Jupiter: Jurnal Pendidikan Terapan
Homepage : https://journal.diginus.id/jupiter/index
Email: jurnalpendidikanterapan@gmail.com

p-ISSN : 2985-3214; e-ISSN : 2964-3171
Jupiter, Vol. 4, No. 3, July 2026
Page 315-326

A Systematic Literature Review of Mathematical Concepts in Hill Cipher-Based Cryptography for Mathematics Education

Auriel A. Y. Tuerah[1*], Vivian E. Regar[2], Philoteus E. A. Tuerah[3], Regina Pakpahan[4]
[1,2,3,4]Universitas Negeri Manado, Manado, Indonesia

ARTICLE INFO

Article history:
Submitted: Juny 09, 2026
Final Revised: July 13, 2026
Accepted: July 17, 2026
Published: July 27, 2026

Keywords:
Caesar Cipher; Cryptography Education; Hill Cipher; Hybrid Cryptosystem; Linear Algebra; Mathematics Education.

ABSTRACT

Purpose: This study aims to systematically review the mathematical concepts represented in Hill Cipher-based cryptography and examine their applications and implications for mathematics education across different educational levels. **Methods**: A systematic literature review was conducted following the PRISMA 2020 guidelines. Literature searches were performed across five academic databases, yielding 1,247 initial records. Following identification, screening, eligibility assessment, and quality appraisal, 14 primary studies published between 2020 and 2023 were included for qualitative thematic synthesis. **Findings**: The review identified modular arithmetic, matrix multiplication, and matrix inversion as the predominant mathematical concepts represented in the reviewed studies. Modular arithmetic appeared in all 14 studies and was primarily associated with secondary-level mathematics, whereas matrix operations were predominantly implemented in undergraduate contexts. The reviewed studies reported educational applications including mathematics learning media, simulation-based learning, and project-based learning. However, only a limited number of studies explicitly investigated classroom implementation, while most focused on algorithmic development and technical applications. In addition, the available evidence was dominated by studies conducted in Indonesia, limiting the broader generalizability of the findings. **Research Implications**: This review provides a conceptual synthesis that connects mathematical concepts, classical cryptographic algorithms, and their potential educational applications. The findings may inform mathematics educators, teacher educators, and curriculum developers in designing contextual mathematics learning activities while also highlighting the need for more classroom-based empirical studies across diverse educational settings. **Originality**: Unlike previous reviews emphasizing cryptographic performance and algorithm development, this study synthesizes the educational dimensions of Hill Cipher-based cryptography by mapping the relationships among mathematical concepts, instructional applications, and research gaps. The review contributes an evidence-based conceptual framework to support future research and curriculum development in mathematics education.

Doi: https://doi.org/10.61255/jupiter.v4i3.1337

INTRODUCTION

The rapid advancement of digital communication technologies has increased the importance of data security literacy across educational settings. Alongside technical developments, mathematics educators have increasingly explored authentic contexts that enable students to connect abstract mathematical concepts with real-world applications. Classical cryptographic algorithms have attracted attention in this regard because they incorporate mathematical ideas such as modular arithmetic, matrix operations, determinants, and inverse matrices while remaining sufficiently accessible for classroom implementation without sophisticated computational resources (Agung et al., 2020; Ayo-Aderele et al., 2022).

Within mathematics education, cryptography has been proposed as a contextual learning environment consistent with the principles of realistic mathematics education, where learners construct mathematical understanding through meaningful problem situations rather than isolated symbolic procedures (Bartzia et al., 2023). Previous studies have

suggested that cryptographic activities may facilitate student engagement and provide opportunities to apply mathematical reasoning in authentic problem-solving contexts (Deolika, 2020). However, these findings originate from diverse educational settings and instructional designs, making it necessary to examine the existing evidence systematically before drawing broader pedagogical conclusions.

Among classical cryptographic algorithms, the Hill Cipher has received considerable attention because it incorporates several mathematical concepts taught in secondary and higher mathematics education, including matrix multiplication, determinants, inverse matrices, and modular arithmetic (Elhabshy, 2019; Endaryono et al., 2021). Meanwhile, the Caesar Cipher is frequently introduced as a simple application of modular arithmetic, particularly for beginners, owing to its straightforward substitution mechanism (Gusmana et al., 2022). Other studies have explored combinations of classical ciphers or hybrid cryptographic approaches to illustrate relationships among multiple mathematical concepts (Permata Dewi et al., 2022; Sylviani et al., 2023). Collectively, these studies indicate that cryptographic algorithms provide diverse opportunities for connecting mathematical theory with practical applications, although their educational emphases vary considerably.

