

Pelatihan Kriptografi Dasar dan Edukasi Keamanan Siber di SMA Muhammadiyah 15 Slipi

Rudi Prasetya^{1*}, Andri², Sepniyanti³

^{1,2} Teknik Informatika, Universitas Indraprasta PGRI

* E-mail: rudiprasetya1@gmail.com, andriecitra@gmail.com, sepniyanti@gmail.com

Abstrak

Sejarah Artikel

Diterima : 18 November 2024

Disetujui : 25 Maret 2025

Dipublikasikan :15 April 2025

Kata kunci: Keamanan Siber,
Edukasi, Dasar Kriptografi

Kemajuan teknologi digital memberikan dampak yang signifikan pada keamanan siber, yang memerlukan pemahaman masyarakat akan risiko dan strategi mitigasi yang relevan ke dalam aktivitas berinternet. Untuk memberikan kontribusi pada peningkatan literasi keamanan siber, Universitas Indraprasta PGRI melaksanakan Kegiatan Pengabdian kepada Masyarakat dengan topik edukasi keamanan siber kepada siswa SMA Muhammadiyah 15 Slipi. Siswa dan siswi SMA merupakan kelompok rentan karena minimnya pemahaman akan ancaman cybercrime. Kegiatan yang dilakukan meliputi pengenalan konsep dasar keamanan siber dan pelatihan keterampilan dasar kriptografi sebagai upaya melindungi data pribadi. Metode pelaksanaan yang dilakukan adalah tatap muka dan keterlibatan siswa-siswi pada sesi ceramah dan pelatihan langsung dengan pengguna berbasis video conference, sehingga memungkinkan interaksi face to face dan berbeda secara aktif antara instruktur dengan siswa. Dari kegiatan tersebut diperoleh hasil bahwa keseluruhan peserta memiliki pemahaman tambahan tentang risiko serta kesiapsiagaannya, serta pemahaman praktis relevan untuk menangkal ancaman di dunia digital. Oleh karena itu, melalui PKM ini diharapkan kesadaran berinternet yang aman menjadi terbentuk, terutama pada generasi muda, sebagai upaya preventif dalam menghadapi ancaman yang semakin kompleks.

Abstract

Keywords: Cybersecurity,
Education, Basic
Cryptography

The advancement of digital technology has significantly impacted cybersecurity, requiring public awareness of risks and relevant mitigation strategies in online activities. To contribute to increasing cybersecurity literacy, Universitas Indraprasta PGRI conducted a Community Service Program focused on cybersecurity education for students at SMA Muhammadiyah 15 Slipi. High school students are considered a vulnerable group due to limited understanding of cybercrime threats. This program included an introduction to basic cybersecurity concepts and training in fundamental cryptographic skills to protect personal data. The implementation method involved in-person interaction, with students participating in lectures and hands-on training sessions conducted via video conference, allowing for active, face-to-face engagement between instructors and students. The results of this program indicated that participants gained additional understanding of cybersecurity risks, enhanced preparedness, and practical knowledge relevant to countering digital threats. Therefore, through this community service initiative, it is hoped that secure internet practices will be established, particularly among the younger generation, as a preventive measure against increasingly complex cyber threats.

