

Workshop Interaktif Kriptografi dan Steganografi untuk Meningkatkan Literasi Keamanan Informasi Siswa SMK

Yasir Hasan

STMIK Mulia Darma, Rantauprapat, Indonesia

Email: yasirhasan.kom@gmail.com

ABSTRACT

The rapid advancement of digital technology has increased the importance of information security literacy, particularly among vocational high school (SMK) students who are prospective professionals in the field of information technology. However, knowledge of cryptography and steganography remains limited and has not been systematically integrated into vocational education. This community service activity aimed to improve students' understanding and practical skills in implementing basic cryptographic and steganographic techniques through an interactive workshop. The activity was conducted face-to-face using a practice-based learning approach (learning by doing), which consisted of four stages: pre-workshop, workshop implementation, post-workshop evaluation, and follow-up activities. Learning methods included lectures, demonstrations, hands-on practice, collaborative discussions, and evaluation through pre-test and post-test. The workshop involved 12 vocational high school students participating in industrial internships at Universitas Budi Darma. The evaluation results showed a significant improvement in participants' learning outcomes, with the average score increasing from 43.00 on the pre-test to 80.50 on the post-test, resulting in an average gain score of 37.50 points. In addition, all participants successfully completed practical exercises involving encryption, decryption, message embedding, and message extraction. These findings indicate that an interactive workshop based on direct practice effectively enhances students' information security literacy and fundamental technical competencies in cryptography and steganography. This program can serve as an alternative model for strengthening cybersecurity literacy in vocational education through sustainable practice-oriented training.

Keywords: *community service; cryptography; steganography; information security; vocational high school.*

Copyright © 2026 Marsipature Hutanabe.

All rights reserved is Licensed under a [Creative Commons Attribution- NonCommercial 4.0 International License \(CC BY-NC 4.0\)](#)

PENDAHULUAN

Perkembangan teknologi digital telah mendorong peningkatan penggunaan internet, komputasi awan, perangkat bergerak, dan berbagai layanan berbasis data dalam aktivitas sehari-hari. Di sisi lain, meningkatnya pertukaran informasi digital juga diikuti oleh bertambahnya ancaman keamanan siber seperti pencurian data, manipulasi informasi, penyadapan komunikasi, serta pelanggaran privasi. Kondisi tersebut menjadikan keamanan informasi sebagai salah satu aspek penting yang harus dipahami oleh masyarakat, khususnya generasi muda yang akan memasuki dunia kerja di bidang teknologi informasi. Oleh karena itu, peningkatan literasi keamanan informasi sejak jenjang pendidikan menengah menjadi langkah strategis dalam mempersiapkan sumber daya manusia yang mampu menghadapi tantangan transformasi digital (Aslam et al., 2022; Michaylov & Sarmah, 2024).

Kriptografi dan steganografi merupakan dua teknik yang banyak digunakan untuk menjaga kerahasiaan informasi digital. Kriptografi berfungsi mengubah informasi menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu, sedangkan steganografi menyembunyikan keberadaan informasi di dalam media digital seperti gambar, audio, maupun video sehingga keberadaan pesan tidak mudah diketahui pihak lain. Kombinasi kedua teknik tersebut mampu memberikan lapisan keamanan yang lebih baik dibandingkan

Workshop Interaktif Kriptografi dan Steganografi untuk Meningkatkan Literasi Keamanan Informasi Siswa SMK – Yasir Hasan

penggunaan salah satu metode secara terpisah. Berbagai penelitian menunjukkan bahwa penerapan kriptografi dan steganografi telah digunakan pada berbagai bidang, seperti komunikasi digital, penyimpanan data, transaksi elektronik, hingga sistem keamanan informasi modern (Ghoul et al., 2023; Pekerti et al., 2024; Subramanian et al., 2021).

Meskipun penting, materi mengenai keamanan informasi, khususnya kriptografi dan steganografi, masih belum banyak diperkenalkan secara praktis kepada siswa Sekolah Menengah Kejuruan (SMK). Pembelajaran di SMK umumnya lebih berfokus pada penguasaan perangkat keras, jaringan komputer, maupun pemrograman dasar, sedangkan kompetensi di bidang keamanan siber masih menjadi materi pendukung. Berdasarkan hasil diskusi awal dengan guru pendamping serta observasi kebutuhan peserta, sebagian besar siswa telah memiliki kemampuan dasar dalam penggunaan komputer, namun belum memahami konsep enkripsi, penyembunyian data, maupun penerapannya dalam menjaga keamanan informasi digital. Kondisi ini menunjukkan perlunya kegiatan pembelajaran berbasis praktik yang mampu meningkatkan pengetahuan sekaligus keterampilan siswa dalam bidang keamanan informasi.