Existing literature also demonstrates considerable diversity in instructional approaches. Cryptography has been implemented through simulation-based learning, game-based learning, unplugged activities, spreadsheet applications, and web-based instructional environments (Bartzia et al., 2023; Endaryono et al., 2021; Kesuma & Rahayuda, 2024; Rosas et al., 2023). Nevertheless, most published studies primarily focus on algorithm development, encryption performance, or technical implementation, while relatively few explicitly investigate instructional design or mathematics learning outcomes. Furthermore, although modular arithmetic and matrix operations frequently appear across the literature, the relationships between specific mathematical concepts, cryptographic algorithms, and educational levels have not been synthesized comprehensively.

A preliminary examination of recent studies also reveals an imbalance in the existing evidence. Most publications concentrate on the Hill Cipher as a standalone algorithm or in combination with cryptographic methods other than the Caesar Cipher, whereas studies explicitly investigating Hill–Caesar hybrid systems remain limited (Rasudin et al., 2022; Setyawati et al., 2021). Consequently, the literature lacks a comprehensive synthesis that maps the mathematical concepts represented across Hill Cipher-based cryptography and evaluates how these concepts have been applied within mathematics education. This absence makes it difficult for educators and curriculum developers to identify which mathematical topics are most appropriate for different educational levels and instructional contexts.

Therefore, this systematic literature review aims to synthesize and critically evaluate studies examining mathematical concepts in Hill Cipher-based cryptography and their applications in mathematics education. Specifically, this review seeks to identify the mathematical concepts most frequently represented in the literature, examine how cryptographic algorithms have been implemented in educational contexts, and analyze their reported implications for mathematics teaching and learning.

To achieve these objectives, this review addresses the following research questions: What mathematical concepts are most frequently represented in Hill Cipher-based cryptographic studies relevant to mathematics education? How have Hill Cipher and related classical cryptographic algorithms been implemented within mathematics education across different educational levels? What pedagogical implications, opportunities, and research gaps emerge from the existing literature concerning the integration of cryptography into mathematics education? By systematically answering these questions, this review provides an evidence-based synthesis that clarifies the relationship between classical cryptography and mathematics education while identifying directions for future research and curriculum development.

METHOD

This study employed a Systematic Literature Review (SLR) following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines. The review consisted of research question formulation, literature searching, study screening and selection, data extraction, methodological quality assessment, and thematic synthesis. The PRISMA protocol was adopted to ensure transparency, consistency, and reproducibility throughout the review process.

Research Questions

This review addressed three research questions concerning the mathematical concepts represented in Hill Cipher-based cryptographic studies, the implementation of classical cryptographic algorithms in mathematics education across different educational levels, and the pedagogical implications and research gaps identified in the existing literature.

Search Strategy

The literature search was conducted from January to March 2025 using five electronic databases, namely Scopus, IEEE Xplore, ERIC, DOAJ, and Google Scholar. These databases were selected because they collectively provide broad coverage of mathematics education, educational technology, and computer science research. The search combined three groups of keywords related to cryptographic algorithms, mathematical concepts, and educational contexts using Boolean operators. The search string included the terms "Hill Cipher," "Caesar Cipher," and "Affine Cipher" combined with "matrix," "determinant," "inverse matrix," "modular arithmetic," and "linear algebra," together with educational terms such as "mathematics education," "education," "learning," "teaching," and "cryptography education." Reference lists of eligible studies were also examined through backward snowballing to identify additional relevant publications. Grey literature and unpublished studies were excluded. Only studies published between 2020 and 2023 were considered because all eligible studies identified during the screening process were published within this period.