PENDAHULUAN

Perkembangan teknologi memberikan perubahan besar bagi manusia, termasuk di seluruh aspek kehidupan yang menyediakan banyak kemudahan. Informasi dan pengetahuan menjadi semakin mudah di akses, diperoleh, dan disebar luaskan. Ditengah kemajuan tersebut terdapat kekhawatiran mengenai degradasi karakter dan *value of human being* Dalam era digital ini, pengembangan *value-character* menjadi sangat penting, terutama empati dan toleransi yang harus dikembangkan bersamaan dengan kompetensi *think critical, innovative, dan creative*. Hal ini disebabkan untuk mengintegrasikan ruang maya dengan ruang fisik sekaligus, Sehingga pada lowongan kerja di masa depan pekerjaan dan aktivitas seseorang akan lebih di tengarai dengan *human centered* dengan tekonologi, yang artinya kebutuhan manusia merupakan tujuan dari pengembangan selaku manusia (Sari & Utami, n.d.). Masyarakat diharapkan mampu mengekstrapolasi data tingkat lanjut, termasuk tetapi tidak terbatas pada kriptografi dasar serta edukasi keamanan siber, guna mengintegrasikan sektor-sektor industri dan budaya. Masyarakat dapat dengan demikian mendorong inovasi multi-sektoral, tidak hanya dalam rangka pemanfaatan teknologi namun juga dalam pengembangan paradigma yang mendukung interkoneksi antara sektor. Namun demikian, masyarakat ini tetap memikirkan kebutuhan akan perlindungan data serta informasi, dan berupaya mempraktikkan keamanan siber yang baik (Dr. Amiruddin, S.Kom. et al., 2023). Masyarakat yang diharapkan terbentuk ke depan adalah masyarakat yang memegang erat prinsip simbiosis antara manusia dan alam, dengan fokus pada keberlanjutan dalam setiap ranah kehidupan, termasuk tapi tidak terbatas pada ranah digital. *Ecosystem* ini dibangun untuk menciptakan sistem yang efisien yang tidak hanya memfasilitasi kegiatan ekonomi, sosial serta budaya, namun memprioritaskan keamanan informasi serta kerahasiaannya. Diharapkan bahwa melalui aplikasi *data-level* yang lebih tingik dan edukasi kriptografi dan keamanan siber, masyarakat di masa depan dapat mencapai pembangunan berkesinambungan *Goals* sambil menciptakan keseimbangan harmonis antara kebutuhan manusia, teknologi serta alam (Dr. Siti Kurnia Rahayu, S.E., M.Ak., n.d.).

Dampak dari setiap inovasi yang baru diperkenalkan selalu akan menyertainya. Salah satunya adalah masalah yang baru muncul terkait dengan keamanan, keamanan siber menjadi tantangan terberat lainnya seiring perkembangan sistem berbasis data (Dr. Sulartopo, S.Pd., n.d.). Sebagian besar informasi yang kita akses sekarang hampir seluruhnya berdasarkan basis data yang terkait dengan sistem digital, hal ini menyebabkan banyak informasi yang bisa diakses oleh publik karena disimpan di internet. Keamanan siber adalah serangkaian tindakan yang diambil untuk melindungi informasi dari bentuk kelihatannya dari dunia maya atau virus digital. Proses ini memungkinkan pencegahan gangguan pada rahasia akibat serangan atau akses ke data tanpa seizin kita. Karena inovasi desentralisasi data kini, kebutuhan keamanannya menampakkan peningkatan dengan sistem kuat pada data dasar. Oleh karena desain kuat dalam organ tunggal yang sering kali

sulit dilakukan, masih ada banyak tantangan yang mengemuka karena hal itu (Naskah Akademik Rancangan Undang Undang Tentang Kesehatan, 2023). Fitur *cybercrime* khusus yang mengancam masyarakat terdiri dari Social Media *Cybercrimes*, tindakan kriminal multi-sektor di media sosial yang ditimbulkan oleh pencurian data, penipuan, dan merusak reputasi. Penerapan kebijakan yang ketat keamanan data dan kesadaran terhadap simak-menyimak data menjadi strategi yang harus dijalankan pengguna data bekerja kesadaran.

Mengingat semakin maraknya insiden *cybercrime* yang terjadi saat ini, kesadaran dan kepedulian terhadap keamanan siber harus ditingkatkan untuk mencegah terus berkembangnya ancaman-ancaman tersebut. Keamanan siber (Citra et al., 2023), yang diartikan sebagai kondisi bebas dari risiko atau bahaya, memerlukan pemahaman mendalam mengenai bentuk ancaman di ruang digital serta langkah-langkah penanganannya. Tanpa perlindungan siber yang memadai, potensi ancaman akan semakin meningkat (Dan & Terbaru, 2023). Untuk mengatasi beragam jenis ancaman siber yang kian kompleks, penting untuk memberikan edukasi dan pelatihan yang memadai, terutama bagi mereka yang masih awam dalam dunia keamanan siber. Salah satu upaya preventif yang dapat dilakukan adalah pengamanan data melalui metode enkripsi atau teknik kriptografi.

