Vol. 11, No. 4, December 2025, Page. 256-260
DOI: http://doi.org/10.22146/jpkm.101525

Mathematics in Cryptography and Its Applications in Cybersecurity

Uha Isnaini[1]*, Nurul Qomariasih[2], Amiruddin[3], Made Tantrawan[1], Arizal[3], Iwan Ernanto[1], Nadia Paramita Retno Adiati[2], Indarsih[1], Ray Novita Yasa[2], Indah Emilia Wijayanti[1], Santi Indarjani[2], Salmah[1], Septia Ulfa[3], Ari Dwi Hartanto[1], Fetty Amelia[2]

[1]Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Yogyakarta, Indonesia
[2]Department of Cryptographic Engineering, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[3]Department of Cyber Security Engineering, Politeknik Siber dan Sandi Negara, Bogor, Indonesia

Submitted: November 14th 2024; Revised: August 22nd 2025; Accepted: December 02nd 2025

Keywords:
Cryptography
Cyber threats
Quantum cryptography

Abstract The growing prevalence of cyber threats and attacks poses significant risks to the security of personal data and the integrity of sensitive information worldwide. Cryptography plays a vital role in establishing strong cybersecurity defenses, and the development of robust cryptographic algorithms is essential for protecting data against cyber-attacks. This workshop aimed to enhance participants' understanding of the mathematical foundations of cryptographic algorithms and equip them with practical skills to identify and mitigate cyber threats. It also introduced innovative educational tools, including an Augmented Reality (AR) application for teaching classical cryptography and a Game-Based URL Phishing Education application. A total of 110 participants attended and completed the pre-test. The post-test measured knowledge gained during the workshop, and an accompanying survey gathered feedback on its effectiveness and identified areas for improvement. Overall, the workshop successfully achieved its objectives by educating participants on cryptography in the Internet of Things (IoT), increasing awareness of social engineering, introducing cryptographic tools from ancient to modern times, and exploring the principles of quantum cryptography.

1. INTRODUCTION

In today's rapidly advancing technological landscape, where digital transformation is reshaping nearly every aspect of life, cybersecurity has emerged as a critical global issue (Daniel et al., 2019). It is no longer solely the responsibility of IT professionals; rather, it demands broad public awareness and understanding. The rising frequency and sophistication of cyber threats pose serious risks to personal data security and the integrity of sensitive information worldwide (von Solms & van Niekerk, 2013). As these threats continue to evolve, the need for widespread cybersecurity education and awareness becomes increasingly urgent.

In response to this challenge, a community service initiative titled "Mathematics in Cryptography and Its Applications in Cybersecurity" was developed. Implemented in the form of a workshop and training program, this initiative aims to equip participants with up-to-date knowledge and practical skills in cryptography and cybersecurity. Its primary objective is to emphasize the essential role of cryptography as a foundational component of strong cybersecurity defenses.

Cryptography is fundamentally rooted in mathematical principles, and a solid grasp of these principles is vital for designing cryptographic algorithms capable of effectively protecting data from cyberattacks (Kizielewicz & Kołodziejczyk, 2020). The workshop seeks to deepen participants' understanding of these mathematical concepts while demonstrating their real-world applications in cybersecurity. Participants explore both the theoretical foundations of cryptography and its practical use in

ISSN 2460-9447 (print), ISSN 2541-5883 (online)

*Corresponding author: Uha Isnaini
Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Sekip Utara Bulaksumur Yogyakarta 55281, Indonesia
Email: isnainiuha@ugm.ac.id

protecting digital systems.

In addition, the workshop introduces participants to innovative cybersecurity education technologies developed through collaborative research between lecturers from Universitas Gadjah Mada (UGM) and cadets from the State Cyber and Cryptography Polytechnic (Poltek SSN). Two notable tools featured in the workshop include an Augmented Reality (AR) application for teaching classical cryptography and a Game-Based URL Phishing Education application (Martín-Gutiérrez et al., 2017). These interactive tools are designed to enhance engagement and improve learning outcomes.

The AR application facilitates hands-on, immersive learning experiences that make classical cryptographic techniques easier to understand (Billinghurst & Duenser, 2012). Meanwhile, the Game URL Phishing Education application helps participants identify and avoid phishing schemes—one of the most prevalent and damaging cyber threats today (Lee et al., 2021; Sheng et al., 2010).

The overarching goal of the workshop is to cultivate a generation of individuals who are not only skilled in using technology but also capable of protecting themselves and others from cyber threats. Through a comprehensive and interactive educational approach, the workshop aims to build a resilient community that can navigate the cybersecurity challenges of an increasingly digital world.

This initiative represents a collective effort to strengthen both national and global cybersecurity ecosystems. By prioritizing education, the program contributes to fostering a culture of cybersecurity awareness and competence, ultimately helping to create a safer and more trustworthy cyberspace for all.

