory (INL)[13] created a scavenger hunt where the students had to solve a single cryptographic puzzle with suduko. The puzzles were modified with letters A through I, corresponding to numbers 1 through 9, and these letters were randomly assigned to the numbers. The coordinates of a geocache were given using these letters. When students solve the puzzle, they decipher the coordinates and had to replace the letters with numbers to find the hidden treasure. Additionally, an alternative encryption approach involved Secret Decoder Wheel created by INL, where letters were matched with symbols, allowing for encoding messages to describe the treasure locations in symbols for students to decode and find.

Similarly, in[14] was developed exclusively for grades third to eight where the students had to solve Caesar shift encryption algorithm. The author designed a worksheet and organized a scavenger hunt for an all-girls STEM-careers camp, catering to ages 6-12. They facilitated the completion of the worksheet collectively and split the participants into two age-based groups for the scavenger hunt. The author reflects that the activity effectively introduces children to the concept of cryptography and highlights that some of the campers showed significant enthusiasm, expressing a desire to delve deeper into the subject to enhance their skills.

In[15], the authors introduce a mathematical scavenger hunt meticulously crafted to engage and enthuse students who are studying RSA cryptography in an initial number theory class. The hunt revolves around the RSA cryptosystem, leveraging Maple[16] for the encryption and decryption of concealed data embedded within the provided hints.

The cyber discovery camp particularly focused on Stem summer camps high schoolers was proposed in[17]. The camp, involving engineering, science, and liberal arts faculties, aimed to highlight the positive and negative aspects of cyberspace, making participants more conscious of cybersecurity and its implications. This residential program exposed high school students and teachers to diverse cyberspace subjects, including history, ethics, applications, and security, through discussions, hands-on labs, activities like a cryptographic treasure hunt, film sessions, and a final cyber challenge. The 2008 camp, hosted by the College of Engineering and Science in collaboration with the College of Liberal Arts, engaged 30 students and 10 teachers, offering a comprehensive learning experience.

University of Illinois at Chicago, "Treasure Hunt" is an interactive educational game designed for middle-grade children, centered around the utilization of cryptography[18]. The game's objective is to discover a concealed treasure within an ancient castle. To advance in the narrative, players must decrypt messages using mathematical abilities. The game blends amusement and mental engagement for students, introducing them to pertinent concepts while satisfying their curiosity for secret codes.

The current work in this domain is either limited to high schoolers or hosting scavenger hunt focussed only on one or two concepts in cryptography. The proposed CTF hosted on Google Earth represents a more dynamic and immersive approach to experiential learning when compared to the existing state of the art techniques in following ways:

- *Teamwork and collaboration*: Cryptographic puzzles can be challenging, and students often benefit from working together to solve them. The scavenger hunt format encourages collaboration and teamwork, which are essential skills many other fields.
- *Geographical Awareness*: Google Earth adds an interesting geographical dimension to the scavenger hunt. Geospatial cryptography[19] can also be an exciting topic in itself, demonstrating how cryptography can be applied in various contexts.
- *Hands-on learning*: Students were asked to use tools and softwares to solve complex math questions. This enables students to actively participate in solving puzzles and navigating Google Earth, which can enhance their understanding and retention of the material.

The proposed methodology can be an effective pedagogical tool for teaching computer security and mathematics because it combines hands-on learning, problem-solving, collaboration, and real-world relevance in an engaging and memorable way. It leverages students' natural curiosity and sense of adventure to make learning these important subjects more enjoyable and effective. Further, the proposed methodology was compared with research based group project.

