

Mengenal kriptografi sejak dini: membangun kesadaran keamanan data pribadi

Yunita Septriana Anwar, Abdillah, Sirajudin

Program Studi Pendidikan Matematika, Jurusan Pendidikan MIPA, Universitas Muhammadiyah Mataram, Indonesia

Corresponding Author: Yunita Septriana Anwar

E-mail : yunitaseptriana@ummat.ac.id

Diterima: 24 Juni 2025 | Direvisi: 12 Juli 2025 | Disetujui: 13 Juli 2025 | Online: 15 Juli 2025

© Penulis 2025

Abstrak

Kegiatan ini bertujuan untuk memperkenalkan konsep dasar kriptografi, khususnya *Caesar Cipher* dan *Vigenère Cipher*, secara sederhana kepada siswa kelas V sebagai upaya menumbuhkan kesadaran akan pentingnya keamanan data pribadi sejak usia dini. Pelaksanaan kegiatan meliputi penyampaian materi, kerja kelompok dalam menyusun dan memecahkan sandi, serta evaluasi melalui observasi dan kuesioner. Hasil kegiatan menunjukkan antusiasme yang tinggi dari para siswa serta dukungan penuh dari pihak sekolah. Rata-rata skor penilaian kegiatan sebesar 3,6 (kategori baik), yang mencerminkan efektivitas pendekatan yang digunakan. Kegiatan ini memberikan kontribusi nyata terhadap peningkatan literasi digital siswa, sekaligus membuka peluang untuk pengembangan program lanjutan, seperti pelatihan bagi guru dan pengembangan media pembelajaran berbasis keamanan digital.

Kata kunci: kriptografi; caesar cipher; vigenère cipher; literasi digital.

Abstract

This activity aimed to introduce the basic concepts of cryptography, particularly the Caesar Cipher and Vigenère Cipher, in a simple manner to fifth-grade students as an effort to raise awareness of the importance of personal data security from an early age. The implementation of the activity included the delivery of material, group work in creating and deciphering codes, and evaluation through observation and questionnaires. The results showed a high level of enthusiasm from the students and strong support from the school. The average assessment score was 3.6 (categorized as good), reflecting the effectiveness of the approach used. This activity made a tangible contribution to enhancing students' digital literacy and opened opportunities for the development of follow-up programs, such as teacher training and the creation of learning media focused on digital security.

Keywords: cryptography; caesar cipher; vigenère cipher; digital literacy.

PENDAHULUAN

Di era digital saat ini, keamanan data pribadi menjadi aspek krusial yang harus diperhatikan oleh setiap individu. Data pribadi mencakup informasi penting seperti nama, alamat, nomor identitas, nomor telepon, serta informasi keuangan, yang jika jatuh ke tangan yang salah dapat disalahgunakan untuk berbagai kejahatan siber (Badan Siber dan Sandi Negara (BSSN), 2022). Salah satu ancaman terbesar yang dihadapi masyarakat saat ini adalah pembobolan data pribadi, yang sering kali berujung pada penipuan keuangan, pencurian identitas, dan penyalahgunaan informasi untuk pinjaman online ilegal (Pratama & Safitri, 2021). Dalam banyak kasus, pelaku kejahatan menggunakan data yang bocor untuk mengakses rekening korban, melakukan transaksi tanpa izin, atau bahkan mendaftarkan pinjaman atas nama korban tanpa sepengetahuan mereka. Kasus kebocoran data pribadi di Indonesia

telah mengakibatkan berbagai kerugian bagi masyarakat, termasuk kerugian finansial, penyalahgunaan identitas, gangguan psikologis, dan kehilangan privasi.

Di era digital, banyak siswa sekolah menggunakan *handphone* dan laptop untuk mengakses sumber belajar, baik melalui internet, aplikasi edukasi, atau platform pembelajaran daring, salah satunya SD Negeri 45 Mataram. Namun, penggunaan perangkat ini juga meningkatkan risiko terhadap kebocoran dan penyalahgunaan data pribadi, sehingga penting bagi siswa, guru, dan orang tua untuk memahami urgensi keamanan data pribadi (Bruhl & Miller, 2020).