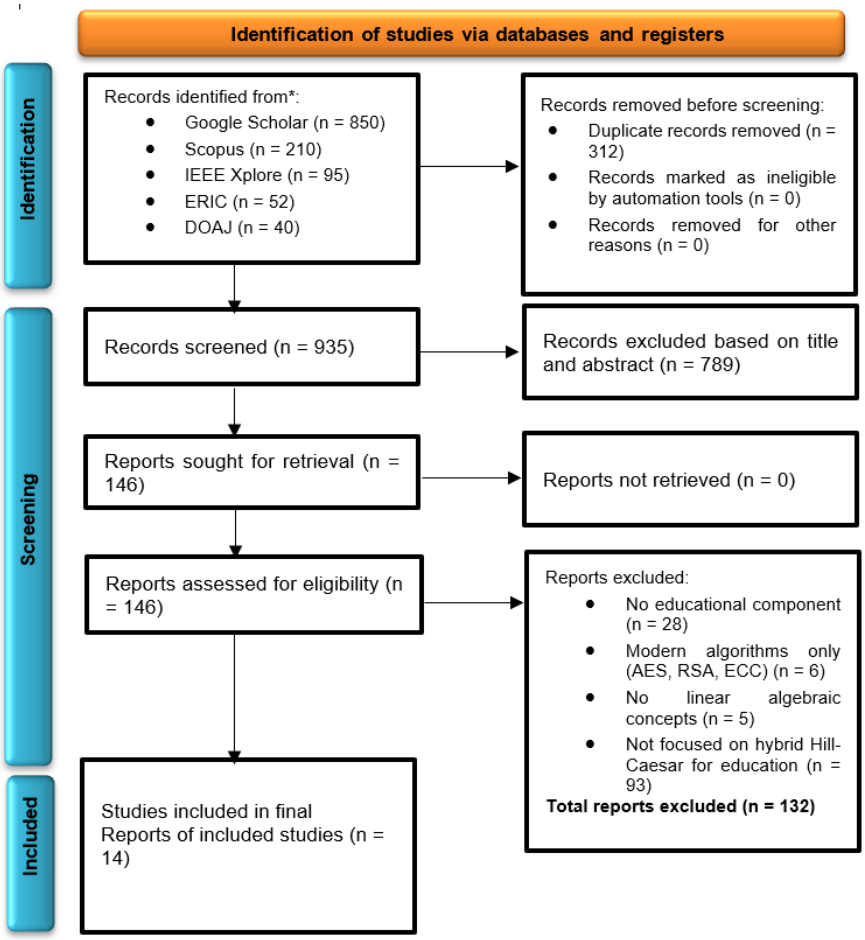

Figure 1. PRISMA Flow Diagram of Study Selection Process

Figure 1 presents the PRISMA flow diagram illustrating the identification, screening, eligibility, and inclusion processes.

Inclusion and Exclusion Criteria

Eligible studies were peer-reviewed journal articles, conference proceedings, or scholarly book chapters published in English or Indonesian between 2020 and 2023. The studies were required to examine Hill Cipher, Caesar Cipher, or related classical cryptographic algorithms while reporting mathematical concepts relevant to mathematics education either explicitly or implicitly. Only original empirical or developmental studies were included. Studies focusing exclusively on modern cryptographic algorithms, lacking educational discussion, consisting of duplicate publications, dissertations, theses, editorials, or providing insufficient methodological information were excluded from the review.

Screening and Study Selection
The study selection followed the four PRISMA stages. A total of 1,247 records were initially identified, and 312 duplicate records were removed, leaving 935 unique publications for title and abstract screening. After this stage, 146 articles remained for full-text assessment. Application of the predefined eligibility criteria resulted in 107 eligible studies. Further content analysis demonstrated that only 37 studies explicitly discussed the relationship between cryptographic algorithms and mathematics education. The final corpus consisted of 14 primary studies that simultaneously demonstrated direct relevance to Hill Cipher-based mathematics learning, reported sufficient methodological detail for data extraction, contained explicit mathematical concepts, and achieved moderate or high methodological quality based on the adapted MMAT assessment. Two reviewers independently conducted the selection process, and disagreements were resolved through discussion with a third reviewer. The inter-rater agreement reached a Cohen's kappa coefficient of 0.87, indicating strong consistency between reviewers.

Data Extraction
A standardized extraction form was piloted before full implementation to ensure consistency. Information extracted from each study included publication characteristics, research objectives, cryptographic algorithms, mathematical concepts, educational context, instructional approach, participant characteristics, principal findings, and reported limitations. Data extraction was independently completed by two reviewers and subsequently cross-checked until agreement was achieved. The extracted information was organized into a synthesis matrix presented in Appendix 1.

Quality Assessment
Methodological quality was evaluated using an adapted version of the Mixed Methods Appraisal Tool (MMAT) 2018. The assessment considered clarity of research objectives, appropriateness of research design, adequacy of data collection procedures, coherence between evidence and conclusions, and educational relevance. Studies demonstrating four or five positive criteria were categorized as high quality, whereas studies meeting two or three criteria were classified as moderate quality. No low-quality studies were retained in the final synthesis. Overall, ten studies were categorized as high quality and four as moderate quality.

Data Synthesis
The included studies exhibited considerable methodological heterogeneity; therefore, thematic synthesis was employed instead of quantitative meta-analysis. The analysis began with a descriptive summary of publication characteristics, research designs, algorithm types, educational contexts, and target educational levels. Subsequently, inductive coding was used to identify recurring mathematical concepts, instructional approaches, and educational applications. Finally, cross-study comparisons were conducted to synthesize relationships among cryptographic algorithms, mathematical concepts, educational implementation, and pedagogical implications while addressing the research questions.

Coding Framework
The coding process classified each study according to research design, cryptographic algorithm, mathematical concepts, educational application, and educational level. Coding was performed independently by two reviewers and subsequently compared to ensure consistency before thematic interpretation.

Limitations
Several methodological limitations should be acknowledged. The review was restricted to five electronic databases and peer-reviewed publications, which may have excluded relevant studies indexed elsewhere or available as grey literature. In addition, the included studies were predominantly conducted in Indonesia, limiting the international generalizability of the findings. Finally, the substantial heterogeneity of research designs and outcome measures prevented quantitative meta-analysis and required qualitative thematic synthesis.