3 Methods

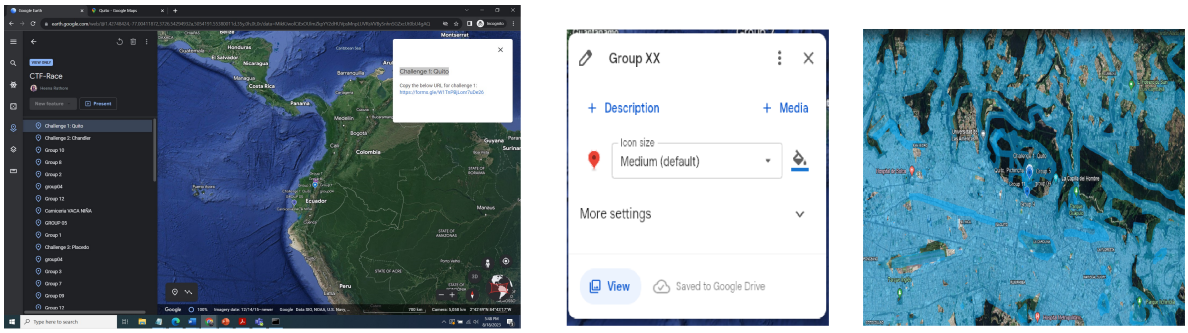
In a CTF competition, participants (often called "hackers" or "players") are tasked with solving a variety of challenges that test their skills in different areas of cybersecurity[20]. These challenges can involve cryptography, reverse engineering, web security, binary exploitation, network analysis, and more[21]. A scavenger hunt-style challenge in a CTF usually involves searching for hidden pieces of information or "flags" within a computer system or network. These flags could be files, passwords, encryption keys, or any other type of data. Players must use their skills to locate and extract these flags, often by analyzing code, manipulating data, exploiting vulnerabilities, or solving puzzles.

3.1 CTF Scavenger Hunt

In the proposed CTF scavenger hunt, students were organized into teams each comprising of four or five members. Each team was shared with a link which led to Google Earth map as shown in Fig 1(a). The map displayed a pin indicating the location of a challenge question on a location.

Each location leads to a challenge where the students were asked to find flags presented in the form of a ciphertext that corresponds to a place or a person's name. Teams members were required to collaborate to decrypt the challenge. As soon as they decrypt the message, each team would drop a single pin (See Figure 1(c)) on the map for each deciphered location (limiting to one pin per location per team) on the map. The process involves saving a location pin then input the name of the location, followed by the "Group number." (See Figure 1(b))

Upon completing the decryption task, the group would be given a flag to another pin location and were asked to inform the instructor. The instructor will then provide a clue to the subsequent map location by dropping the pin and the process continues. The amazing race comprised a total of six challenges, with the team achieving the fastest completion and maximum drops of pins and flags



(a) (b) (c)

Figure 1: (a) Google Earth Map (b) Dropping a pin (c) Pins dropped on location

were given the title of "Codebreakers" and received extra credit. The students were allowed to use all online tools, as well as textbooks to crack the code. The students were allowed to use language tools such as chatGPT, Bard and others[22]. Details of challenges are given below.

3.1.1 Challenge 1

The challenge entails decrypting the random ciphertext using one of three potential encryption techniques: Caesar cipher, ROT13, or Vigenère cipher. A provided hint guides study to consider these three specific encryption techniques when attempting to decrypt the ciphertext. Teams were asked to decipher it to reveal the original message was a person's name.

3.1.2 Challenge 2

This challenge presents the task of decrypting the provided ciphertext by employing two encryption techniques: Hill Cipher or Advanced Encryption Standard (AES). The cipher text given in this location was a geographical location. For the Hill Cipher, a specific key was provided. For AES, the key was not provided and the students were asked to derive from the binary equivalent of the key numbers provided for Hill Cipher. The students were asked to use the Electronic Codebook (ECB) mode of operation to encrypt each data block to get the binary equivalent. Later, the students were asked to convert binary to ASCII using a binary to ASCII converter to obtain the final answer. The second clue also revealed a person's name.

3.1.3 Challenge 3

In this challenge, a situation was given to the students. The narrative is: Alice aims to communicate with Bob through an insecure channel. Bob employs the RSA algorithm, an asymmetric encryption technique, to send the message. He has created a pair of public-private keys, and the task is to decipher the given message using these keys. The public and private were given to the teams where the private key follows the PKCS#8 format, and the public key is in X.509 format. The encrypted message was a geographical location and the decryption leads to a person's name.