Keamanan data pribadi sangat penting bagi siswa karena melindungi mereka dari berbagai risiko di dunia digital (Livingstone & Helsper, 2007). Saat ini, banyak aplikasi dan situs web yang meminta akses ke informasi pribadi siswa, seperti nama, email, lokasi, atau data akademik. Jika data ini jatuh ke tangan yang tidak bertanggung jawab, siswa dapat menjadi target iklan berlebihan, penyalahgunaan identitas, atau bahkan pencurian data. Selain itu, mereka rentan terhadap kejahatan siber seperti *phishing*, di mana pelaku menyamar sebagai lembaga resmi untuk mencuri informasi login atau data pribadi lainnya. Tanpa pemahaman yang baik tentang privasi digital, siswa juga dapat secara tidak sengaja membagikan informasi pribadi di media sosial atau forum online, yang dapat dimanfaatkan oleh orang lain untuk tujuan yang merugikan, termasuk perundungan digital (Kementerian Komunikasi dan Informatika Republik Indonesia, 2021). Bahkan dalam lingkungan pendidikan, data siswa yang dikumpulkan oleh *platform* pembelajaran digital harus dikelola dengan baik agar tidak disalahgunakan oleh pihak ketiga. Oleh karena itu, menjaga keamanan data pribadi sangat penting agar siswa dapat belajar dengan aman, tanpa harus menghadapi risiko eksploitasi, pencurian identitas, atau ancaman kejahatan siber lainnya (Ng, 2012).

Salah satu solusi yang dapat diterapkan dalam pengamanan data pribadi adalah penggunaan kriptografi. Kriptografi merupakan ilmu dan teknik yang digunakan untuk melindungi informasi dengan mengubahnya ke dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang (Aliyu & Olaniyan, 2016). Dalam kriptografi, pesan atau data asli (*plaintext*) dikonversi menjadi bentuk terenkripsi (*ciphertext*) menggunakan algoritma dan kunci tertentu, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengembalikannya ke bentuk semula.

Tujuan utama kriptografi adalah untuk menjaga keamanan informasi dengan memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang (Stallings, 2017). Salah satu aspek penting dalam kriptografi adalah kerahasiaan (*confidentiality*), yang memastikan bahwa pesan atau data hanya dapat dibaca oleh penerima yang sah. Selain itu, kriptografi juga berfungsi untuk menjaga integritas (*integrity*) data, sehingga informasi tidak dapat diubah atau dimanipulasi tanpa terdeteksi. Autentikasi (*authentication*) merupakan tujuan lain dari kriptografi, yang memungkinkan verifikasi identitas pengirim dan penerima dalam suatu komunikasi, sehingga memastikan bahwa data benar-benar berasal dari sumber yang terpercaya. Selain itu, kriptografi juga mendukung non-repudiasi (*non-repudiation*), yaitu mencegah seseorang menyangkal bahwa mereka telah mengirim atau menerima data tertentu, yang sangat penting dalam transaksi digital dan komunikasi elektronik. Dengan keempat tujuan utama ini, kriptografi menjadi teknologi yang sangat penting dalam melindungi informasi, baik dalam komunikasi online, transaksi perbankan, maupun sistem keamanan digital lainnya (Jain et al., 2015).

Beberapa jenis kriptografi klasik yang dapat diterapkan untuk anak sekolah dasar adalah Morse Code, Cipher Caesar, Cipher Pigpen, dan Cipher Vigenère. Morse Code adalah sistem pengkodean yang menggunakan titik (•) dan garis (-) untuk mewakili huruf, angka, dan simbol tertentu (Stallings, 2017). Ini sering digunakan dalam komunikasi radio dan sinyal darurat. Contohnya huruf A menjadi •-, huruf B menjadi -•••, atau huruf S menjadi •••. Morse Code dapat dikirim melalui suara, cahaya, atau sinyal elektrik. Caesar Cipher merupakan metode enkripsi sederhana yang menggunakan pergeseran huruf dalam alfabet (Jain et al., 2015). Setiap huruf dalam teks asli (*plaintext*) digantikan dengan huruf lain yang terletak beberapa posisi setelahnya dalam alfabet. Contohnya pada pergeseran 3 huruf, plain text: "HELLO" akan dienkripsi menjadi ciphertext: "KHOOR". Pigpen Cipher adalah sistem substitusi yang menggantikan setiap huruf dengan simbol berdasarkan pola tertentu dalam grid atau diagram. Prinsip kerjanya adalah Setiap huruf digantikan dengan simbol yang berasal dari pola dalam "pigpen grid",