2. METHOD

The primary activity of this community service initiative was a workshop held on Saturday, July 27, 2024, from 08:00 AM to 01:00 PM (Western Indonesian Time). The event took place at the 7th Floor Auditorium, Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada (UGM), and was simultaneously accessible online via Zoom. The workshop was free of charge, and interested participants registered through the provided Google Form link (`ugm.id/PkMSiber2024`), with the option to attend either onsite or online. A dedicated area in front of the auditorium was also prepared for students to disseminate their research through poster presentations.

Upon arrival, participants registered and completed a pre-test consisting of 30 multiple-choice questions designed to measure their baseline knowledge of cryptography and cybersecurity. The workshop featured a series of presentations and interactive sessions led by experts in cryptography and cybersecurity. These sessions emphasized the mathematical foundations of cryptographic algorithms (Koblitz, 1994), their practical applications in cybersecurity, and the use of innovative educational tools, including the Augmented Reality (AR) application for classical cryptography instruction and the Game-Based URL Phishing Education application (Kizielewicz & Kołodziejczyk, 2020).

Alongside the main workshop sessions, a poster session was conducted in which students presented cybersecurity-related research. This session facilitated knowledge sharing and allowed participants to gain insights into ongoing research developments and innovations in the field.

At the conclusion of the workshop, participants completed a post-test and a survey. The post-test evaluated the knowledge gained during the workshop, while the survey collected feedback on the workshop's effectiveness and identified areas for improvement. Completing both the post-test and survey was required to receive an e-certificate.

Motivated by Bada & Nurse (2019), and to ensure the sustainability of this initiative, a series of follow-up webinars on cybersecurity topics was organized after the workshop. These webinars provided continued learning opportunities, reinforced key concepts introduced during the event, and highlighted new developments in cybersecurity.

Overall, the workshop aimed to strengthen participants' understanding of the mathematical principles underlying cryptographic algorithms and equip them with practical skills to identify and mitigate cyber threats. It also promoted the integration of innovative educational tools in cybersecurity learning and fostered a community of learners and researchers committed to advancing cybersecurity knowledge and practices. By combining theoretical and practical components, the workshop provided a comprehensive learning experience designed to support participants in effectively addressing cybersecurity challenges.

3. RESULT AND DISCUSSION

The series of activities conducted in this program was evaluated using the Public Satisfaction Index (IKM), based on the Regulation of the Ministry of State Apparatus Empowerment and Bureaucratic Reform Number 17 of 2017 concerning Guidelines for Compiling Public Satisfaction Surveys. The survey consisted of twelve closed-ended questions and two open-ended questions. The closed-ended questions used a Likert scale to assess participant satisfaction with facilitators, materials, and supporting activities. The open-ended questions explored additional knowledge gained and participant suggestions after attending the event. The following subsections present the results of the analysis.

3.1 Closed questions

The Descriptive analysis of the twelve closed-ended questions showed that most participants selected responses in the "good" and "very good" categories. The three aspects rated as very good, in order of highest to lower scores, were:

1. the politeness and competence of the facilitators,
2. the quality of facilities and resources used during the activities, and
3. the positive impact of the workshop materials on participants' knowledge.