Workshop dipilih sebagai metode pengabdian karena memberikan kesempatan kepada peserta untuk mempelajari konsep sekaligus mempraktikkan secara langsung teknik kriptografi dan steganografi. Pendekatan pembelajaran berbasis praktik (*learning by doing*) terbukti mampu meningkatkan keterlibatan peserta, memperkuat pemahaman konsep, serta mengembangkan kemampuan pemecahan masalah melalui pengalaman langsung. Dalam kegiatan ini peserta tidak hanya memperoleh materi teoritis, tetapi juga melakukan praktik enkripsi, dekripsi, penyisipan pesan ke dalam media digital, serta ekstraksi kembali informasi menggunakan perangkat lunak sederhana sehingga proses pembelajaran menjadi lebih kontekstual dan aplikatif.

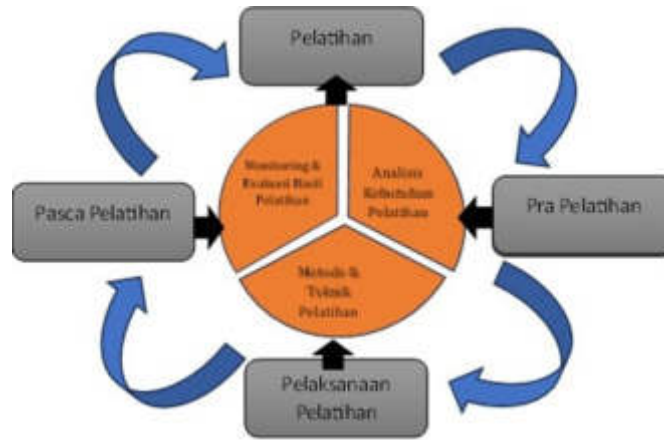
Berdasarkan kondisi tersebut, kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan literasi keamanan informasi serta keterampilan dasar siswa SMK dalam menerapkan kriptografi dan steganografi melalui workshop interaktif berbasis praktik. Kegiatan ini diharapkan dapat memberikan pengalaman belajar yang relevan dengan kebutuhan industri digital sekaligus menjadi salah satu upaya penguatan kompetensi keamanan siber pada pendidikan vokasi. Selain meningkatkan pemahaman peserta terhadap konsep keamanan data, hasil kegiatan ini juga diharapkan dapat menjadi model pelatihan yang dapat diadopsi oleh sekolah dalam mengembangkan program pembelajaran keamanan informasi secara berkelanjutan.

METODE

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk workshop interaktif yang bertujuan meningkatkan literasi keamanan informasi melalui pembelajaran kriptografi dan steganografi bagi siswa Sekolah Menengah Kejuruan (SMK). Kegiatan dilaksanakan secara tatap muka di lingkungan Universitas Budi Darma dengan melibatkan siswa SMK yang sedang melaksanakan Praktik Kerja Industri (Prakerin). Peserta berasal dari SMK Multi Karya Medan, SMK Tamansiswa Medan, dan SMK Yapim Biru-Biru Deli Serdang. Pendekatan yang digunakan mengintegrasikan penyampaian materi, demonstrasi, praktik langsung (*learning by doing*), diskusi interaktif, serta evaluasi menggunakan pre-test dan post-test untuk mengukur peningkatan pemahaman peserta.

Metode pelaksanaan kegiatan mengadopsi siklus pelatihan yang terdiri atas empat tahapan utama, yaitu pra-workshop, pelaksanaan workshop, pasca-workshop, dan evaluasi serta pelatihan lanjutan, sebagaimana ditunjukkan pada Gambar 1. Pendekatan ini dirancang

agar proses pembelajaran berlangsung secara sistematis, mulai dari identifikasi kebutuhan peserta hingga evaluasi keberhasilan kegiatan dan penyusunan tindak lanjut.



Gambar 1. Siklus Perencanaan Pelatihan

1. Tahap Pra-Workshop

Tahap awal difokuskan pada identifikasi kebutuhan peserta melalui diskusi dengan pihak sekolah mitra, guru pendamping, serta observasi terhadap kemampuan awal siswa. Hasil identifikasi menunjukkan bahwa sebagian besar peserta telah memiliki pengetahuan dasar mengenai komputer, namun belum memahami konsep keamanan informasi, khususnya kriptografi dan steganografi. Berdasarkan hasil tersebut, tim pengabdian menyusun kurikulum pelatihan yang menitikberatkan pada pembelajaran berbasis praktik dengan komposisi sekitar 30% teori dan 70% praktik. Selain itu, disiapkan berbagai perangkat pendukung berupa modul pelatihan, media presentasi, perangkat lunak pendukung, contoh data, serta instrumen evaluasi yang digunakan selama pelaksanaan workshop.