kemudian terdapat dua set grid, satu tanpa titik dan satu dengan titik untuk membedakan huruf. Contohnya huruf *A* mungkin digantikan dengan simbol yang menyerupai bentuk *L* terbalik, dan seterusnya. Karena berbasis simbol, Pigpen Cipher sering digunakan dalam teka-teki dan sandi rahasia. Cipher Vigenère dinamai dari seorang diplomat dan kriptografer Prancis bernama *Blaise de Vigenère* (Aliyu & Olaniyan, 2016). Untuk mengenkripsi pesan teks dengan cipher Vigenère, misalkan kunci dari cipher Vigenère terdiri dari $l_1 l_2 \dots l_n$ dengan nilai numerik huruf yang bersesuaian k_1, k_2, \dots, k_n . Sebuah blok yang terdiri dari huruf-huruf dengan nilai numerik p_1, p_2, \dots, p_n diubah menjadi blok sandi berupa huruf-huruf dengan nilai numerik c_1, c_2, \dots, c_n dengan c_i merupakan sisa dari hasil penjumlahan p_i dan k_i dengan 26. Dalam pengabdian ini akan diterapkan Cipher Caesar dan Cipher Vigenère.

Dengan mengenalkan konsep dasar kriptografi sejak dini, siswa dapat memahami pentingnya menjaga kerahasiaan informasi serta melatih keterampilan berpikir logis dan analitis (Sari & Hartati, 2021). Kegiatan pengabdian ini bertujuan untuk meningkatkan kesadaran siswa terhadap urgensi perlindungan data pribadi, mengenalkan strategi sederhana dalam mengamankan informasi, serta mendorong peran aktif guru dan orang tua dalam membimbing anak-anak menghadapi risiko di dunia digital. Selain itu, metode enkripsi dasar ini dapat diintegrasikan ke dalam aktivitas pembelajaran yang menyenangkan, seperti permainan sandi rahasia atau pesan tersembunyi, sehingga siswa lebih antusias dalam mempelajari konsep-konsep dasar keamanan data. Dengan pemahaman ini, diharapkan siswa menjadi lebih waspada terhadap potensi penyalahgunaan informasi pribadi di era digital.

METODE

Metode yang akan digunakan adalah *coaching* (pelatihan) dengan melakukan penyampaian materi secara sistematis dan terstruktur. Materi yang disampaikan mencakup kriptografi klasik, setiap jenis sandi akan dijelaskan dengan contoh yang menarik dan aplikatif. Setelah memahami konsep dasar, siswa akan diajak untuk membuat sandi mereka sendiri menggunakan salah satu metode kriptografi tersebut. Dengan cara ini, mereka tidak hanya memahami teori, tetapi juga dapat langsung menerapkannya dalam aktivitas kreatif dan menyenangkan, seperti membuat pesan rahasia atau menyusun tantangan sandi untuk teman mereka. Selain itu, aktivitas ini bertujuan untuk melatih keterampilan berpikir logis, analitis, serta meningkatkan kesadaran mereka terhadap pentingnya menjaga informasi pribadi dalam kehidupan sehari-hari. Dengan pengalaman langsung dalam membuat dan memecahkan sandi, siswa akan lebih memahami bagaimana keamanan data bekerja serta mengembangkan sikap lebih berhati-hati dalam berbagi informasi pribadi di dunia digital.

