МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2025
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2025
Proceedings of the Fifty-Fourth Spring Conference
of the Union of Bulgarian Mathematicians
Varna, March 31 – April 4, 2025

EVALUATING THE EFFECTIVENESS OF PRACTICAL EXERCISES IN CRYPTOGRAPHY AND AUTHENTICATION COURSES OF CYBERSECURITY EDUCATION

Dilyana Dimitrova
Department of Information Technologies,
Nikola Vaptsarov Naval Academy, Varna, Bulgaria
e-mail: di.dimitrova@naval-acad.bg

This study analyzes the effectiveness of practical exercises in higher education cybersecurity programs, specifically within the disciplines of authentication and cryptography. Based on student feedback, the study assesses the alignment between theoretical and practical components, and proposes improvements for better industry preparedness. The findings highlight that both individual and teamwork-based exercises significantly enhance students understanding of key concepts. The results emphasize the need for a balanced curriculum that integrates practical skills, bridging the gap between theory and real-world application, and preparing students for evolving cybersecurity challenges.

Keywords: authentication, cryptography, cybersecurity education, practical exercises, survey

ОЦЕНКА НА ЕФЕКТИВНОСТТА НА ПРАКТИЧЕСКИТЕ УПРАЖНЕНИЯ В КУРСОВЕТЕ ПО КРИПТОГРАФИЯ И АВТЕНТИКАЦИЯ В ОБУЧЕНИЕТО ПО КИБЕРСИГУРНОСТ

Диляна Димитрова
Катедра „Информационни технологии“, ВВМУ „Н. Й. Вапцаров“, Варна
e-mail: di.dimitrova@naval-acad.bg

https://doi.org/10.55630/mem.2025.54.118-124

* The report is in implementation of the National Scientific Program "Security and Defense adopted with RMS No. 731/21.10.2021, and financed by the Ministry of Education and Science of the Republic of Bulgaria according to Agreement No. D01-74/19.05.2022.

2020 Mathematics Subject Classification: 94A60, 94A62.

Настоящото изследване анализира ефективността на практическите упражнения в програмите за висше образование по киберсигурност и по-конкретно в дисциплините, свързани с автентикация и криптография. Чрез обратната връзка от студентите, изследването оценява съответствието между теоретичните и практическите компоненти и предлага подобрения за по-добра подготовка на обучаемите за индустрията. От изследването се подчертава, че както индивидуалните, така и екипните упражнения, значително подобряват разбирането на студентите за ключови концепции. Резултатите показват необходимостта от балансирани учебни програми, които интегрират практически умения и подготвят студентите за непрекъснато развиващите се предизвикателства в киберсигурността.
Ключови думи: автентикация, криптография, обучение по киберсигурност, практическо обучение, анкета

1. Introduction. Cryptography and authentication are fundamental parts of cybersecurity, ensuring the confidentiality, integrity, and authenticity of digital communications and data. Cryptography protects sensitive information from unauthorized access by encrypting it, making it unreadable without the proper decryption key. This is essential in preventing data breaches and securing communications over networks. Authentication mechanisms confirm the identity of users, devices, and systems, establishing trust in interactions. Strong authentication techniques, such as multifactor authentication (MFA), biometrics, and digital certificates, protect against identity theft and unauthorized access.

Integrating theoretical knowledge with practical application in the curriculum for cryptography and authentication courses is crucial for providing students with a systematic understanding in these fields. However, there are gaps between the theoretical depth offered in some programs and the hands-on experience needed to fully prepare students for the real-world challenges of the industry. One of the things is the overemphasis on theory, particularly in the foundations of cryptography, where students are often introduced to complex mathematical concepts and cryptographic protocols without enough emphasis on their real-world applications. This can leave them with a strong theoretical understanding but limited practical experience. While theoretical lessons may cover a range of cryptographic techniques, practical exercises might fail to incorporate widely-used tools or platforms, leaving students underprepared for real-world environments. The main aim of the paper is to evaluate the effectiveness of practical exercises in cybersecurity education, specifically in the fields of cryptography and authentication.

The structure of the paper includes an introduction, a literature review, methodology, results, and discussion, followed by conclusions and recommendations for improving the curriculum to better prepare students for real-world challenges.

2. Literature review. In the context of education, bridging the gap between theoretical learning and practical application is a significant challenge. Theoretical learning provides the fundamental understanding of concepts, but without the practical part, students may struggle to apply their knowledge effectively in professional environment. On the other hand, practical exercises help students develop valuable skills, but without theoretical background, they may lack the deep understanding required to solve complex real-world problems.

Several studies have examined this gap and suggested methods for better integration. The paper [5] examines trends in cybersecurity education, focusing on various cybersecurity topics, including cryptography, and presents insights into how these subjects are

being taught in the classroom. It explores educational models that help bridge the cybersecurity skills gap and discusses how technologies like virtual classrooms and online platforms can be utilized to enhance teaching outcomes for cybersecurity courses. In [3] a review focused on the teaching methods and practices in cybersecurity education is presented, particularly looking into topics like encryption and authentication, and how they are taught in academia. Key aspects in study [1] include the teacher's role in engaging students, the need for specific engagement methods in virtual learning environments, and the challenges students face in them. The paper [4] explores the development of specialized postgraduate education in maritime cybersecurity at the Nikola Vaptsarov Naval Academy, focusing on meeting International Maritime Organization standards and improving the cybersecurity competencies of maritime professionals. The paper [2] explores the challenges of teaching cryptography by using certificateless signature schemes as a case study in cryptography education. Additionally, it proposes simple improvements to enhance security and suggests that case-based teaching methods can make cryptographic concepts more accessible and clear for students.