3.1.4 Challenge 4

The challenge involves performing multiplication on two large numbers, p and q, and subsequently finding the factors of the resultant number. To achieve this, participants are instructed to download and employ the yafu tool. The values of p and q are provided as hexadecimal representations. The students were given extra commands such as "yafu.exe "p*q"" to be executed in the command prompt to perform the multiplication. Afterward, the task entails factorizing the computed number and identifying the P3 value as the answer. To factorize the number, the command "yafu.exe factor (number)" was used. An additional doc file was given to students for consultation. The decrypted flag was a location to a particular place.

3.1.5 Challenge 5

In this challenge, participants are required to perform an XOR operation on a given cipher text using a key of 1. The cipher text was presented in the form of binary sequences separated by exclamation marks. The students were asked to perform the XOR operation by performing bitwise combining each bit of the cipher text with the corresponding bit of the key. Subsequently, the resulting output needs to be converted, replacing the groups of numbers with their equivalent ASCII codes. This process will lead to the discovery of the final location encoded within the modified text.

3.1.6 Challenge 6

In the ultimate challenge of the CTF race, students were tasked with uncovering the underlying relationship that ties all the previous challenges together. The hint suggests contemplating the connections between the individuals and the locations given in the CTF race. By identifying this overarching relationship, students were asked to ascertain the name of a specific place. The challenge culminates with the team dropping a final pin on the map to mark this location, signifying their successful completion of the race.

3.2 Group Project

In order to compare the active learning experience, we also asked the students to work in a group project (for half a semester). The groups were involved in a pedagogical method centered around research experience. In this approach, student groups were tasked with examining a research paper in the field of Cyber-Physical Systems (CPS) security having cryptography as an essential topic. This project involved activities such as replicating simulations detailed in the paper or showcasing an alternate solution. The primary aim of this approach was to not only familiarize students with advanced concepts in CPS security but also to see whether they like the experience of research vs CTF challenge. Students were presented with a set of eight representative papers from which they could choose for their review. Additionally, students had the liberty to opt for research papers that pertained to the subject matter addressed in the course. Following was the list of papers each group could choose from different domains of CPS such as internet of things devices, connected vehicles, medical devices and some recent papers in security domain.

- Internet Of things

  - Sensitive Information Tracking in Commodity IoT[24]
  - Perils of Zero-Interaction Security in the Internet of Things[25]
- Connected Vehicles
  - LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in The Internet of Vehicles[26]
  - MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles[27]
- Medical Devices
  - Energy-Aware Digital Signatures for Embedded Medical Device[28]
  - Secure and Privacy-Preserving Automated End-to-End Integrated IoT-Edge-Artificial Intelligence-Blockchain Monitoring System for Diabetes Mellitus Prediction[29]
- Recent Advancements
  - Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review[30]
  - Defending Against Neural Fake News[31]
  - Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection[32]
  - Universal and Transferable Adversarial Attacks on Aligned Language Models[33]

4 Results

This section presents the combined outcomes of the Spring 2023 and Fall 2023 semesters. For both research project as well as CTF scavenger hunt, fourteen-fifteen groups were established, with group sizes varying between 3 to 5 members. In both the semesters, one team was able to capture all the flags including the final challenge. Overall, the students enjoyed the CTF, with students engaging enthusiastically and investing significant time in solving exercises, thereby enhancing engagement and enjoyment in coursework. Figure 3 shows that 77.4% of students strongly believe that the CTF Scavengers Hunt was a valuable learning experience. 40.3% of students strongly agreed that it was a valuable learning experience. 37.1% of students agreed that it was a valuable learning experience. 19.4% of students were neutral. There were no students who disagreed or strongly disagreed that it was a valuable learning experience. Overall, the results suggest that the majority of students found the CTF Scavengers Hunt to be a valuable learning experience.

In the group project, fifteen teams selected papers focusing on recent advancements to implement. Five groups concentrated on connected vehicles, two on medical devices, three on IoT devices, three on LLM security, and a couple proposed new papers as their chosen focus. To evaluate the success of research-oriented group project, a pre and post survey was administered to the students with the objective of gauging their inclination towards research activities. The survey featured the following questions:

- Q1: I plan to attend graduate school after completing my degree.