RESULTS
This section presents the findings derived from the 14 selected studies (Appendix 1), organized according to the three research questions. All findings reported in this section are exclusively based on the studies included in Appendix 1. Analysis of the selected studies identified seven major linear algebraic concepts applied within cryptography-based mathematics learning. Table 1 summarizes the three most frequently reported concepts and their corresponding educational applications.

Table 1. Main Linear Algebraic Concepts and Their Educational Applications

Concept	Occurrence	Educational Level	Main Learning Objective
Modular arithmetic	14 studies	Secondary to undergraduate	Understanding remainders and cyclic patterns through Caesar Cipher
Matrix multiplication	13 studies	Undergraduate	Applying matrix operations for data transformation
Determinant and inverse matrices	10 studies	Undergraduate	Understanding invertibility conditions in decryption processes

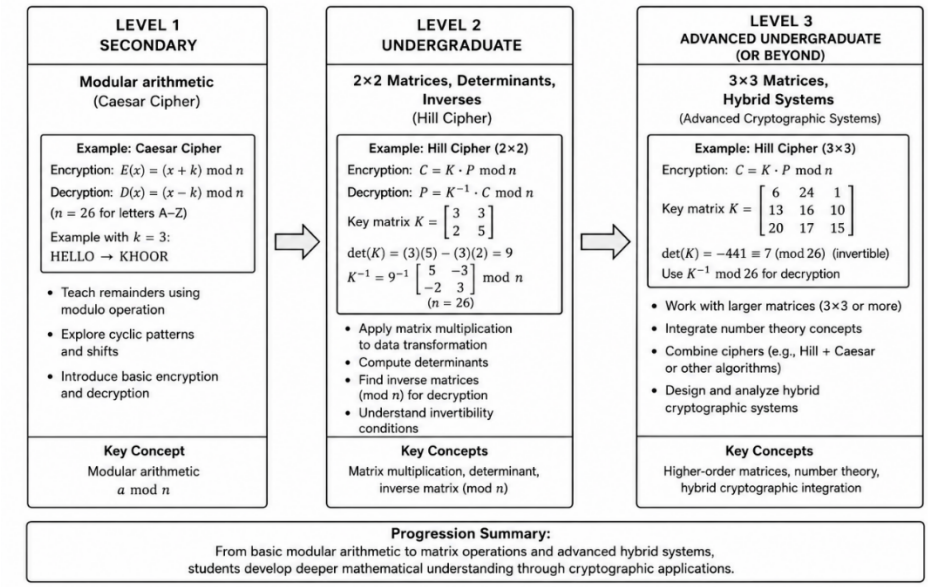

Figure 2. Illustrates The Progression of Algebraic Concepts Across Educational Levels Within Cryptographic Learning Contexts

Modular arithmetic emerged as the foundational concept, appearing in all 14 studies. Study 6 explicitly stated that cryptography was used as "realistic mathematics learning media for modulo material." Similarly, Study 1 reported that cryptographic applications "can be used to teach modular arithmetic and linear functions in high school mathematics." Matrix operations were identified in 13 studies. Study 5 described the Hill Cipher as "an excellent teaching tool for matrix operations," enabling students to practice determinants, inverse matrices, and modular arithmetic within authentic security-related contexts. Table 2 presents the distribution of cipher integration approaches identified in the selected studies.

Table 2. Cipher Types and Educational Suitability

Cipher Type	Number of Studies	Suitable Educational Level	Primary Mathematical Content
Hill Cipher only	10	Undergraduate	Matrix operations, determinants, inverse matrices
Hybrid Hill–Caesar Cipher	1	Secondary to undergraduate	Modular arithmetic and matrix operations
Hybrid Caesar-based systems	1	High school	Modular arithmetic and linear functions
Hybrid Hill-based systems with other methods	4	Advanced undergraduate	Integration of matrices and number theory

The studies demonstrated two primary integration approaches: sequential integration and simultaneous integration. Sequential integration, as reported in Study 1, allows students to master individual mathematical concepts before

combining them into more complex cryptographic systems. In contrast, simultaneous integration, identified in Study 6, challenges learners to coordinate multiple mathematical structures concurrently. Study 6 was particularly notable for its explicit educational orientation, as it was "directly designed for education" and integrated multiple cipher techniques to enhance student engagement and conceptual understanding. Table 3 summarizes the educational applications identified across the reviewed studies.

Table 3. Educational Contexts and Target Educational Levels

Educational Context	Number of Studies	Target Level
Mathematics learning media	1 (Study 6)	Secondary school
Simulation-based learning	1 (Study 8)	Secondary, undergraduate, and teacher education
Project-based learning	1 (Study 11)	Undergraduate
General cryptography education	11	Primarily undergraduate

Among the reviewed studies, Study 6 demonstrated the strongest pedagogical emphasis by explicitly positioning cryptography as "realistic mathematics learning media for modulo material." In addition, Study 8 utilized Microsoft Excel-based Hill Cipher simulations to support students' understanding of matrix operations without requiring programming expertise, thereby increasing accessibility for beginner learners. Several recurring limitations were identified across the studies (Appendix 3). Most studies lacked real-world implementation or empirical classroom testing (13 studies). Additional limitations included text-only encryption applications (4 studies) and restricted key-space capacity (2 studies).

