AN INTERACTIVE LEARNING APPROACH FOR TEACHING DIFFIE – HELLMAN KEY EXCHANGE PROTOCOL

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

Abstract: *The article presents an interactive learning approach for teaching the Diffie-Hellman key exchange protocol. The proposed framework combines structured exercises with an interactive web-based simulation that visualizes each stage of the protocol. The learning process is organized into a sequence of tasks, starting from modular arithmetic and leading to full protocol execution and security analysis.*

The approach was implemented with first-year Cybersecurity and DevOps students and evaluated through a questionnaire assessing learners' perceptions of understanding and usability. Results indicate that students reported improved understanding of the Diffie-Hellman protocol and found the visual and interactive elements helpful in understanding the computation of the shared secret. Participants also reported that the simulation helped them follow the sequence of operations in the protocol and improved engagement compared to traditional manual problem-solving. Future work will focus on controlled experimental evaluation and extension of the framework to additional public-key cryptographic algorithms.

Keywords: cybersecurity education, cryptography, Diffie-Hellman key exchange, interactive simulation, modular arithmetic, task-based learning

1. Introduction

Cryptography is a core component of modern computer science and cybersecurity curricula. The Diffie-Hellman (DH) key exchange protocol is of particular importance due to its relatively simple mathematical foundation and its historical significance as the first practical mechanism for enabling two parties to establish a shared secret over an insecure communication channel (Katz, Lindell 2015).

The main aim of the study is to propose an approach that integrates the traditional learning process with visual and interactive representations of the DH protocol. The simulation presented in this work uses tasks designed to enhance understanding of modular arithmetic and the underlying symmetry of the protocol. The classroom activity was conducted with first-year

Cybersecurity and DevOps students and provides an evaluation of their learning experience and understanding of the presented concepts.

2. Related work

For the literature review, peer-reviewed publications indexed in the Scopus database from 2020 to 2025 were analysed. The search was conducted using the keywords "cryptography", "education", and "Diffie-Hellman". Given the limited research addressing the teaching of the Diffie-Hellman protocol, an additional source was included in the analysis to expand the understanding of existing educational approaches related to the topic.

Table 1. Papers relevant to the topic

Paper	Use of DH	Domain / Application	Educational aspect
(Kalaiyarasi et al. 2023)	DH is used for secure key exchange integrated into cloud-based engineering education platform	Cloud computing and education	Designed for secure user data in engineering education.
(Borodzhieva 2022)	Teaching Diffie-Hellman and ElGamal using project-based learning	Higher education, telecommunication security	Flipped classroom and project-based learning.
(Lodi et al. 2022)	Remote-unplugged DH exercise	K-12 education, cryptography teaching	Focus on learning outcomes and engagement.
(Zhao et al. 2022)	DH is used for authentication in digital museum system	Digital museum, cultural heritage protection	No
(Vyas 2021)	Modified DH protocol for mutual authentication	Authentication scheme	No
(Diop et al. 2021)	Security proof based on q-SDH (Strong DH assumption)	Mobile transit systems, privacy-preserving e-payments	No

Recent studies (Table 1) have explored the Diffie-Hellman key exchange protocol in various contexts, highlighting its significance both as a cryptographic technique and as a topic for cybersecurity education. In paper (Kalaiyarasi et al. 2023) authors propose DHPKey, an encryption scheme that combines DH and symmetric cipher. Its purpose is to secure sensitive data within a cloud-based platform. The pedagogical aspect of the work is limited to the application of the system in an educational environment.

The author in (Borodzhieva 2022) presents a project-based learning approach for teaching the Diffie-Hellman algorithm and the ElGamal cryptosystem in an undergraduate Telecommunication Security course. The proposed methodology combines flipped classroom principles with project-based learning, encouraging students to develop practical implementations while strengthening problem-solving and other skills. Although the work demonstrates the value of active learning, it focuses primarily on project development rather than providing an interactive visualization of the protocol or a structured sequence of conceptual learning activities.

The authors in (Lodi et al. 2022) design and evaluate a cryptography course for Grade 10 students which includes interactive activities with the Snap! visual programming language and a "remote-unplugged" DH exercise. This study demonstrates the potential of DH as a learning topic and highlights students' positive perceptions of such activities.