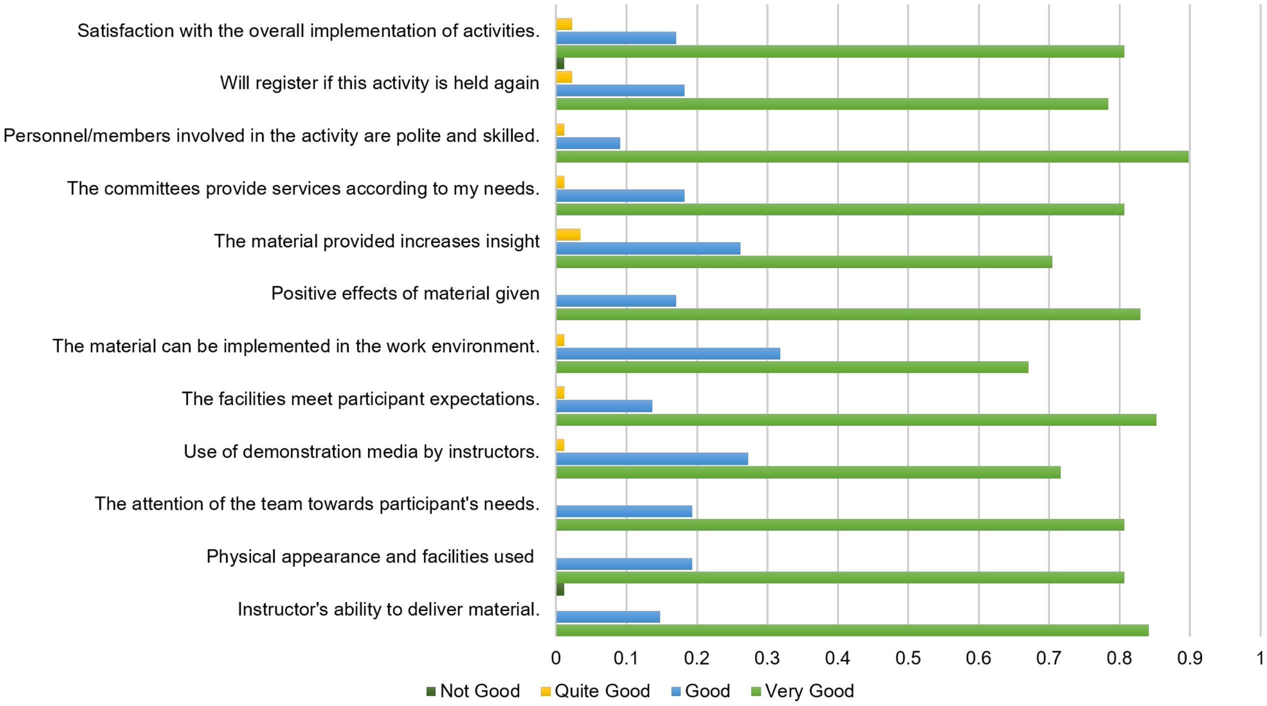

Figure 1 . Results of the survey on the implementation of the community service activities

An overall representation of the data is shown in Figure 1. Based on the conversion of the Public Satisfaction Index, applying equal weighting for each question item, the program achieved a score of 95.5 out of 100, or 3.82 on a 4-point scale, indicating a very high level of participant satisfaction.

3.2 Open questions

Descriptive analysis of the open-ended questions was conducted by identifying recurring keywords in both the "additional knowledge gained" and "suggestions" categories. For the additional knowledge category, participants most frequently mentioned gaining insights related to "cybersecurity", "cryptographic mathematics", "cryptography", "cybercrime", and "practical implementation".

Meanwhile, keywords that emerged in the suggestions category included the need for "improvement of materials," "additional time," "online involvement," and "practical simulation." These keywords reflect participants' expectations for deeper content, extended workshop duration, greater opportunities for remote engagement, and more hands-on activities.

3.3 Post-test result

3.3.1 Respondent characteristics

Based on Figure 2, a total of 110 respondents attended the workshop and completed the pre-test. The majority of participants were students, accounting for 43.6% of all respondents. Lecturers made up 30%, followed by teachers at 10.9%, general participants at 10%, and the remaining 5.5% consisting of other student categories.

Based on Figure 3, a total of 89 respondents completed the post-test questions related to the workshop material. Meanwhile, Figure 4 shows that 51 respondents completed the post-test questions on the Museum of Sandi material, with students still representing the largest proportion of respondents.

3.3.2 Results of pre-test and post-test analysis

Although the initial number of respondents in this survey was relatively large, only 43 respondents met the required data quality criteria after the data screening and validation process. The results of the pre-test and post-test analysis using the paired t-test (Walpole, 2012) are presented in Figure 2, Figure 3, and Figure 4.

Based on Table 1, the average post-test score is higher than the pre-test score, indicating that participants' understanding improved after the activity (Bada & Nurse, 2019). Furthermore, a significance test was conducted, and the results are presented in Table 2.

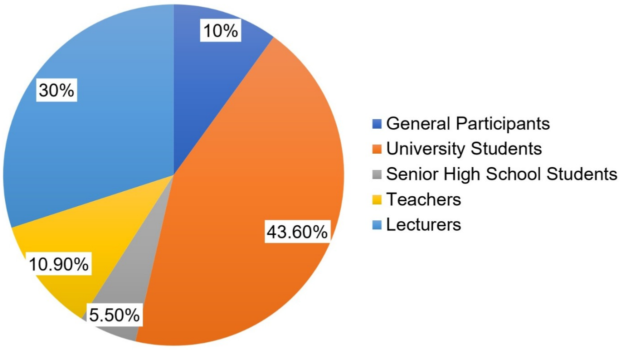

Figure 2 . Pie chart of respondents who filled out the pre-test questions

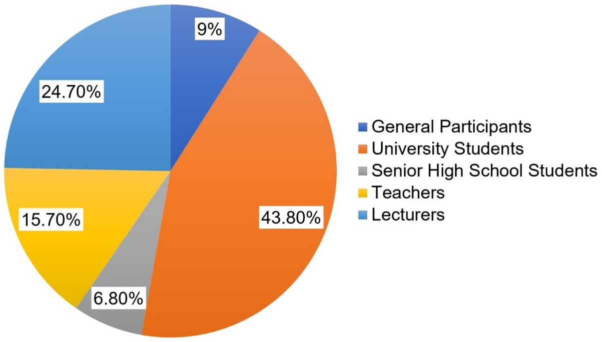

Figure 3 . Pie chart of respondents who filled out the post-test questions for workshop material