DISCUSSION

Mathematical Concepts in Hill Cipher-Based Cryptography

The synthesis of the fourteen primary studies indicates that modular arithmetic constitutes the most consistently represented mathematical concept in Hill Cipher-based cryptography, followed by matrix multiplication and matrix inversion. This pattern suggests that researchers have primarily employed cryptographic algorithms as a context for introducing foundational mathematical concepts that can be readily connected to authentic problem-solving activities. Rather than emphasizing abstract procedures alone, the reviewed studies demonstrate a tendency to situate mathematical learning within practical encryption and decryption processes, allowing learners to recognize the functional role of mathematics in information security.

The predominance of modular arithmetic may be explained by its fundamental role in classical cryptographic algorithms and its accessibility across different educational levels. Most reviewed studies introduced modular arithmetic before more advanced mathematical concepts, indicating that it serves as an entry point for understanding encryption mechanisms. This progression reflects an instructional sequence in which students first develop an understanding of cyclic number systems before applying more complex matrix operations required in the Hill Cipher. Consequently, modular arithmetic functions not only as a mathematical prerequisite but also as a bridge between elementary number theory and more advanced algebraic reasoning.

The reviewed studies further reveal that matrix multiplication and matrix inversion are predominantly introduced through Hill Cipher implementations at the undergraduate level. This tendency reflects the higher cognitive demands associated with matrix operations, particularly the requirement to understand determinants and invertibility under modular arithmetic. Instead of treating these concepts as isolated computational procedures, the reviewed studies consistently positioned them within authentic encryption tasks, enabling students to connect abstract linear algebra concepts with practical applications. Such an approach may enhance conceptual understanding by demonstrating why matrix properties are essential for successful encryption and decryption rather than merely requiring procedural calculations.

Although several studies explored combinations of classical cryptographic algorithms, the synthesis indicates that the Hill Cipher remained the dominant instructional context throughout the reviewed literature. Explicit implementations of Hill–Caesar hybrid cryptosystems were comparatively limited, suggesting that current research has concentrated more heavily on individual cryptographic algorithms than on integrated instructional models. This imbalance indicates that the existing literature has established a relatively strong foundation for teaching individual mathematical concepts through cryptography, whereas empirical evidence concerning the educational value of hybrid cryptographic approaches remains insufficient. Accordingly, hybrid implementations should be regarded as an emerging area requiring further pedagogical investigation rather than as the prevailing instructional practice identified in this review.

Educational Patterns and Their Implications

The reviewed studies reveal that educational applications of Hill Cipher-based cryptography remain relatively limited compared with the large number of studies emphasizing algorithm development and encryption performance. This pattern indicates that cryptography research has predominantly evolved from a computer science perspective, where improvements in computational efficiency and security receive greater attention than instructional design or learning outcomes. Consequently, empirical evidence demonstrating how cryptographic activities support mathematics learning remains less developed than evidence concerning algorithmic implementation.

Another notable pattern is the concentration of educational applications at the undergraduate level. Most studies employed the Hill Cipher to illustrate matrix operations within university courses, whereas comparatively few investigated its use in secondary mathematics education. This distribution may reflect curriculum differences, as matrix algebra is generally introduced more extensively in higher education than in secondary schools. Nevertheless, the presence of several studies involving school-level learners suggests that cryptography-based activities can be adapted to different educational stages when mathematical complexity is aligned with students' prior knowledge. These findings imply that broader implementation in school mathematics is feasible but requires carefully designed instructional materials and learning sequences.

The synthesis also indicates that the educational value of cryptography extends beyond the presentation of mathematical procedures. Across the reviewed studies, encryption activities consistently positioned mathematical concepts within meaningful problem-solving contexts, encouraging learners to apply rather than merely memorize mathematical operations. Such contextualization may increase students' awareness of the practical relevance of mathematics while simultaneously supporting reasoning, logical thinking, and analytical problem-solving. However, because relatively few studies directly evaluated learning outcomes through rigorous educational research designs, current evidence remains insufficient to conclude the overall effectiveness of cryptography-based instruction.

An additional finding concerns the limited integration of multiple classical cryptographic algorithms within a single instructional framework. Although several studies discussed combinations of cryptographic techniques, explicit educational implementations involving integrated learning activities were uncommon. This pattern suggests that existing research has primarily treated individual algorithms as separate instructional tools instead of exploring how different cryptographic methods can collectively support progressively more complex mathematical understanding. Future instructional research should therefore examine whether integrating multiple classical cryptographic algorithms provides additional pedagogical benefits beyond those achieved through single-algorithm approaches.