In paper (Zhao et al. 2022) authors integrate DH into a digital museum platform alongside Digital Twin, Artificial intelligence (AI) and 5G technologies, using the protocol for secure authentication of users accessing cultural heritage content. In (Vyas 2021) authors develop a lightweight, smart card-based multi-server authentication scheme that applies a modified DH protocol for secure and efficient communication. In (Diop et al. 2021) it is proposed PAYGO - a privacy-preserving mobile transit pass system built on Direct Anonymous Attestation, whose security is based on a strong DH assumption. This work emphasizes the protocol as a practical tool in real-world critical systems but does not address its pedagogical potential. Although it is widely applied in technological and security contexts, its use as a pedagogical subject remains underexplored.

After the review, the results indicate that research on teaching the Diffie-Hellman protocol remains limited. Existing educational work has primarily focused on project-based learning in higher education and interactive activities for secondary-school students. A limited number of studies investigate how interactive visualization can be integrated into a structured teaching approach for introducing the Diffie-Hellman protocol to undergraduate students.

Further research is therefore needed to explore effective instructional approaches for introducing the protocol.

3. Teaching approach

The teaching approach of the Diffie-Hellman key exchange protocol is based on three principles:

- Simplicity - all computations use small prime numbers and exponents to ensure that students can perform calculations manually or with basic tools, allowing focus on conceptual structure rather than computational complexity.
- Visual-first learning - mathematical operations are consistently introduced alongside visual or interactive representations, aligning with dual coding theory (Sadoski, Paivio 2013).
- Guided discovery - the task sequence is designed to encourage students to infer the core property of DH through exploration rather than being presented with it directly.

  The method is organized around a sequence of five guided tasks (Fig. 1):

  1. Understanding modular arithmetic - students compute simple expressions such as $5^3 \bmod 23$ by hand, building familiarity with exponentiation and understanding the behavior of modular arithmetic.
  2. Exploring generators and cycles - students compute successive powers of a small generator modulo a small prime and observe how the resulting sequence cycles introducing the idea of a generator without formal group theory.
  3. Simulating one party's key generation - students compute a public value from a chosen private exponent (for example, Alice's public key as $g^a \bmod p$), emphasizing that the computation is straightforward to perform but computationally difficult to reverse.
  4. Simulating the full key exchange - working in pairs, students each play the role of "Alice" or "Bob", independently choose private values, exchange public components and independently derive the same shared secret.
  5. Reasoning about security - students are shown what an eavesdropper ("Eve") can observe - the prime, the generator, and both public values - and are asked to explain, in their own words, why this information is insufficient to compute the shared secret, introducing the concept of computational hardness.

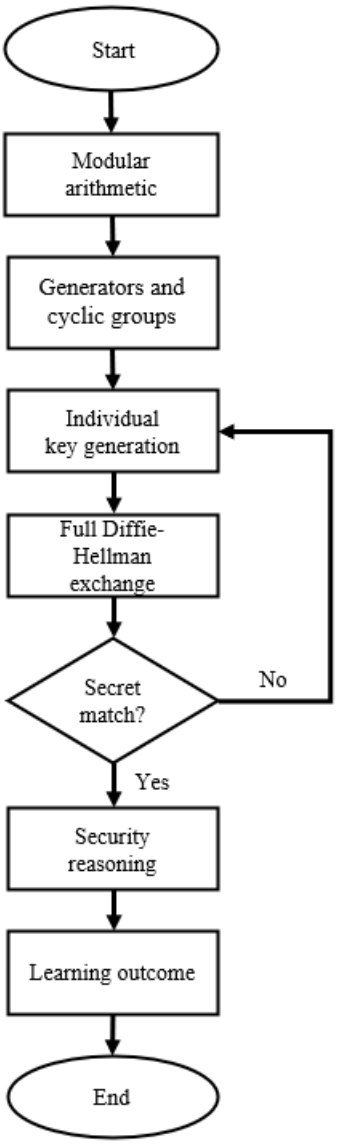

Figure 1. Algorithm of the proposed teaching approach for the Diffie-Hellman key exchange protocol

Each task includes objectives, step-by-step instructions, examples and expected outputs. The activities progress from foundational modular arithmetic to security reasoning, with each task building on knowledge acquired in the preceding stage.