Kriptografi bukan sekadar ilmu untuk melindungi data, tetapi juga seni dalam menjaga kerahasiaan informasi (Rifai et al., n.d.). Di dalamnya terdapat algoritma-algoritma khusus yang bertujuan untuk mengubah teks biasa (plaintext) menjadi bentuk teks yang tidak terbaca atau disebut *ciphertext*. *Ciphertext* ini tidak dapat diinterpretasikan secara langsung oleh pengguna tanpa melalui proses deskripsi yang tepat. Melalui teknik enkripsi, kriptografi mampu mengonversi teks atau data umum menjadi bentuk rahasia, serta melakukan proses kebalikannya, yakni mendekripsi data yang sudah tersandi menjadi teks atau informasi yang dapat diakses kembali.

Pada proses ini, kunci rahasia berperan penting, dan semakin kompleks kunci yang digunakan, semakin tinggi pula tingkat keamanannya. Algoritma kriptografi terbagi menjadi dua jenis utama, yaitu algoritma simetris dan algoritma asimetris (Arif et al., 2023). Algoritma asimetris seperti RSA, misalnya, merupakan contoh algoritma yang menggunakan kunci publik dan kunci privat, memberikan perlindungan data yang lebih efektif dalam berbagai aplikasi keamanan siber.

Penggunaan dan akses data di kalangan siswa SMA mengalami peningkatan yang signifikan, terutama sebagai dampak dari pandemi yang mendorong pelaksanaan pembelajaran daring (Arjunanta et al., 2021). Oleh karena itu, untuk memastikan bahwa data yang diunduh maupun diunggah tetap aman dan terlindungi hak kepemilikannya, penting untuk memperkenalkan konsep keamanan siber sejak dini, khususnya kepada siswa SMA. Langkah ini akan membantu mereka memahami teknik penyimpanan dan perlindungan data secara lebih baik, sehingga mampu menjaga kerahasiaan informasi pribadi mereka.

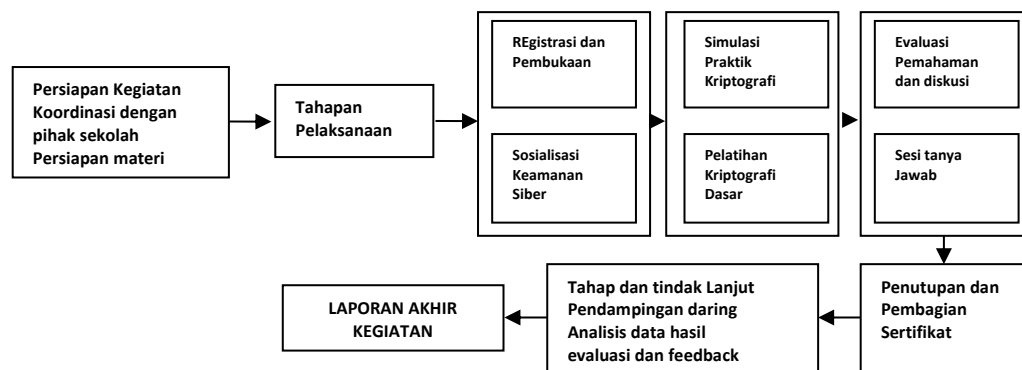
Sekolah Menengah Atas (SMA) Muhammadiyah 15, yang berlokasi di Kota Jakarta Barat, adalah sekolah berbasis Islam yang menawarkan fasilitas berkualitas tinggi dan didukung oleh