Kegiatan pengabdian ini dilaksanakan dalam empat tahapan utama, yaitu:

- 1) Tahap Penelusuran Informasi Awal: Tim pengabdian melakukan identifikasi terhadap permasalahan aktual di lingkungan mitra, khususnya terkait minimnya pemahaman siswa sekolah dasar tentang pentingnya keamanan data pribadi. Penelusuran ini juga mencakup pemetaan pengetahuan awal siswa dan kesiapan sekolah dalam mendukung kegiatan pengabdian. Informasi ini menjadi dasar dalam merancang kegiatan yang sesuai dengan kondisi mitra.
- 2) Tahap Perencanaan: Pada tahap ini, tim menentukan sasaran kegiatan, yakni 30 siswa kelas V SDN 45 Mataram, serta menetapkan waktu, tempat, dan teknis pelaksanaan. Perencanaan mencakup pembagian tugas antaranggota tim: satu anggota bertugas menyampaikan materi, sementara anggota lainnya melakukan observasi dan penilaian proses pembelajaran. Tim menyiapkan bahan ajar, instrumen pembelajaran, dan instrumen penilaian. Materi dikembangkan untuk memperkenalkan konsep dasar kriptografi secara menyenangkan. Siswa dibekali dengan alat kerja (instrumen) yang digunakan untuk menyusun dan memecahkan sandi. Untuk menilai ketercapaian tujuan, disusun pula kuesioner penilaian, yang mencakup indikator partisipasi siswa, kerja sama, kemampuan berpikir logis, dan sikap saling menghargai.
- 3) Tahap Pelaksanaan: Kegiatan dimulai dengan pengenalan materi selama 15 menit oleh salah satu anggota tim. Setelah itu, siswa dibagi menjadi 6 kelompok (masing-masing beranggotakan 5 siswa). Soal pertama: setiap kelompok diminta membuat sandi mereka sendiri berdasarkan aturan yang mereka tetapkan secara mandiri. Soal kedua: kelompok diberikan sandi acak yang harus

dipecahkan menggunakan kunci tertentu. Waktu pengerjaan dua soal kelompok adalah 30 menit, dilanjutkan dengan presentasi hasil oleh perwakilan masing-masing kelompok.

- 4) Tahap Evaluasi: Setelah kegiatan selesai, dilakukan refleksi dan penilaian oleh tim pengabdian berdasarkan observasi langsung. Evaluasi ini juga mencakup umpan balik dari guru pendamping, serta diskusi internal untuk meningkatkan kualitas pelaksanaan pada kegiatan serupa di masa mendatang.

HASIL DAN PEMBAHASAN

Kegiatan pengabdian ini dilaksanakan di SD Negeri 45 Mataram pada siswa kelas V yang berjumlah 30 orang. Dalam pelaksanaannya, salah satu anggota tim pengabdian memberikan penjelasan mengenai pembentukan sandi menggunakan Caesar Cipher dan Vigenère Cipher seperti ditunjukkan pada Gambar 1(a). Contoh yang diberikan adalah menyusun sandi pada kata "Rahasia" menggunakan Caesar Cipher, serta pengubahan kata "Rahasia" menggunakan Vigenère Cipher dengan kunci "OKE".



(a)

(b)

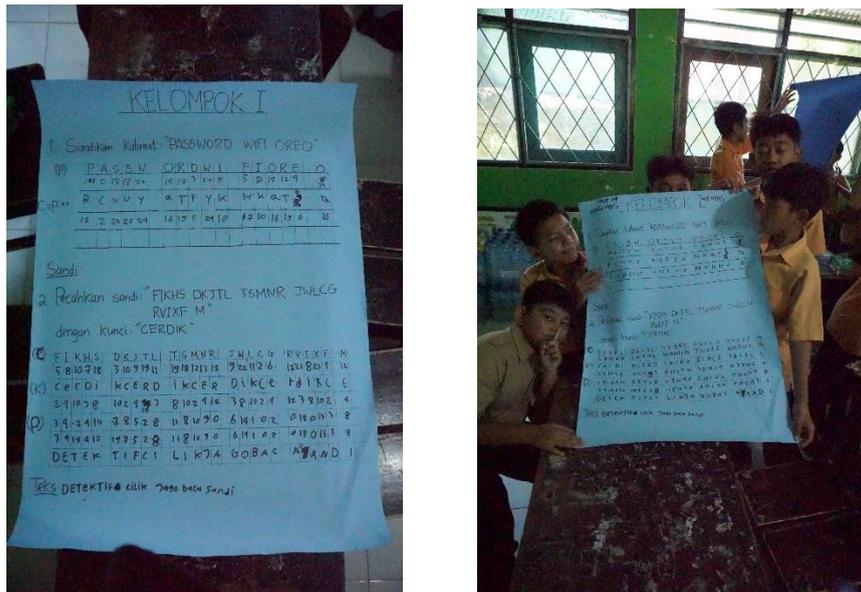
Gambar 1.(a) Penyampaian Materi; (b) Diskusi Kelompok