2. Tahap Pelaksanaan Workshop

Pelaksanaan workshop dilakukan secara tatap muka selama satu hari melalui beberapa sesi pembelajaran yang saling terintegrasi. Sesi pertama berisi penyampaian konsep dasar keamanan informasi, pengenalan kriptografi dan steganografi, serta demonstrasi penggunaan perangkat lunak yang digunakan dalam proses enkripsi, dekripsi, dan penyembunyian pesan.

Selanjutnya peserta mengikuti sesi praktik secara langsung dengan menerapkan algoritma kriptografi sederhana dan teknik steganografi menggunakan media digital yang telah disediakan. Peserta melakukan latihan mengenkripsi pesan, menyisipkan pesan ke dalam citra digital, melakukan ekstraksi pesan, serta mendekripsi kembali informasi yang telah diamankan. Selama proses praktik, tim pengabdian memberikan pendampingan sehingga seluruh peserta dapat menyelesaikan setiap tahapan sesuai prosedur. Pendekatan learning by doing dipilih untuk meningkatkan pemahaman konseptual sekaligus keterampilan teknis peserta dalam mengimplementasikan keamanan informasi.

3. Tahap Pasca-Workshop

Setelah seluruh sesi pelatihan selesai, dilakukan evaluasi terhadap capaian pembelajaran peserta. Evaluasi dilaksanakan melalui pemberian post-test serta penugasan praktik untuk mengetahui kemampuan peserta dalam menerapkan teknik

kriptografi dan steganografi. Hasil evaluasi kemudian didokumentasikan sebagai bahan penyusunan laporan kegiatan dan diseminasi hasil pengabdian kepada masyarakat melalui publikasi ilmiah.

4. Tahap Evaluasi dan Pelatihan Lanjutan

Tahap akhir dilakukan melalui pengumpulan umpan balik dari peserta maupun guru pendamping mengenai efektivitas pelaksanaan workshop. Masukan tersebut digunakan sebagai dasar penyempurnaan materi, metode pembelajaran, dan penyusunan program pelatihan lanjutan. Data hasil pre-test dan post-test dianalisis menggunakan statistik deskriptif yang meliputi nilai rata-rata, median, nilai tertinggi, nilai terendah, standar deviasi, serta nilai peningkatan (gain score). Analisis ini digunakan untuk menggambarkan perubahan kemampuan peserta setelah mengikuti workshop.

HASIL DAN PEMBAHASAN

Hasil Pelaksanaan Kegiatan

Workshop interaktif kriptografi dan steganografi dilaksanakan di lingkungan Universitas Budi Darma dengan melibatkan siswa SMK yang sedang melaksanakan Praktik Kerja Industri (Prakerin). Peserta berasal dari SMK Multi Karya Medan, SMK Tamansiswa Medan, dan SMK Yapim Biru-Biru Deli Serdang yang memiliki latar belakang kompetensi keahlian di bidang teknologi informasi dan jaringan komputer. Pelaksanaan kegiatan berlangsung secara tatap muka selama satu hari dengan pendekatan pembelajaran yang mengombinasikan penyampaian teori, demonstrasi, praktik langsung, dan diskusi interaktif.

Pada sesi awal, peserta memperoleh materi mengenai konsep dasar keamanan informasi, prinsip kerja kriptografi dan steganografi, serta contoh penerapan kedua teknik tersebut dalam pengamanan data digital. Penyampaian materi dilakukan menggunakan media presentasi visual yang disertai demonstrasi sehingga peserta memperoleh gambaran mengenai proses enkripsi, dekripsi, penyisipan pesan, dan ekstraksi pesan pada media digital.

Selanjutnya peserta mengikuti sesi praktik menggunakan perangkat komputer yang telah disediakan. Pada tahap ini peserta menerapkan algoritma kriptografi sederhana, melakukan penyisipan pesan ke dalam citra digital, serta mengembalikan kembali informasi yang telah diamankan. Pendekatan *learning by doing* memberikan kesempatan kepada peserta untuk memahami konsep secara langsung melalui pengalaman praktik sehingga proses pembelajaran menjadi lebih aktif dan aplikatif.