tenaga pengajar yang kompeten. Berdasarkan hasil survei di lapangan, seluruh siswa di sekolah ini secara aktif memanfaatkan fasilitas berbasis internet seperti email, media sosial, dan berbagai media pendukung lainnya untuk mendukung proses pembelajaran. Namun, penggunaan layanan-layanan tersebut belum diiringi dengan pengetahuan yang memadai mengenai keamanan data dan informasi. Sebagian besar siswa hanya memanfaatkan layanan tersebut sebagai pengguna awam, sekadar untuk kebutuhan komunikasi dasar generasi milenial. Pihak sekolah sendiri belum pernah mengadakan pelatihan khusus mengenai pengamanan data dan informasi. Padahal, mereka menyadari bahwa pemahaman mengenai keamanan data sangat penting, mengingat pesatnya perkembangan digital yang mempersempit batasan privasi di antara para pengguna teknologi.

Oleh karena itu, melalui program Pengabdian Kepada Masyarakat, Kepala Sekolah SMA Muhammadiyah 15 Jakarta mengusulkan penyelenggaraan sosialisasi mengenai keamanan siber serta pelatihan dasar kriptografi bagi para siswa. Langkah ini diharapkan dapat meningkatkan kesadaran dan keterampilan mereka dalam mencegah *cybercrime* serta membekali siswa dengan kemampuan untuk melindungi data mereka menggunakan metode kriptografi. Dalam program ini, tim PKM dari Universitas Indraprasta PGRI akan memberikan pelatihan dasar kriptografi dan edukasi tentang keamanan siber di SMA Muhammadiyah 15. Tujuan dari pelatihan dan edukasi ini adalah untuk memperluas wawasan dan meningkatkan keterampilan para siswa agar siap menghadapi perkembangan teknologi yang pesat serta mampu menjaga keamanan data digital mereka, sehingga dapat terhindar dari risiko *cybercrime* di masa depan.

METODE PELAKSANAAN

Metode ini mencakup alur yang rinci dan terstruktur, mulai dari persiapan hingga analisis hasil pelatihan, guna memastikan kegiatan berjalan efektif dan memberi dampak positif bagi siswa. Berikut adalah diagram alur metode pelaksanaan kegiatan Pengabdian Masyarakat untuk pelatihan keamanan siber dan kriptografi



Gambar 1. Diagram alur metode pelaksanaan kegiatan

Untuk menjelaskan metode pelaksanaan kegiatan pengabdian masyarakat dengan lebih lengkap, termasuk rincian waktu, durasi, lokasi, penggunaan alat dan bahan, cara kerja, serta analisis data.

1. Waktu dan Durasi Kegiatan

Waktu Pelaksanaan, Kegiatan direncanakan berlangsung selama satu hari penuh pada hari kerja, agar seluruh siswa dan tenaga pengajar dapat berpartisipasi. Durasi, Total durasi kegiatan adalah sekitar 6-7 jam, termasuk sesi istirahat dan makan siang.

2. Tempat Pelaksanaan

Lokasi, Aula atau ruang kelas besar di SMA Muhammadiyah 15 Jakarta Barat, yang dapat menampung peserta dalam jumlah banyak dengan tetap memungkinkan interaksi yang kondusif selama sesi pelatihan.

3. Penggunaan Alat dan Bahan

Alat, proyektor untuk menampilkan materi presentasi dan video edukasi, Laptop yang akan digunakan oleh nara sumber untuk presentasi dan simulasi enkripsi, Speaker audio untuk memastikan suara pembicara terdengar dengan jelas, koneksi internet mendukung materi yang berbasis daring dan simulasi penggunaan aplikasi. Bahan, modul pelatihan modul fisik atau digital yang mencakup materi keamanan siber dan dasar-dasar kriptografi. Studi kasus praktis, lembar kerja atau contoh studi kasus yang digunakan untuk latihan praktis. Kuesioner atau *Feedback Form* untuk mengumpulkan umpan balik dari peserta dan mengevaluasi pemahaman siswa setelah kegiatan. sertifikat partisipasi, sertifikat yang akan diberikan kepada peserta di akhir kegiatan.