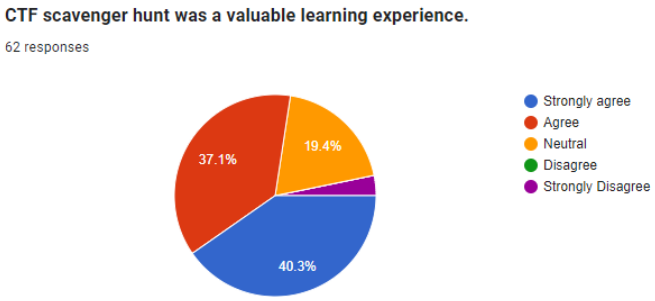


Figure 2: Post Scavenger Hunt Responses

- Q2: I am interested in getting research experience.
- Q3: I have interest in learning CPS security.
- Q4: I am comfortable in reading research papers.
- Q5: I am confident in my ability to do research.

Figure 3 (a)-(e) shows the comparative analysis of pre and post survey questions for Q1, Q2, Q3, Q4 and Q5 respectively. Based on the results, students particularly showed interest in reading the research papers, and showed interest in learning the CPS concepts.

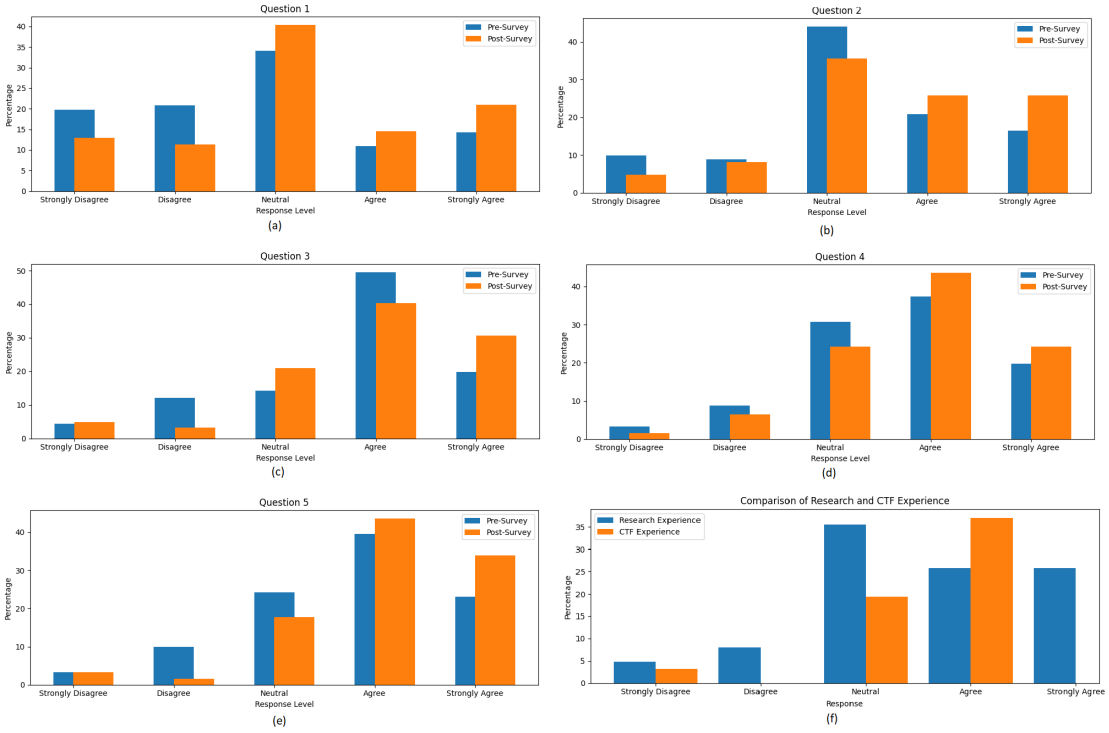


Figure 3: Pre and Post Group Project Experience

4.1 Comparative Analysis

We also compared CTF experience with group based research experience (See Figure 3 (f)). It was found that 25% of students strongly agreed or agreed that group based research experience was a valuable learning experience. Furthermore, more than 35% of students strongly agreed or agreed that CTF experience was a valuable learning experience. This suggests both CTF experience and group based research experience is a valuable learning experience in making students learn security concepts. Table 1 summarizes the key differences between group based research experience vs CTF experience based on the survey:

Table 1: Comparative analysis

Feature	Research Experience	CTF Experience
Focus	Deep understanding of underlying concepts	Practical skills
Time commitment	Typically longer-term	Typically shorter-term
Level of difficulty	Typically more difficult	Typically less difficult
Benefits	Can lead to publications and conference presentations	Can lead to job opportunities and scholarships

4.2 Limitations and Future Directions

The study emphasizes practical application over theory. While valuable, a strong foundation in theory is also crucial for deeper understanding and problem-solving in cryptography. The study does not address the long-term retention of knowledge gained through the scavenger hunt. Future research could investigate whether students retain the cryptographic principles they learned during the activity and whether they can apply them effectively in real-world scenarios over time. To evaluate the effectiveness of our approach in enhancing students' understanding of cryptographic concepts, we will utilize both quantitative and qualitative measures. This will involve administering pre- and post-tests to assess the knowledge gained by students who participated in the scavenger hunt compared to those who did not. Additionally, we will gather qualitative feedback from students through exams to gain insights into their learning. This comprehensive assessment strategy will provide valuable data to determine the efficacy of the scavenger hunt in achieving its educational objectives.

5 Conclusion

Integrating cryptography concepts within the scavenger hunt activity not only made learning enjoyable but also significantly increased engagement among participants. By presenting encrypted messages and challenging puzzles throughout the hunt, students were encouraged to apply cryptographic principles actively. This hands-on approach not only deepened their understanding of encryption and decryption but also underscored the importance of secure communication in a real-world context. This heightened engagement had a motivating effect, compelling students to invest the additional time and effort needed to develop the essential math skills required for decoding

the messages effectively. In our assessment, the CTF exercise has proven to be a valuable tool for enhancing students' comprehension of the security implications of system intricacies, a facet not extensively covered previously. Engaging in the formulation of a CTF challenge compels students to meticulously scrutinize and grasp the theory of cryptography. CTF exercises inherently encourage teamwork, often making them suitable for extracurricular engagement, although efforts are ongoing to integrate CTF-related content into the curriculum. This approach also offers students an opportunity to engage with the broader hacker community.

6 Acknowledgements

This work is supported by the National Science Foundation (NSF) under CISE Research Initiation Initiative (CRII) award #2153510 and #2313351 and award HRD-2119930 NSF Eddie Bernice Johnson INCLUDES Alliance Engineering PLUS (Partnerships Launching Underrepresented Students). 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

[1] S. Hansche, "Designing a security awareness program: Part 1". *Information systems security*, vol. 9, no. 6, pp.1-9, 2001.

[2] E. Crowley, "Information system security curricula development". In Proc. *4th conference on Information technology curriculum*. pp. 249-255, 2003.

[3] J. Seberry, and J. Pieprzyk, "Cryptography: an introduction to computer security". *Prentice-Hall*, Inc, 1989.

[4] Cryptography in Digital Age, https://www.mckinsey.com/ /media/mckinsey/business%20functions/risk/our%20insights/cybersecurity%20in%20a%20digital%20era/cybersecurity%20in%20a%20digital%20era.pdf [accessed on August 18, 2023]

[5] G. Baumslag et al., "A course in mathematical cryptography". *Walter de Gruyter GmbH & Co KG*, 2015.

[6] S.D. Galbraith, "Mathematics of public key cryptography". *Cambridge University Press*, 2012.

[7] S.Y. Yan, "Computational number theory and modern cryptography". *John Wiley & Sons*, 2013.

[8] L. McDaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction". In *49th hawaii international conference on system sciences (hicss)*, pp. 5479-5486, IEEE, 2016

[9] J. Mirkovic, and P.A. Peterson, "Class Capture-the-Flag Exercises". In *USENIX Summit on Gaming, Games, and Gamification in Security Education*, (3GSE 14), 2014.

[10] Michael Serra, "Pirate Math Treasure hunt puzzles with cryptography", *CMC-S Palm Springs Fall*, 2012.

[11] D.W. Johnson, and R.T. Johnson, "Social skills for successful group work". *MAA notes*, pp.201-204, 1997.