Gambar 2. Pembukaan Sesi Teori



Gambar 3. Peserta Workshop Mengikuti Praktik Kriptografi dan Steganografi

Kegiatan berlangsung secara interaktif yang ditunjukkan oleh tingginya partisipasi peserta selama sesi diskusi maupun praktik. Peserta mampu mengikuti setiap tahapan pelatihan mulai dari proses enkripsi, penyisipan pesan, ekstraksi pesan, hingga dekripsi sesuai prosedur yang diberikan. Kondisi tersebut menunjukkan bahwa metode pembelajaran berbasis praktik mampu meningkatkan keterlibatan peserta selama kegiatan berlangsung.

Hasil Evaluasi Pembelajaran

Untuk mengetahui efektivitas workshop, dilakukan evaluasi menggunakan pre-test sebelum pelatihan dan post-test setelah seluruh materi serta praktik selesai dilaksanakan.

Tabel 1. Data Hasil Evaluasi Workshop Kriptografi dan Steganografi

No.	Nama Siswa	Nilai Pra-Pelatihan (0-100)	Nilai Pasca-Pelatihan (0-100)	Peningkatan (Gain)
1	Siswa 1	45	82	+37
2	Siswa 2	38	76	+38
3	Siswa 3	52	88	+36
4	Siswa 4	40	79	+39
5	Siswa 5	35	74	+39
6	Siswa 6	48	85	+37
7	Siswa 7	42	80	+38
8	Siswa 8	50	86	+36
9	Siswa 9	36	75	+39
10	Siswa 10	44	81	+37
11	Siswa 11	39	77	+38
12	Siswa 12	47	83	+36
Rata-rata		43,00	80,50	+37,50

Berdasarkan Tabel 1, seluruh peserta mengalami peningkatan hasil belajar setelah mengikuti workshop. Nilai rata-rata pre-test sebesar 43,00 meningkat menjadi 80,50 pada post-test, dengan rata-rata peningkatan (gain score) sebesar 37,50 poin. Seluruh peserta menunjukkan peningkatan nilai antara 36-39 poin, yang mengindikasikan bahwa materi dapat dipahami secara relatif merata oleh seluruh peserta tanpa adanya kesenjangan hasil belajar yang signifikan.

Peserta dengan nilai awal terendah juga mampu menunjukkan peningkatan yang tinggi setelah mengikuti workshop. Hal ini menunjukkan bahwa pendekatan pembelajaran berbasis praktik tidak hanya efektif bagi peserta dengan kemampuan awal yang baik, tetapi juga

mampu meningkatkan pemahaman peserta yang sebelumnya belum mengenal konsep keamanan informasi.

Analisis Statistik Deskriptif

Tabel 2. Rekapitulasi Statistik Deskriptif Hasil Workshop

Statistik	Pra-Pelatihan	Pasca-Pelatihan	Gain
Nilai Tertinggi	52	88	39
Nilai Terendah	35	74	36
Rata-rata	43,00	80,50	37,50
Median	43,00	81,00	37,50
Standar Deviasi	5,78	4,52	1,17

Berdasarkan Tabel 2, rata-rata nilai peserta meningkat dari 43,00 menjadi 80,50, sedangkan nilai median meningkat dari 43,00 menjadi 81,00. Standar deviasi hasil post-test sebesar 4,52 dan standar deviasi gain score sebesar 1,17 menunjukkan bahwa peningkatan hasil belajar terjadi secara relatif konsisten pada seluruh peserta. Nilai standar deviasi yang rendah mengindikasikan bahwa metode workshop memberikan dampak yang cukup merata terhadap kemampuan peserta meskipun kemampuan awal mereka berbeda-beda.

Pembahasan

Peningkatan nilai pre-test dan post-test menunjukkan bahwa workshop interaktif memberikan kontribusi positif terhadap peningkatan literasi keamanan informasi peserta. Pendekatan pembelajaran yang mengombinasikan ceramah, demonstrasi, praktik langsung, dan diskusi memungkinkan peserta memperoleh pengalaman belajar yang lebih kontekstual dibandingkan pembelajaran berbasis teori semata. Melalui praktik secara langsung, peserta tidak hanya memahami konsep dasar kriptografi dan steganografi, tetapi juga mampu mengimplementasikan teknik tersebut pada media digital.