Setelah pemberian materi, siswa dibagi ke dalam 6 kelompok, masing-masing terdiri dari 5 orang (Gambar 1(b)). Setiap kelompok diberi dua jenis tugas: (1) Membuat sandi dari kalimat "Password Wifi Ore" menggunakan Caesar Cipher dengan aturan yang mereka rumuskan sendiri, (2) Memecahkan sandi menggunakan Vigenère Cipher dengan kunci tertentu yang telah ditentukan oleh tim pengabdian. Adapun distribusi sandi dan kunci yang diberikan kepada masing-masing kelompok diberikan pada Tabel 1.

Tabel 1. Sandi yang dipecahkan tiap kelompok

Kelompok	Sandi	Kunci
1	FIKHS DKJTL TSMNR JWLCG RVIXF M	CERDIK
2	BATIT MRYAZ IDXET AOKSV KFDLR SPAJI H	RAHASIA
3	OEKHM SVMBD MMFEY GAFOI EBFC RXNAF	CERDAS
4	BIGXM RIQXT SVBCQ THSTZ ZTIEE CMSLV	PINTAR
5	BEALC KNVHJ CCRRX IGABI ZIHYJ X	JENIUS
6	EUQDP FYUPL OUKKH ZCOMB NYUTH YVDH	MUDAH

Seluruh kelompok mampu menyelesaikan tugas pemecahan sandi dengan tepat. Sebagai contoh, kelompok pertama berhasil menguraikan sandi "FIKHS DKJTL TSMNR JWLCG RVIXF M" dengan kata kunci "CERDIK" menjadi "DETEKTIF CILIK JAGO BACA SANDI", seperti ditunjukkan pada Gambar 2 berikut.



Gambar 2. Hasil Kelompok 1

Dalam tugas pembuatan sandi, semua kelompok berhasil menyusun sandi untuk kalimat "PASSWORD WIFI OREO". Namun, beberapa kelompok sempat mengalami kekeliruan dalam penghitungan, terutama pada proses pengurangan angka besar dalam perumusan Caesar Cipher. Setelah dibantu oleh fasilitator untuk mengingat kembali konsep pengurangan bilangan, mereka mampu memperbaiki dan menyusun sandi dengan benar.

Proses diskusi dalam kelompok berlangsung sangat baik. Para siswa menunjukkan kerja sama yang solid dengan membagi peran secara merata: ada yang bertugas menulis hasil, melakukan penghitungan, dan menjelaskan jawaban. Mereka juga saling menghargai pendapat baik antar anggota dalam kelompok maupun terhadap kelompok lain. Tabel 2 menunjukkan hasil penilaian proses diskusi berdasarkan lima indikator:

Tabel 2. Hasil Penilaian Proses

Kriteria Penilaian	Skor (1 – 4)
Interaksi siswa dalam pembelajaran kelompok	3,5
Kerjasama antar siswa dalam pembelajaran kelompok	3,5
Kemampuan dalam menyusun sandi	3,5
Kemampuan memecahkan sandi	4
Menghargai pendapat teman dalam satu kelompok dan kelompok lain	3,5
Total	18
Nilai Akhir Total	18/5=3,6

Dukungan dari pihak sekolah, khususnya para guru dan kepala sekolah, sangat membantu kelancaran kegiatan. Mereka secara kooperatif membantu mengondisikan ruang kelas dan mendampingi siswa selama kegiatan berlangsung. Dengan rata-rata skor 3,6 dari skala 4, kegiatan ini masuk dalam kategori "Baik". Secara keseluruhan, kegiatan pengabdian menunjukkan bahwa siswa

mampu memahami dan menerapkan prinsip dasar kriptografi klasik dengan aktif, kolaboratif, dan antusias. Hal ini memperkuat pentingnya pengenalan konsep keamanan data pribadi sejak usia dini dalam upaya membekali generasi muda menghadapi tantangan di era digital.