Integration with Existing Literature on Mathematics Education

The synthesis of the fourteen primary studies demonstrates that mathematical concepts embedded in Hill Cipher-based cryptography are predominantly associated with modular arithmetic and matrix operations. This finding is consistent with the broader literature emphasizing that classical cryptographic algorithms rely fundamentally on number theory and linear algebra to perform encryption and decryption processes (Thanh-Giang, 2023). Nevertheless, the reviewed studies indicate that these mathematical concepts have been applied more frequently as technical components of cryptographic algorithms than as explicitly designed instructional resources for mathematics education.

Another important pattern emerging from the synthesis concerns the geographical concentration of the available evidence. Most of the reviewed studies were conducted in Indonesia, suggesting that research on cryptography-based mathematics learning has developed within relatively specific educational contexts. Similar observations have been reported by Ayo-Aderele et al. (2022), who noted that educational applications of classical cryptography remain unevenly distributed across countries and educational systems. Consequently, caution should be exercised when generalizing the present findings because curriculum structures, technological infrastructure, and instructional practices differ considerably among educational settings.

The reviewed studies also reveal that explicit pedagogical design receives substantially less attention than algorithmic implementation. Most investigations evaluated encryption procedures, algorithm modifications, or computational performance, whereas only a limited number incorporated learning objectives, instructional strategies, or educational evaluation. This tendency corresponds with the argument advanced by Naidoo and Reddy (2023), who emphasized that educational technology should be supported by appropriate instructional design rather than technological innovation alone. Therefore, the current evidence suggests that stronger collaboration between mathematics educators and cryptography researchers is necessary to transform technical developments into classroom-ready learning resources.

Several studies included in the synthesis further illustrate that meaningful mathematics learning does not necessarily depend on sophisticated computational environments. For example, learning activities utilizing spreadsheet

simulations and unplugged approaches demonstrate that abstract mathematical concepts can be explored through accessible instructional media while maintaining authentic cryptographic contexts. Similar conclusions were reported by Bartzia et al. (2023), who argued that cryptography-based learning can remain pedagogically effective even in environments with limited technological resources. Collectively, these findings reinforce the potential of classical cryptography as a contextual medium for mathematics learning while simultaneously highlighting the need for more rigorous empirical evaluations of instructional effectiveness.

Pedagogical Implications for Mathematics Instruction

The synthesis of the reviewed studies suggests that classical cryptographic algorithms provide meaningful contexts for connecting abstract mathematical concepts with authentic problem-solving situations. Rather than functioning solely as technical encryption tools, Hill Cipher-based activities create opportunities for students to apply modular arithmetic and matrix operations within realistic scenarios. This contextualization is consistent with the principles of meaningful mathematics learning, where abstract concepts are introduced through applications that are relevant to students' experiences (Bartzia et al., 2023; Naidoo & Reddy, 2023).

Another implication emerging from the reviewed studies concerns the sequencing of mathematical concepts across educational levels. Modular arithmetic frequently appears as the foundational concept in school-level learning, whereas matrix multiplication, determinants, and inverse matrices are predominantly implemented in undergraduate mathematics courses. This pattern suggests that cryptography-based instruction may be more effective when mathematical complexity is aligned with learners' prior knowledge and cognitive readiness rather than introducing multiple advanced concepts simultaneously. Such progression supports a gradual development of mathematical reasoning while maintaining coherence between curriculum content and cryptographic applications (Kesuma & Rahayuda, 2024; Endaryono et al., 2021).

The reviewed studies further indicate that the educational effectiveness of cryptography depends not only on the selection of algorithms but also on the instructional design through which those algorithms are implemented. Studies employing simulations, spreadsheet applications, web-based environments, and contextual learning activities demonstrate that accessible instructional media can facilitate students' exploration of mathematical structures without requiring advanced programming skills (Endaryono et al., 2021; Rosas et al., 2023). These findings suggest that the successful integration of cryptography into mathematics education relies on pedagogical design that supports conceptual understanding rather than emphasizing technical implementation alone.

The synthesis also highlights implications for curriculum development. Although Hill Cipher-based cryptography demonstrates considerable potential for enriching mathematics instruction, explicit classroom-oriented instructional models remain limited within the reviewed literature. Consequently, future curriculum development should place greater emphasis on designing learning activities that systematically connect mathematical concepts, cryptographic applications, and expected learning outcomes. Strengthening this alignment would help bridge the existing gap between technical cryptography research and mathematics education while supporting more authentic and interdisciplinary learning experiences (Arifin, 2025; Naidoo & Reddy, 2023).