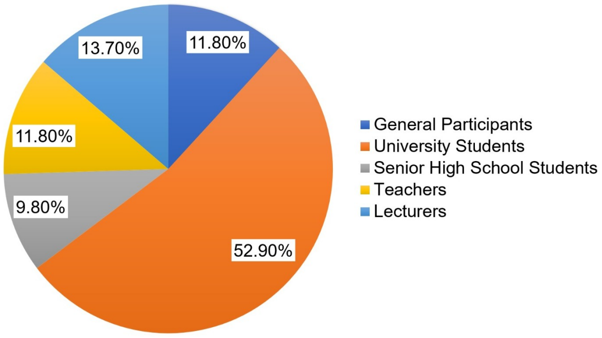

Figure 4 . Pie chart of respondents who filled out the post-test questions on the Museum of Sandi material

The p-value of 0.027 obtained from the analysis is smaller than $\alpha = 0.05$, indicating strong statistical evidence to reject the null hypothesis. This result confirms that there was a statistically significant increase in participants' understanding after the activity, demonstrating that the workshop was effective in enhancing knowledge (Daniel et al., 2019).

Table 1 . Descriptive statistics

Sample	N	Mean	St Dev	SE Mean
posttest	43	99.53	16.29	2.48
pretest	43	95.00	18.48	2.82

Table 2 . Significance test

Criteria	Value
Null hypothesis	$H^0 : \mu_{\text{diff}} = 0$
Alternative hypothesis	$H_1 : \mu_{\text{diff}} > 0$
t-Value	1.98
p-Value	0.027

Significancy (α<0.05)

4. CONCLUSION

After conducting the workshop on mathematics in cryptography and its applications, it was observed from the pre-test results that participants possessed a basic familiarity with the subject. However, after receiving the workshop materials, engaging in discussions, and completing the assigned tasks, participants showed a substantial improvement in their comprehension of mathematical concepts in cryptography and their applications in cybersecurity. Most participants performed exceptionally well in the post-test, with many answering nearly all questions correctly.

Based on these outcomes, it can be concluded that the workshop was successful in achieving its objectives. Participants gained knowledge about cryptography in the Internet of Things (IoT), increased their awareness of social engineering, were introduced to cryptographic tools from ancient to modern times, and explored foundational concepts in quantum cryptography. Additionally, participants experienced the historical process of sending and receiving secret messages during their visit to the Museum of Sandi.

ACKNOWLEDGMENT

The authors wish to extend sincere appreciation to the National Cyber and Crypto Institute, the Faculty of Science at Universitas Gadjah Mada, and the Museum of Sandi for their invaluable contributions to the workshop on Mathematics in Cryptography and Its Applications in Cybersecurity. Their support greatly enriched the learning experience and enhanced participants' knowledge. It is hoped that the knowledge shared will be highly beneficial and bring lasting value for all involved.

CONFLICT OF INTERESTS

The authors declare that there are no conflicts of interest.

REFERENCES

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security, 27*, 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Billinghurst, M. & Duenser, A. (2012). Augmented reality in the classroom. *Computer, 45*, 56 – 63. https://doi.org/10.1109/MC.2012.111

Daniel, R. M., Rajsingh, E. B., & Silas, S. (2019). An efficient eCK secure certificateless authenticated key agreement scheme with security against public key replacement attacks. *Journal of Information Security and Applications, 47*, 156-172. https://doi.org/10.1016/j.jisa.2019.05.003

Kizielewicz, B., & Kołodziejczyk, J. (2020). Effects of the selection of characteristic values on the accuracy of results in the COMET method. *Procedia Computer Science, 176*, 3581-3590. https://doi.org/10.1016/j.procs.2020.09.028

Koblitz, N. (1994). *A course in number theory and cryptography*. Springer Science & Business Media.

Lee, D., Rothstein, R., Dunford, A., Berger, E., Rhoads, J. F., & DeBoer, J. (2021). "Connecting online": The structure and content of students' asynchronous online networks in a blended engineering class. *Computers & Education, 163*, 104082. https://doi.org/10.1016/j.compedu.2020.104082

Martín-Gutiérrez, J., Mora, C. E., Añorbe-Díaz, B., & González-Marrero, A. (2017). Virtual technologies trends in education. *Eurasia Journal of Mathematics, Science and Technology Education, 13*, 469-486. https://doi.org/10.12973/eurasia.2017.00626a

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. *CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382. https://doi.org/10.1145/1753326.1753383

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.https://doi.org/10.1016/j.cose.2013.04.004

Walpole, R. E. (2012). *Pengantar statistika (9th ed.)*. Jakarta: PT Gramedia Utama.