SIMPULAN DAN SARAN

Kegiatan pengabdian yang dilaksanakan di SD Negeri 45 Mataram berhasil meningkatkan pemahaman siswa kelas V terhadap konsep dasar kriptografi klasik, khususnya melalui penerapan *Caesar Cipher* dan *Vigenère Cipher*. Siswa menunjukkan antusiasme dan keterlibatan aktif dalam menyusun serta memecahkan sandi secara berkelompok. Kegiatan ini tidak hanya memperkuat literasi digital dasar, tetapi juga menumbuhkan keterampilan kolaboratif, berpikir logis, dan rasa ingin tahu terhadap keamanan data pribadi di era digital. Penilaian terhadap proses diskusi dan hasil kerja kelompok menunjukkan bahwa kegiatan telah mencapai kategori "Baik", dengan nilai rata-rata 3,6 dari skala 4.

Meskipun kegiatan berjalan dengan lancar, tim pengabdian menghadapi tantangan pada tahap penyusunan instrumen dan rubrik penilaian. Oleh karena itu, disarankan agar pada kegiatan serupa di masa mendatang, proses perencanaan, terutama dalam penyusunan instrumen, soal, dan rubrik penilaian dilakukan secara lebih cermat dan terstruktur. Instrumen sebaiknya disesuaikan dengan karakteristik dan tingkat pemahaman siswa sekolah dasar, agar mereka dapat menyelesaikan tugas secara mandiri dengan cara yang menyenangkan namun tetap bermakna secara edukatif. Pelibatan guru dalam tahap perencanaan juga direkomendasikan untuk memastikan keselarasan antara materi pengabdian dan kurikulum sekolah.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada kepala sekolah, guru, dan siswa SD Negeri 45 Mataram yang telah mempercayakan tim dalam melaksanakan pengabdian di SD Negeri 45 Mataram, serta kepada LPPM Universitas Muhammadiyah Mataram yang telah memberikan hibah pengabdian masyarakat dengan nomor SK 104/II.3.AU/LPPM UMMAT/D/IV/2025.

DAFTAR RUJUKAN

- Aliyu, A. M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. *International Journal of Computer Applications*, 135(11), 46–50.
- Badan Siber dan Sandi Negara (BSSN). (2022). *Modul Literasi Keamanan Siber untuk Anak dan Remaja*.
- Bruhl, J., & Miller, L. (2020). Teaching Cryptography in Elementary Schools: Exploring Engagement through Hands-On Activities. *Journal of Computer Science Education*, 30(1), 50–66.
- Jain, A., Dedhia, R., & Patil, A. (2015). Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. *International Journal of Computer Applications*, 129(13), 1–4.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). *Pedoman Literasi Digital untuk Pendidikan Dasar dan Menengah*.
- Livingstone, S., & Helsper, E. J. (2007). Gradations In Digital Inclusion: Children, Young People And The Digital Divide. *New Media & Society*, 9(4), 671–696. <https://doi.org/10.1177/1461444807080335>
- Ng, W. (2012). Can We Teach Digital Natives Digital Literacy? *Computers & Education*, 59(3), 1065–1078.
- Pratama, R. Y., & Safitri, R. (2021). Sosialisasi Kesadaran Keamanan Data Pribadi Bagi Siswa Sekolah Dasar Melalui Media Interaktif. *Jurnal Pengabdian Kepada Masyarakat Indonesia (JPMI)*, 2(1), 25–30.
- Sari, D. K., & Hartati, S. (2021). Pengenalan Kriptografi Dasar untuk Siswa Sekolah Dasar melalui Media Pembelajaran Interaktif. *Jurnal Pengabdian Kepada Masyarakat*, 3(2), 80–87.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice (7th ed.)*. Pearson.