Theoretical Contributions

The present review contributes to the growing body of literature on mathematics education by synthesizing how classical cryptographic algorithms have been used to represent mathematical concepts across different educational contexts. Rather than evaluating individual instructional interventions, this review identifies broader patterns showing that modular arithmetic, matrix multiplication, and matrix inversion constitute the principal mathematical concepts underlying Hill Cipher-based cryptography. This synthesis clarifies the conceptual relationships among these topics and demonstrates how they collectively support contextualized mathematics learning.

An important theoretical insight emerging from the reviewed studies is the imbalance between technical and educational perspectives. Most studies concentrated on algorithm development, encryption performance, or cryptographic modification, whereas comparatively few explicitly examined instructional design or mathematics learning processes. This pattern suggests that the theoretical development of cryptography in education has been driven primarily by computer science rather than educational research. Consequently, the pedagogical foundations supporting the integration of cryptography into mathematics instruction remain less developed than the technical foundations of the algorithms themselves.

The review also highlights the need for stronger interdisciplinary integration between mathematics education and cryptography research. The reviewed studies consistently demonstrate that cryptographic algorithms provide authentic contexts for applying mathematical concepts; however, evidence explaining how students construct conceptual understanding through these activities remains limited. This finding indicates that future theoretical development

should move beyond demonstrating the applicability of cryptographic algorithms toward explaining the mechanisms through which cryptography facilitates mathematical reasoning, conceptual understanding, and problem-solving skills.

From a systematic review perspective, the synthesis further demonstrates that existing evidence remains concentrated within a limited range of educational settings and research designs. The predominance of undergraduate contexts and technical implementation studies suggests that the current knowledge base has not yet fully captured the diversity of instructional practices that may emerge across different educational levels. Accordingly, future theoretical models should incorporate both mathematical content and pedagogical variables to provide a more comprehensive framework for integrating classical cryptography into mathematics education.

Methodological Limitations of the Review

Several limitations should be considered when interpreting the findings of this review. First, the literature search was limited to five major academic databases, namely Scopus, IEEE Xplore, ERIC, DOAJ, and Google Scholar. Although these databases provide broad coverage of mathematics education and computer science publications, relevant studies indexed elsewhere may not have been captured. Consequently, the synthesized evidence may not represent the complete body of literature on cryptography-based mathematics education.

Second, the review was restricted to peer-reviewed publications published between 2020 and 2023. While this criterion ensured the inclusion of recent and academically validated studies, it may have excluded earlier investigations or emerging evidence available through grey literature and other scholarly sources. This limitation should be considered when interpreting the comprehensiveness of the current synthesis.

Third, the geographical distribution of the included studies was uneven, with most primary studies originating from Indonesia. This concentration reflects the current development of research in the field but may limit the transferability of the findings to educational systems with different curriculum structures, instructional practices, and technological resources. Future reviews incorporating a broader international evidence base may provide a more comprehensive understanding of cryptography-based mathematics education.

Finally, considerable heterogeneity was observed across the reviewed studies regarding research design, educational context, instructional approach, and reported outcomes. Such variation prevented quantitative synthesis through meta-analysis and required the adoption of thematic synthesis. Although recurring patterns could be identified across the fourteen primary studies, the findings should be interpreted as qualitative evidence rather than generalized estimates of instructional effectiveness.

Future Research Directions

The synthesis of the reviewed studies identifies several priorities for future research. First, more empirical studies are needed to evaluate the educational effectiveness of Hill Cipher-based learning activities using rigorous research designs, such as quasi-experimental, longitudinal, or mixed-method approaches. Although the reviewed literature demonstrates considerable interest in cryptographic applications, evidence regarding their impact on students' mathematical understanding, reasoning, and problem-solving skills remains limited. Strengthening the empirical basis of this field would provide more robust evidence for integrating cryptography into mathematics education.

Second, future research should expand beyond technical algorithm development by placing greater emphasis on instructional design and classroom implementation. The reviewed studies indicate that educational applications remain relatively scarce compared with studies focusing on encryption performance and algorithm modification. Consequently, researchers should develop and evaluate instructional models that explicitly align cryptographic activities with mathematics learning objectives, curriculum standards, and students' cognitive development across different educational levels.

Finally, broader geographical representation and interdisciplinary collaboration are needed to strengthen the current evidence base. Most of the reviewed studies originated from a limited number of educational contexts, reducing the generalizability of the findings. Future investigations involving diverse educational systems, together with collaboration among mathematics educators, computer scientists, and curriculum developers, would contribute to a more comprehensive understanding of how classical cryptography can support meaningful mathematics learning and inform future curriculum innovation.

CONCLUSION

This systematic literature review addressed three research questions concerning the mathematical concepts represented in Hill Cipher-based cryptography, its implementation in mathematics education, and the pedagogical implications emerging from the existing literature. Regarding the first research question, the synthesis of the fourteen primary

studies indicates that modular arithmetic, matrix multiplication, and matrix inversion are the most frequently represented mathematical concepts. These concepts form the principal mathematical foundation underlying the educational use of classical cryptographic algorithms, with modular arithmetic generally serving as an introductory concept and matrix operations appearing predominantly in undergraduate learning contexts.