One effective approach bridging the gap is to adopt combined learning models, which incorporate both theoretical lessons and practical assignments, ensuring that students are not only exposed to abstract concepts but also given opportunities to apply them in simulated or real-world scenarios. Similarly, methods like action learning, which emphasize real-life work experience, have proven effective in helping students connect theory with practice. Educational frameworks must be continuously adapted to offer a balance between academic and practical exercises, preparing students for the dynamic demands of the industry.

Inconsistent assessment metrics present another challenge in aligning theoretical learning with practical competence. In many cases, students are evaluated primarily on their theoretical knowledge, without sufficient emphasis on their ability to apply concepts in practical situations. The lack of continuous feedback in practical exercises can restrict skill development, as students might not receive the necessary guidance to improve their practical abilities during the course. Practical exercises often fail to reflect the challenges students will face in the industry, such as securing cloud applications, implementing Public Key Infrastructure (PKI), or designing zero-trust authentication models. Group projects or team-based activities, which are essential for simulating real-world collaborative environments, are also often underrepresented. Without these, students may struggle to develop the collaborative and problem-solving skills required in a professional setting.

By examining and addressing these gaps, it is possible to ensure that students are well-prepared to handle the complexities of their future careers, qualified with both the theoretical knowledge and practical skills required to succeed in the rapidly evolving field of cybersecurity.

3. Methodology. To evaluate the effectiveness of cryptography and authentication courses in cybersecurity education, a survey was developed consisting of 22 questions. It aimed to assess students' perceptions of curriculum quality, the balance of theoretical and practical content, the relevance of course materials to industry needs, and students overall satisfaction with the learning process.

A total of 55 students participated in the survey. Most of them are in the fourth year of their BSc program of cybersecurity and a few – from previous years. The partici-

pants represented a diverse group in terms of academic performance and prior knowledge of cryptography and authentication, ensuring a well-rounded perspective on the course outcomes.

The survey included multiple types of questions:

- Multiple-choice – to gather insights on specific preferences of the course and teaching methods.
- Likert scale – to evaluate satisfaction and confidence levels regarding the course content and practical exercises.
- Open-ended questions – to provide students with the opportunity to elaborate on challenges, suggestions, and overall impressions.

The survey was conducted anonymously over two weeks using the Microsoft Forms platform to establish accessibility. This approach ensured honest responses and reduced any potential biases.

To analyze the data from the exercises a quantitative analysis was conducted. This included examining the frequency distribution of student responses to different exercises.

4. Results and discussion. The exercises included in this study cover a wide range of tasks, which allowed for an in-depth examination of various security aspects. From password-related attacks on different operating systems to multi-factor authentication (MFA) vulnerabilities, the exercises provided valuable insights into system security weaknesses. Practical tasks on cryptography enhanced understanding of encryption techniques, while case studies involving biometric methods demonstrated their potential and limitations in authentication. Overall, the exercises highlighted the diverse and evolving nature of security challenges and the importance of multi-layered defense strategies.

Table 1 presents the survey results based on responses to the question: „To what extent did the tasks in the conducted practical exercises help you understand the key principles and concepts related to authentication?". The survey responses in the table were combined from two categories: „To a large extent" and „All tasks contributed to understanding the material". These responses reflect how the students perceived the exercises effectiveness in deepening their understanding of the subject matter, providing insight into which tasks were most impactful.

Table 1. Impact of practical exercises on understanding key principles and concepts

Topic of the exercises	**Survey results (%)**	**Exercise type**
Analysis of security breaches	78.2%	Individual
Password attacks	78.1%	Individual
Password security assessment	96.3%	Individual
Password managers	89.1%	Individual
Cases related to biometrics	85.4%	Teamwork
Handwriting analysis	85.4%	Teamwork
Practical tasks related to cryptography	89.1%	Teamwork

Topic of the exercises	Survey results (%)	Exercise type
PKI and working with certificates	87.3%	Individual

Table 1 indicates that individual exercises, such as those focused on security breaches, password attacks, and password managers, received high ratings, ranging from 78.1% to 96.3%. In contrast, teamwork exercises, like those on biometrics, handwriting analysis, and cryptography, also received strong feedback, with results between 85.4% and 89.1%. This indicates that both individual and teamwork-based exercises significantly contributed to enhancing students understanding of the subject matter.

The average values for each exercise type and standard deviation are calculated to provide a clearer understanding of the overall effectiveness and consistency of the exercises. The results are presented on figure 1 and table 2.