4. Cara Kerja

Tahap persiapan, melakukan koordinasi dengan pihak sekolah mengenai waktu dan kebutuhan tempat. menyiapkan materi presentasi dan modul pelatihan yang mencakup dasar-dasar keamanan siber, jenis-jenis *cybercrime*, serta konsep dasar kriptografi. Menyusun kuesioner dan evaluasi akhir untuk mengukur pemahaman peserta. Menyiapkan alat-alat dan memastikan ketersediaan fasilitas teknis, seperti proyektor dan koneksi internet. Tahap pelaksanaan, registrasi dan pembukaan registrasi peserta, diikuti dengan sambutan dari pihak sekolah dan tim pengabdian masyarakat. sosialisasi keamanan siber, sesi penyampaian materi dasar mengenai keamanan siber, pentingnya melindungi data pribadi, dan potensi ancaman *cybercrime*. Pelatihan kriptografi dasar, penyampaian materi tentang enkripsi, dekripsi, dan penggunaan algoritma sederhana dalam melindungi data.



Gambar 2. Penyampaian materi dasar mengenai keamanan siber

Selanjutnya adalah simulasi dan latihan praktis, peserta mencoba teknik enkripsi sederhana dalam kelompok kecil, disertai diskusi tentang hasil praktik. Evaluasi, Dilakukan melalui kuis atau tes untuk menilai pemahaman peserta, diikuti sesi diskusi dan tanya jawab.



Gambar 3. Simulasi dan latihan praktis teknik enkripsi sederhana

Penutupan dan pembagian sertifikat, mengakhiri acara dengan pembagian sertifikat partisipasi kepada peserta. Tahap tindak lanjut, mengadakan sesi pendampingan daring selama satu bulan pasca pelatihan untuk menjawab pertanyaan lanjutan dari peserta dan memastikan pemahaman yang lebih mendalam.

5. Analisis Data

Data evaluasi peserta, data dari hasil tes akhir dan kuesioner dianalisis untuk menilai pemahaman siswa terkait keamanan siber dan kriptografi. *Feedback* peserta, umpan balik dari siswa akan dianalisis untuk mengukur efektivitas pelatihan dan sebagai bahan evaluasi untuk peningkatan program berikutnya. Laporan akhir, hasil analisis data evaluasi dan feedback akan dirangkum dalam laporan akhir yang diserahkan kepada pihak sekolah dan Universitas Indraprasta sebagai dokumentasi kegiatan pengabdian masyarakat.

HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMA Muhammadiyah 15 Jakarta Barat, dengan tujuan untuk meningkatkan pemahaman dan kesadaran siswa mengenai pentingnya keamanan siber serta teknik enkripsi data sebagai bentuk perlindungan terhadap ancaman *cybercrime*. Program ini dilaksanakan dengan tujuan untuk memberikan pemahaman tentang pentingnya menjaga kerahasiaan data pribadi dan memberikan keterampilan dasar dalam pengamanan data menggunakan kriptografi.

Hasil yang diperoleh dari kegiatan ini meliputi :