Hasil kegiatan ini sejalan dengan penelitian Subramanian et al. (2021) yang menyatakan bahwa pemahaman terhadap steganografi akan lebih efektif apabila disertai implementasi langsung pada media digital. Selain itu, Aslam et al. (2022) juga menjelaskan bahwa penguasaan teknik kriptografi dan steganografi merupakan salah satu kompetensi penting dalam meningkatkan keamanan informasi digital. Kedua temuan tersebut memperkuat bahwa pelatihan berbasis praktik dapat menjadi pendekatan yang efektif dalam meningkatkan kompetensi keamanan siber bagi siswa SMK.

Selain peningkatan aspek kognitif yang ditunjukkan melalui hasil evaluasi, kegiatan ini juga memberikan pengalaman praktis kepada peserta dalam menyelesaikan kasus sederhana yang berkaitan dengan pengamanan data digital. Kemampuan melakukan proses enkripsi, penyisipan pesan, ekstraksi, dan dekripsi menunjukkan bahwa peserta tidak hanya memahami teori, tetapi juga telah memiliki keterampilan dasar yang dapat menjadi bekal awal dalam mempelajari keamanan siber secara lebih mendalam.

Secara keseluruhan, workshop ini memberikan manfaat bagi peserta dalam meningkatkan literasi keamanan informasi sekaligus memperkenalkan bidang keamanan siber sebagai salah satu kompetensi yang relevan dengan kebutuhan dunia industri digital. Model pelatihan yang digunakan berpotensi diterapkan pada kegiatan serupa di sekolah lain sebagai salah satu bentuk penguatan kompetensi siswa di bidang teknologi informasi.

KESIMPULAN

Workshop interaktif kriptografi dan steganografi berhasil meningkatkan literasi keamanan informasi serta keterampilan dasar siswa SMK dalam mengamankan data digital. Peningkatan tersebut ditunjukkan oleh kenaikan rata-rata nilai peserta dari 43,00 pada pre-test menjadi 80,50 pada post-test dengan rata-rata gain score sebesar 37,50 poin. Pendekatan learning by doing yang mengombinasikan penyampaian materi, demonstrasi, dan praktik langsung terbukti efektif dalam meningkatkan pemahaman peserta, sehingga model pelatihan ini berpotensi diterapkan sebagai salah satu upaya penguatan literasi keamanan siber di lingkungan pendidikan vokasi

REFERENSI

- Aslam, M. A., Rashid, M., Azam, F., Abbas, M., Rasheed, Y., Alotaibi, S. S., & Anwar, M. W. (2022). Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review. *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022*, 32-38. <https://doi.org/10.1109/ICCIT52419.2022.9711628>
- Cyber Academy Indonesia. (2024, March 1). Mengenal Capture The Flag Dalam Cyber Security. Cyber Academy Indonesia. <https://www.cyberacademy.id/blog/mengenal-capture-the-flag-dalam-cyber-security>
- Ghoul, S., Sulaiman, R., Shukur, Z., & Malaysia UKM Bangi, K. (2023). A Review on Security Techniques in Image Steganography. *IJACSA International Journal of Advanced Computer Science and Applications*, 14(6). www.ijacsa.thesai.org
- Hasan, Y. (2025). Steganography Test for Exif Metadata on JPEG Files With AES-256 Encryption for Secret Message Security. *INFOKUM*, 13, 1562-1578. <https://doi.org/10.58471/infokum.v13i05>
- L Nikhitha V S Arjun Naveen Chandra Gowda, A. B. (2023). Survey of applications, advantages, and comparisons of AES encryption algorithm with other standards. *International Journal of Computational Learning & Intelligence*, 2(2), 87-98. www.milestoneresearch.in
- Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. *Journal of Cyber Security Technology*, 1-27. <https://doi.org/10.1080/23742917.2024.2304441>
- Pekerti, A. A., Sasongko, A., & Indrayanto, A. (2024). Secure End-to-End Voice Communication: A Comprehensive Review of Steganography, Modem-Based Cryptography, and Chaotic Cryptography Techniques. *IEEE Access*, 12, 75146-75168. <https://doi.org/10.1109/ACCESS.2024.3405317>
- Saabith, A. L. S., Vinothraj, T., & Fareez, M. (2020). POPULAR PYTHON LIBRARIES AND THEIR APPLICATION DOMAINS. *International Journal of Advance Engineering and Research Development*, 7(11). <https://www.researchgate.net/publication/349828209>
- Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, 9, 23409-23423. <https://doi.org/10.1109/ACCESS.2021.3053998>
- Sunardi, S., Riadi, I., & Akbar, M. H. (2020). Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics. *Jurnal Nasional Teknologi Dan Sistem Informasi*, 6(1), 1-8. <https://doi.org/10.25077/teknosi.v6i1.2020.1-8>