4. Interactive simulation of the DH key exchange protocol

The interactive simulation (Figure 2) presents the visual component of the proposed learning method. It was developed to support the teaching approach's learning sequence by allowing students to observe, manipulate, and experiment with the individual stages of the protocol in a controlled environment. The simulation visualizes the process as communication

between two ships sharing public information over an insecure channel. This metaphor was selected to emphasize that the communicating parties can establish a shared secret despite operating over a publicly observable communication medium.

The simulation was implemented as a standalone web application using HTML, CSS, and JavaScript, running entirely in the browser. It includes four learning modes, each addressing different pedagogical objectives.

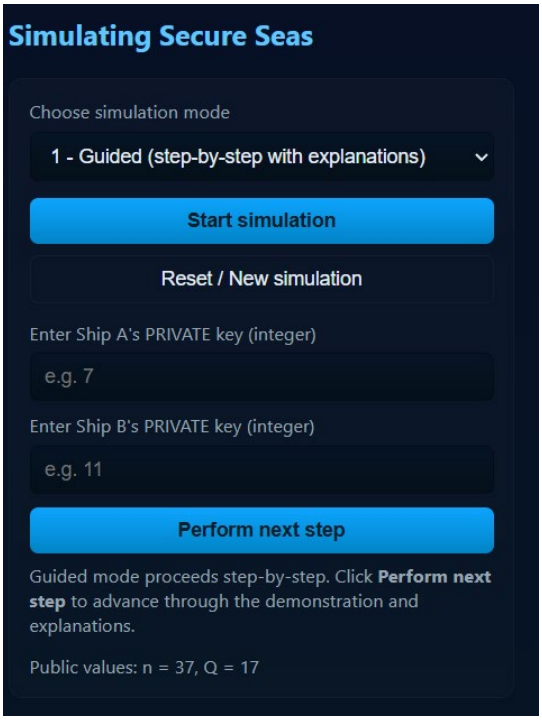

Figure 2. User interface for step-by-step Diffie-Hellman simulation

Guided mode provides a step-by-step walkthrough of the Diffie-Hellman key exchange protocol. Students manually enter the private keys of the two communicating parties and observe how public keys are generated through modular exponentiation. Each step is enhanced by explanations describing mathematical operations and their cryptographic significance.

Automatic demonstration mode performs the complete protocol automatically using randomly generated parameters. Its main goal is to demonstrate the overall workflow of the protocol.

Attack mode presents a Man-in-the-Middle attack. An adversary intercepts the exchanged public values and establishes independent shared keys with each participant. This visualization enables students to distinguish between confidentiality and authentication and

shows why the basic Diffie-Hellman protocol must be combined with authentication mechanisms in practical applications.

Mathematical practice mode focuses on modular exponentiation. Students calculate expressions of the form $g^a \bmod p$ manually and verify their answers using the simulator. It reinforces the mathematical foundations of the protocol and reduces calculation errors that might otherwise distract from conceptual understanding.

Throughout all modes, intentionally small prime numbers are used to make the computations transparent and suitable for classroom discussion. The objective is not to simulate cryptographically secure parameters but rather to support conceptual understanding of the algorithmic process.

5. Methodology

The proposed teaching approach and interactive simulation were used during a classroom session involving 45 first-year undergraduate Cybersecurity and DevOps students. The lesson began with a brief review of modular arithmetic and the basic principles of the Diffie-Hellman protocol, followed by guided exercises based on the five-stage teaching approach presented in Figure 1. Students then used the interactive simulation in Guided Mode to complete the protocol step by step and subsequently explored the Attack Mode to observe a Man-in-the-Middle scenario and discuss the importance of authentication.

Following the activity, participants completed an anonymous questionnaire designed to evaluate their understanding and their experience using the simulation. It consisted of four sections:

(1) demographic information and previous experience with programming and cryptography;
(2) self-assessment of understanding and confidence before the activity;
(3) perceptions of the interactive simulation after the activity;
(4) an overall evaluation of the simulation's usefulness. Responses were collected using five-point Likert scales, with an optional open-ended question for comments and suggestions.