1. Peningkatan pemahaman tentang keamanan siber, peserta kegiatan memperoleh pemahaman dasar mengenai ancaman siber yang sering terjadi, seperti phishing, malware, dan serangan lainnya yang dapat merusak data pribadi mereka. Selain itu, peserta juga memahami pentingnya menjaga kerahasiaan informasi pribadi, baik di dunia nyata maupun dalam lingkungan digital.
2. Pelatihan kriptografi dasar, peserta dilatih untuk memahami dan mempraktikkan konsep dasar kriptografi, termasuk enkripsi dan dekripsi data menggunakan metode yang sederhana. Peserta mampu memanfaatkan teknik-teknik dasar dalam melindungi informasi pribadi mereka dari ancaman *cybercrime* yang ada di dunia maya.
3. Simulasi praktik keamanan siber, Dalam sesi latihan, peserta dilibatkan dalam simulasi nyata yang memungkinkan mereka untuk mempraktikkan langsung apa yang telah dipelajari, yaitu teknik-teknik enkripsi sederhana, serta cara mengidentifikasi dan menghindari ancaman siber.
4. Umpan balik positif, berdasarkan kuesioner yang diberikan kepada peserta, mayoritas siswa menunjukkan pemahaman yang baik terkait materi yang telah diajarkan. Banyak dari mereka yang mengaku mendapatkan wawasan baru mengenai pentingnya melindungi data pribadi mereka dari serangan siber.

Dengan hasil-hasil tersebut, kegiatan ini berhasil memenuhi tujuannya untuk memberikan pengetahuan yang berguna bagi siswa dalam menghadapi tantangan di dunia digital.

Validitas hasil pelaksanaan kegiatan ini dapat dilihat dari beberapa indikator, dengan menggabungkan berbagai data ini, validitas hasil kegiatan dapat dipastikan dengan tingkat akurasi yang tinggi, karena didasarkan pada pengukuran objektif, umpan balik peserta, serta pengamatan langsung selama praktik.

Tabel 1. Tabel Uji Validitas Untuk Mengukur Pemahaman Peserta

No	Nama Siswa	Tes Pemahaman Sebelum Kegiatan (Skor 1-10)	Tes Pemahaman Setelah Kegiatan (Skor 1-10)	Perubahan Skor (Skor Setelah - Sebelum)	Validitas/Penilaian Pemahaman
1	Sandi	4	8	4	Valid, menunjukkan peningkatan yang signifikan
2	Johan	5	9	4	Valid, menunjukkan peningkatan yang signifikan
3	Mutia	3	7	4	Valid, peningkatan moderat
4	Zahra	6	8	2	Valid, peningkatan moderat
5	Sulistyawati	2	6	4	Valid, menunjukkan peningkatan yang signifikan
6	Amanda Feb	7	9	2	Valid, peningkatan moderat
7	Ernawati	5	7	2	Valid, peningkatan moderat
8	Putra Rosli	6	9	3	Valid, menunjukkan peningkatan yang signifikan
9	Jeanda	4	8	4	Valid, menunjukkan peningkatan yang signifikan
10	Kokoy	5	8	3	Valid, peningkatan moderat

Sumber: Rudi Preasetya, dkk., 2024

Berdasarkan hasil tabel uji validitas ini, kegiatan pengabdian masyarakat dapat dinyatakan valid karena Terjadi peningkatan skor yang signifikan pada sebagian besar peserta, pemahaman peserta meningkat secara substansial setelah mengikuti pelatihan, yang mengindikasikan bahwa materi yang diberikan dapat dipahami dan diterapkan, uji validitas ini mendukung efektivitas pelatihan dalam meningkatkan kesadaran dan keterampilan peserta dalam hal pengamanan data menggunakan teknik kriptografi.

Evaluasi dan tes pemahaman peserta, pada akhir kegiatan, peserta diminta untuk mengikuti tes atau kuis yang bertujuan untuk mengukur pemahaman mereka terhadap materi yang disampaikan, seperti konsep dasar keamanan siber, jenis-jenis ancaman siber, dan teknik enkripsi dasar. Berdasarkan hasil tes, mayoritas peserta menunjukkan peningkatan pemahaman yang signifikan dibandingkan sebelum pelatihan.

Umpan balik peserta setelah kegiatan, peserta diminta untuk mengisi kuesioner yang berisi pertanyaan tentang materi yang disampaikan dan pelaksanaan kegiatan secara keseluruhan. Hasil umpan balik menunjukkan tingkat kepuasan yang tinggi, dengan banyak siswa mengungkapkan bahwa pelatihan ini sangat bermanfaat dan memberikan mereka keterampilan praktis yang dapat diterapkan dalam kehidupan digital sehari-hari.