[12] M. Sweet, and L.K. Michaelsen eds., "Team-based learning in the social sciences and humanities: Group work that works to generate critical thinking and engagement". *Taylor & Francis*, 2023.

[13] Cryptography Scavenger Hunt, https://inl.gov/content/uploads/2023/04/Cryptography-Scavenger-Hunt-Lesson-Plan.pdf [Accessed on August 17, 2023]

[14] Jonestastic Math, Cryptography Worksheet and Scavenger Hunt: Caesar Shift, https://www.teacherspayteachers.com/Product/Cryptography-Worksheet-and-Scavenger-Hunt-Caesar-Shift-1939146 [Accessed on August 17, 2023]

[15] A. Judy Holdener and J. Eric Holdener. "A Cryptographic Scavenger Hunt". *Cryptologia 31*, no. 4, pp. 316–323, 2007

[16] T. Le, and T. Hoang, "MAPLE: A Metadata-Hiding Policy-Controllable Encrypted Search Platform with Minimal Trust". *Cryptology ePrint Archive*, 2023

[17] H. Tims, G. Turner, C. Duncan and B. Etheridge, 2009. "Work in progress - Cyber Discovery camp — Integrated approach to cyber studies," *39th IEEE Frontiers in Education Conference*, San Antonio, TX, USA, pp. 1-2, 2009.

[18] D. Tsoupikova, R. Zeng, V. Pless, and J. Beissinger, "Cryptography and mathematics: educational game "Treasure Hunt"". In *ACM SIGGRAPH 2006 Research posters (SIGGRAPH '06). Association for Computing Machinery, New York*, NY, USA, 40–es. 2006.

[19] GM Jacquez, et al., "Geospatial cryptography: enabling researchers to access private, spatially referenced, human subjects data for cancer control and prevention". *J Geogr Syst*. vol. 19, no. 3, pp. 197-220, 2017.

[20] L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, pp. 5479-5486, doi: 10.1109/HICSS.2016.677, 2016.

[21] LCDR Chris Eagle, and John L. Clark, 2004. "Capture-the-Flag: Learning Computer Security Under Fire", Naval Postgraduate School 833 Dyer Rd., Code CS/Cp Monterey, CA 93943-5118.

[22] J. Crawford et al., "Artificial Intelligence and Authorship Editor Policy: ChatGPT, Bard Bing AI, and beyond". *Journal of University Teaching & Learning Practice*, vol. 20, no. 5, p.1., 2023.

[23] K. Leune, and S.J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education". In *Proceedings of the 18th annual conference on information technology education*, pp. 47-52, 2017.

[24] Z.B. Celik et al., "Sensitive information tracking in commodity IoT". *In 27th USENIX Security Symposium (USENIX Security 18)*, pp. 1687-1704, 2018.

[25] M. Fomichev et al., "Perils of zero-interaction security in the internet of things". *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 1, pp.1-38, 2019.

[26] L. Yang et al., "LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in The Internet of Vehicles," *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, pp. 3545-3550, 2022.

[27] L. Yang, A. Moubayed and A. Shami, "MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles," in *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616-632, 1 Jan.1, 2022.

[28] M.O. Ozmen, A.A. Yavuz, and R. Behnia, "Energy-aware digital signatures for embedded medical devices" In *IEEE Conference on Communications and Network Security (CNS)*, pp. 55-63, 2019.

[29] L. Ismail et al. "Secure and Privacy-Preserving Automated End-to-End Integrated IoT-Edge-Artificial Intelligence-Blockchain Monitoring System for Diabetes Mellitus Prediction". *arXiv preprint arXiv:2211.07643*, 2022.

[30] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review." *Expert Systems with Applications*, p.118401, 2022.

[31] R. Zellers et al., "Defending against neural fake news". *Advances in neural information processing systems*, 32, 2019.

[32] K. Greshake et al. "Not what you've signed up for: Compromising real-world llm-integrated applications with indirect prompt injection". In *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*, pp. 79-90, 2023.

[33] A. Zou et al., "Universal and transferable adversarial attacks on aligned language models". *arXiv preprint arXiv:2307.15043*, 2023.