The participants represented the intended audience for the proposed approach. Most students (67%) reported no previous study of the Diffie-Hellman protocol, 31% indicated only basic prior knowledge and 2% reported strong familiarity with the underlying algorithms. More than half (56%) described themselves as beginners in programming.

To examine changes in students' self-reported understanding before and after the activity, pre- and post-simulation responses were compared using the Wilcoxon signed-rank test (Wilcoxon 1945).

6. Results and discussion

Participants evaluated the simulation positively - 38% rated it as very useful and 49% as useful (Fig. 3), meaning that 87% of participants provided a positive evaluation. The remaining 13% selected the neutral option, while no participant provided a negative evaluation. These findings indicate that the simulation was perceived as a valuable resource for learning the Diffie-Hellman key exchange protocol.

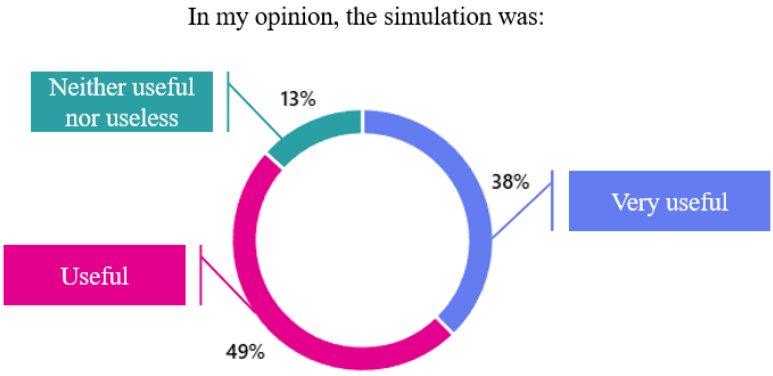

Figure 3. Students' opinion of the simulation

Tables 2 and 3 summarize students' self-assessments before and after the classroom activity. The composite self-assessment score increased from M = 3.13 (SD = 1.15) before the activity to M = 3.33 (SD = 1.07) after completing the proposed learning sequence. The difference was statistically significant according to the Wilcoxon signed-rank test ($p = 0.047$), indicating a modest improvement in students' perceived understanding and confidence.

Students' qualitative comments complemented the quantitative results. Several participants noted that modular arithmetic remained challenging, whereas the interactive visualization helped them better understand the sequence of operations and the exchange of public and private values. The visualization of the Man-in-the-Middle attack was also frequently mentioned as helpful for understanding why authentication is required in practical implementations of the protocol.

Table 2. Self-reported understanding before the simulation

No	Statement	M	SD
1	Understanding of the basic idea of the protocol	3.33	1.26
2	Knowledge of how the shared key is calculated	3.07	1.34
3	Understanding of why the algorithm is secure	3.51	1.29
4	Confidence describing how the shared key is obtained	2.62	1.32
5	Perceived difficulty of cryptographic algorithms	3.04	1.21
6	Preference for visual/interactive learning methods	4.18	0.94
	Composite score (items 1-4)	**3.13**	**1.15**

Note: M - mean; SD - standard deviation.

Table 3. Self-reported perceptions after the simulation

No	Statement	M	SD
1	Clarity of understanding of the key exchange	3.07	1.27
2	Visual representation eased understanding	3.51	1.29
3	Ability to explain how the shared key is obtained	2.78	1.35
4	Simulation more effective than solving by hand	3.36	1.26
5	Appropriateness of visualization for teaching cryptography	3.93	1.19
	Composite score (all 5 items)	**3.33**	**1.07**

Note: M - mean; SD - standard deviation.

The findings indicate that combining guided classroom activities with interactive visualization can support the teaching of the Diffie-Hellman key exchange protocol. Rather than replacing traditional mathematical instruction, the simulation helps students understand the conceptual flow of the protocol and the relationship between its individual steps.