Observasi praktik selama sesi simulasi, peserta dapat melakukan enkripsi dan dekripsi data dengan menggunakan aplikasi atau metode yang telah diajarkan. Hal ini menunjukkan bahwa mereka tidak hanya memahami konsep dasar, tetapi juga mampu mengaplikasikan teknik-teknik tersebut dalam praktik.

Diskusi dan tanya jawab sesi diskusi dan tanya jawab setelah pelatihan memberikan kesempatan bagi peserta untuk mengajukan pertanyaan lebih lanjut mengenai materi yang diajarkan. Pertanyaan-pertanyaan yang diajukan oleh peserta menunjukkan bahwa mereka telah memahami dan tertarik untuk mendalami lebih lanjut topik-topik yang berkaitan dengan keamanan siber.

PENUTUP

Sebagai penutup, kegiatan pengabdian kepada masyarakat yang diselenggarakan di SMA Muhammadiyah 15 Jakarta Barat telah menunjukkan hasil positif dalam meningkatkan pemahaman siswa tentang keamanan siber dan teknik dasar kriptografi. Program ini menjawab pertanyaan mengenai sejauh mana pemahaman siswa mengenai perlindungan data pribadi dapat ditingkatkan melalui sosialisasi dan pelatihan. Berdasarkan uji validitas yang dilakukan, terdapat peningkatan signifikan dalam skor pemahaman peserta, yang mengindikasikan bahwa metode pelatihan ini efektif dalam memberikan pengetahuan praktis dan teoretis kepada siswa terkait dengan risiko *cybercrime* dan pentingnya menjaga kerahasiaan data.

Dari hasil pelaksanaan ini, beberapa saran dapat diberikan untuk berbagai pihak terkait. Pertama, untuk pihak sekolah, disarankan agar materi terkait keamanan siber dan kriptografi dimasukkan ke dalam kurikulum tambahan atau kegiatan ekstrakurikuler. Dengan demikian, pemahaman siswa tentang pentingnya pengamanan data akan lebih terintegrasi dalam keseharian mereka, membantu mempersiapkan mereka menghadapi perkembangan teknologi yang semakin pesat. Selain itu, pihak sekolah diharapkan dapat mengadakan pelatihan lanjutan secara berkala guna memperdalam pengetahuan siswa dan mengikuti perkembangan terbaru dalam teknik pengamanan data.

Selanjutnya, bagi siswa, disarankan agar mereka terus mempraktikkan pengetahuan yang telah diperoleh dalam kehidupan sehari-hari, terutama saat berinteraksi di dunia digital. Kesadaran akan potensi ancaman siber dan cara melindungi data pribadi adalah keterampilan yang semakin penting di era digital. Dengan terus menerapkan praktik keamanan yang baik, siswa akan lebih siap dalam menghadapi tantangan teknologi di masa depan.

Terakhir, untuk institusi pendidikan tinggi, khususnya Universitas Indraprasta PGRI, diharapkan kegiatan pengabdian masyarakat semacam ini dapat terus dilanjutkan dan dikembangkan. Memperluas cakupan materi atau menjangkau sekolah-sekolah lain akan sangat bermanfaat dalam meningkatkan literasi digital di kalangan pelajar. Selain itu, kegiatan-kegiatan seperti ini juga dapat melibatkan pihak-pihak eksternal, seperti praktisi keamanan siber, yang dapat memberikan wawasan lebih dalam mengenai praktik nyata di dunia kerja.