Table 2. Average value for exercise type and standard deviation

Exercise type	Average value for exercise type	Standard deviation
Teamwork	86.63%	2.136195996
Individual	85.80%	7.75306391

The results show that the average of 86.63% of students felt that teamwork exercises significantly contributed to their understanding. Furthermore, the low standard deviation (2.14) indicates that student perceptions about the effectiveness of teamwork exercises were very consistent – most students had a similar, positive experience. An average of 85.80% of students felt that individual exercises significantly contributed to their understanding. While this average is only slightly lower than teamwork, the much higher standard deviation (7.75) shows a large variation in student perceptions. Some students found the individual exercises extremely helpful, while others found them less so. The responses were far less consistent than for teamwork exercises.

In conclusion, while the overall perceived helpfulness of both types of exercises was similar on average, teamwork exercises led to a more consistent positive perception among students. Individual exercises, while helpful for some, resulted in a much wider range of opinions regarding their effectiveness in deepening understanding. This suggests that teamwork exercises may provide a more reliable and consistently positive learning experience for students in key concepts. The larger variation in individual exercise effectiveness is because some of them are more challenging or require different learning styles, leading to the wider range of responses.

This highlights the value of collaborative activities in encouraging a deeper comprehension of complex topics, supporting peer interaction, and sharing diverse perspectives, which often enhance the learning experience.

Key findings from the various tasks include:

- Password attacks - both Windows and Linux operating systems were found to be vulnerable to common password-based attacks.

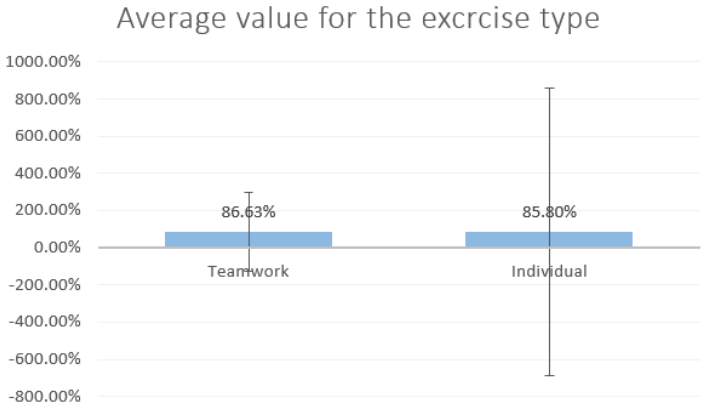

Figure 1. Average value for the exercise type

- Biometric systems - case studies on fingerprint and handwriting analysis revealed strengths and limitations of biometric authentication, emphasizing the need for continuous improvement in these technologies.

- Practical exercises on cryptography highlighted the importance of secure key management and the need for up-to-date encryption algorithms to protect data effectively.

These findings collectively underline the need for multi-layered security approaches and constant awareness in the face of evolving threats.

To enhance cybersecurity education in cryptography and authentication courses, it is crucial to emphasize practical application by incorporating hands-on exercises and real-world simulations that strengthen students' ability to apply theoretical concepts. Integrating emerging technologies such as post-quantum cryptography and lightweight cryptography will better prepare students for future challenges. Encouraging teamwork through collaborative projects can mirror industry environments, while regular feedback during practical exercises will enhance the learning experience. Revising assessment methods to balance theoretical and practical evaluations will ensure that students are prepared for real-world cybersecurity scenarios.

5. Conclusion. The findings of this study emphasize the critical role of practical exercises in enhancing students understanding of key concepts in cryptography and authentication. Both individual and teamwork-based tasks were highly effective in reinforcing theoretical knowledge, as evidenced by the survey results. Teamwork exercises, in particular, encouraged deeper comprehension through collaboration, while individual tasks ensured students could apply their knowledge independently. In conclusion, practical exercises provide a comprehensive approach to cybersecurity education, bridging the gap between theory and real-world application, and preparing students to address the evolving challenges in the field of cybersecurity.

References

[1] H. Balalle. Exploring student engagement in technology-based education in relation to gamification, online/distance learning, and other factors: A systematic literature review. *Social Sciences & Humanities Open* [Internet]. 2024 Jan 1;9:100870–0. Available from: https://www.sciencedirect.com/science/article/pii/S2590291124000676.

[2] X. Hu, W. Jiang, C. Ma, C. Yu. Security and design analysis of certificateless signature schemes as teaching cases of cryptography and security course education. 9th International Conference on Information Technology in Medicine and Education (ITME), (2018), 601–605. https://doi.org/10.1109/itme.2018.00138.

[3] M. Mukherjee, Ngoc Thuy Le, Chow YW, W. Susilo. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information* 2024, 15, 117. https://doi.org/10.3390/info15020117

[4] B. Nikolov. Maritime cybersecurity education and training at Nikola Vaptsarov Naval Academy. *Pedagogika-Pedagogy: Bulgarian Journal of Educational Research and Practice*, 95(6s) (2023), 1-10. https://doi.org/10.53656/ped2023-6s.05.

[5] V. Švábenský, J. Vykopal, P. Čeleda. What Are Cybersecurity Education Papers About? Proceedings of the 51st ACM Technical Symposium on Computer Science Education. 2020 Feb 26.