7. Conclusion

This paper presented a structured framework for teaching the Diffie-Hellman key exchange protocol through a combination of tasks and interactive visualization. The approach was implemented using a five-stage learning sequence that gradually introduces modular arithmetic, cyclic patterns, key generation, full protocol execution, and security analysis. A web-based simulation supported these stages through multiple learning modes.

The evaluation with first-year Cybersecurity and DevOps students indicates that the proposed approach was associated with improved perceived understanding of the protocol and increased learner engagement. Students particularly valued the visual representation of the key exchange process and the ability to interact with each step of the protocol. The results also suggest that visualization helps students follow the conceptual flow between the protocol's steps, even though the underlying modular arithmetic itself remained challenging for some participants, and supports the development of more intuitive models of cryptographic operations.

Future work will include experimental studies with larger participant groups and extend the approach to other public-key cryptographic systems, such as RSA and ElGamal, to investigate the broader applicability of task-based visualization in cryptography education.

REFERENCES

BORODZHIEVA, Adriana, 2022. Project-Based Learning for Teaching "Diffie-Hellman Algorithm, Elgamal Variant." In: *International Conference on Systems, Signals, and Image Processing*, vol. 2022-June, pp. 1–5. Sofia: IEEE Computer Society. ISBN 9781665495783. ISSN 2157-8702. Available from: https://doi.org/10.1109/IWSSIP55020.2022.9854393.

DIOP, Aïda, DESMOULINS, Nicolas, TRAORÉ, Jacques, 2021. Pass-As-You-Go: A Direct Anonymous Attestation-Based Untraceable Contactless Transit Pass. In: *Applied Cryptography and Network Security Workshops. ACNS 2021. Lecture Notes in Computer Science*, pp. 417–435. Kamakura: Springer, Cham. ISBN 978-3-030-81644-5. ISSN 1611-3349. Available from: https://doi.org/10.1007/978-3-030-81645-2_24.

KALAIYARASI, R., MOHANAPRAKASH, T. A., PRAKAASH, A. S., DIVYA, V., NAVEEN, P., SUNITHA, T., 2023. Enhancing Security and Confidentiality using Trust Based Encryption (DHPKey) in Cloud Computing. In: *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, pp. 1–6. Delhi: Institute of Electrical and Electronics Engineers Inc. ISBN 9798350335095. Available from: https://doi.org/10.1109/ICCCNT56998.2023.10306732.

KATZ, Jonathan, LINDELL, Yehuda, 2015. *Introduction to Modern Cryptography*. Boca Raton: CRC Press. ISBN 978-1-4665-7027-6.

LODI, Michael, SBARAGLIA, Marco, MARTINI, Simone, 2022. Cryptography in Grade 10: Core Ideas with Snap! and Unplugged. In: *Annual Conference on Innovation and Technology*

in Computer Science Education, ITiCSE, vol. 1, pp. 456–462. Turku: Association for Computing Machinery. ISBN 9781450392013. ISSN 1942-647X. Available from: https://doi.org/10.1145/3502718.3524767.

SADOSKI, Mark, PAIVIO, Allan, 2013. *Imagery and Text: A Dual Coding Theory of Reading and Writing - 2nd Ed*. New York: Routledge.

VYAS, Pranav, 2021. A Smart Card Based Lightweight Multi Server Encryption Scheme. In: *Soft Computing and its Engineering Applications. icSoftComp 2020. Communications in Computer and Information Science*, vol. 1374, pp. 212–223. Changa, Anand: Springer, Singapore. ISBN 9789811607073. ISSN 1865-0937. Available from: https://doi.org/10.1007/978-981-16-0708-0_18.

WILCOXON, Frank, 1945. Individual Comparisons by Ranking Methods. *Biometrics Bulletin*, vol. 1, no. 6, pp. 80–83. Available from: https://sci2s.ugr.es/keel/pdf/algorithm/articulo/wilcoxon1945.pdf.

ZHAO, Jing, GUO, Lei, LI, Yueqiao, 2022. Application of Digital Twin Combined with Artificial Intelligence and 5G Technology in the Art Design of Digital Museums. *Wireless Communications and Mobile Computing*, vol. 2022. ISSN 1530-8677. Available from: https://doi.org/10.1155/2022/8214514.