Secara keseluruhan, kegiatan ini berhasil mencapai tujuan utamanya, yaitu meningkatkan kesadaran siswa akan pentingnya keamanan data serta memperkenalkan teknik dasar kriptografi. Harapannya, pengetahuan ini akan menjadi bekal yang berharga bagi para siswa, tidak hanya untuk melindungi data pribadi, tetapi juga sebagai landasan untuk memahami tantangan teknologi masa depan.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami sampaikan kepada seluruh pihak yang telah berkontribusi langsung dalam pelaksanaan kegiatan pengabdian masyarakat ini. Terima kasih kepada saudara Andri, M.Kom narasumber dan pakar keamanan siber yang telah memberikan wawasan dan materi pelatihan yang mendalam, serta kepada Kepala Sekola SMA Muhammadiyah 15 Bapak Sumito Supriyanto yang telah mendukung pendanaan kegiatan ini sehingga dapat berlangsung dengan lancar. Kami juga berterima kasih kepada tim pengabdian masyarakat yang bekerja sama dengan penuh dedikasi untuk mempersiapkan dan menyelenggarakan kegiatan ini. Semoga kontribusi yang diberikan dapat membawa manfaat jangka panjang bagi para siswa siswa SMA Muhammadiyah 15 Jakarta Barat dan komunitas di sekitar mereka.

DAFTAR PUSTAKA

- Naskah Akademik Rancangan Undang Undang Tentang Kesehatan, Badan Legislasi DPR RI 1 (2023).
- Arif, Z., Nurokhman, A., Studi, P., Informatika, T., & Data, K. (2023). *Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi*. 4(2), 394–405.
- Arjunanta, V., Pratama, H., & Kurniawan, S. (2021). *DAMPAK PANDEMI COVID 19 TERHADAP PROSES PEMBELAJARAN PADA PESERTA DIDIK*. 01(02), 77–90.
- Citra, Y., Desy, N. K., Pinatih, S. A., & Negara, S. P. (2023). *KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA*. 6, 1941–1949.
- Dan, K., & Terbaru, R. (2023). *Jurnal Hukum dan Kewarganegaraan*. 1(5).
- Dr. Amiruddin, S.Kom., M. T. I., Ir. Setiadi Yazid, M.Sc., P. D., Bayu Anggorojati, S.T., M.Sc., P. D., Hermawan Setiawan , S.Si., M. T., Rahmat Purwoko, S.T., M. T., Herman Kabetta, M. T., R. Budiarto Hadiprakoso, M. M. S. I., & I Komang Setia Buana, M. T. (2023). *Tinjauan Strategis Keamanan Siber Indonesia– Teknologi Cloud dan Tata Kelola Data* (M. C. Dimas Febriyan Priambodo & M. T. Septia Ulfa Sunaringtyas, S.Tr.MP., Eds.). h Politeknik Siber dan Sandi Negara Press. https://poltekssn.ac.id/wp-content/uploads/2023/07/TINJAUAN-STRATEGIS-KEAMANAN-SIBER_Teknologi-Cloud-dan-Tata-Kelola-Data.pdf
- Dr. Siti Kurnia Rahayu, S.E., M.Ak., A. C. (n.d.). *Keamanan Digital Dalam Audit Pajak : Integrasi Cyber Security dengan CRM , BDA , dan BI untuk Revolusi Compliance*.
- Dr. Sulartopo, S.Pd., M. K. (n.d.). *MANAJEMEN PERIKLANAN* (M. K. Dr. Joseph Teguh Santoso, S.Kom., Ed.). Universitas Sains & Teknologi Komputer (Universitas STEKOM). https://digi-lib.stekom.ac.id/assets/dokumen/ebook/feb_8c64c96c655ec7b34259d9a6fec2f70bcd8d2743_1652751504.pdf

- Rifai, R. Y., Christyono, Y., & Santoso, I. (n.d.). *SHAMIR ADLEMAN , DAN METODE STEGANOGRAFI UNTUK PENGAMANAN PESAN RAHASIA PADA BERKAS TEKS DIGITAL*.
- Sari, R., & Utami, E. (n.d.). *Rancangan Lowongan Kerja Online Menggunakan Metode User Centered Design (Studi Kasus : Business Placement Center STMIK AMIKOM Yogyakarta)*. 62–73.