With respect to the second research question, the reviewed studies show that Hill Cipher-based cryptography has been implemented through a variety of instructional approaches, including classroom activities, simulations, spreadsheet applications, and web-based learning environments. However, the evidence demonstrates that most studies primarily emphasize algorithmic implementation rather than instructional design or educational evaluation. Furthermore, explicit educational applications involving integrated classical cryptographic algorithms remain limited, indicating that classroom-oriented implementations have not yet become a dominant focus of the literature.

Regarding the third research question, the review identifies both opportunities and research gaps for mathematics education. The existing literature suggests that classical cryptography provides a meaningful contextual framework for connecting mathematical concepts with authentic applications. Nevertheless, the available evidence remains insufficient to establish the overall effectiveness of cryptography-based instruction because relatively few studies directly evaluated student learning outcomes using rigorous educational research designs. Consequently, the principal contribution of this review lies in providing a conceptual synthesis that maps the relationships among mathematical concepts, classical cryptographic algorithms, and their potential educational applications rather than demonstrating the effectiveness of specific instructional interventions.

Overall, this review highlights the need for greater collaboration between mathematics educators and cryptography researchers to develop instructional models supported by stronger empirical evidence. Future research should prioritize classroom-based studies, broader international representation, and instructional designs that explicitly evaluate how cryptography-based learning contributes to students' mathematical understanding across different educational contexts.

REFERENCE

Agung, A., Heryana, N., & Solehudin, A. (2020). Combination of Hill Cipher Algorithm and Caesar Cipher Algorithm for Exam Data Security. Buana Information Technology and Computer Sciences (BIT and CS), 1(2), 42–45.

Alawiyah, T., Hikmah, A. B., Wiguna, W., Kusmira, M., Sutisna, H., & Simpony, B. K. (2020). Generation of rectangular matrix key for Hill Cipher algorithm using Playfair Cipher. Journal of Physics: Conference Series, 1641(1). https://doi.org/10.1088/1742-6596/1641/1/012094

Arifin, S. (2025). Mathematical foundations of data science and cryptography: Implications for mathematics education. Bandung, Indonesia: Institut Teknologi Sains Bandung.

Ayo-Aderele, S., Misra, S., & Maskeliūnas, R. (2022). A review of classical cryptographic techniques and their modern applications. Informatics, 9(2), 45. https://doi.org/10.3390/informatics9020045

Bartzia, E.-I., Lodi, M., Sbaraglia, M., Modeste, S., Durand-Guerrier, V., & Martini, S. (2023). An unplugged didactical situation on cryptography between informatics and mathematics. Informatics in Education, 23, 25–56. https://doi.org/10.15388/infedu.2024.06

Deolika, A. (2020). Modifikasi metode Hill Cipher dan Vernam Cipher menggunakan kode administrasi dan pajak. Jurnal Teknologi Informasi (JurTI), 4(2), 224–227. https://doi.org/10.36294/JURTI.V4I2.1345

Elhabshy, A. A. (2019). Augmented Hill Cipher. International Journal of Network Security, 21(5), 812. https://doi.org/10.6633/IJNS.201909

Endaryono, E., Dwitiyanti, N., & Setiawan, H. S. (2021). Aplikasi operasi matriks pada perancangan simulasi metode Hill Cipher menggunakan Microsoft Excel. String (Satuan Tulisan Riset dan Inovasi Teknologi), 6(1). https://doi.org/10.30998/String.V6i1.8603

Fadlilah, S. N., Turmudi, T., & Khudzaifah, M. (2022). Penggabungan algoritma Hill Cipher dan Elgamal untuk mengamankan pesan teks. Jurnal Riset Mahasiswa Matematika, 1(5). https://doi.org/10.18860/Jrmm.V1i5.14496

Fitroti, H., Romdhini, M. U., & Switrayni, N. W. (2021). Hill Cipher algorithm with generalized Fibonacci matrix in message encoding. Eigen Mathematics Journal, 4(2).

Ginting, V. S. (2020). Penerapan algoritma Vigenere Cipher dan Hill Cipher menggunakan satuan massa. Jurnal Teknologi Informasi, 4(2), 241–246. https://doi.org/10.36294/jurti.v4i2.1365

Gusmana, R., Haryansyah, & Wibisono, A. D. (2023). Implementasi algoritma Hill Cipher menggunakan kunci matriks 2x2 dalam mengamankan data teks. Generation Journal, 7(3), 31–39.

Gusmana, R., Haryansyah, H., & Fitria, F. (2022). Implementasi algoritma Affine Cipher dan Caesar Cipher dalam mengamankan data teks. Sebatik, 26(2). https://doi.org/10.46984/Sebatik.V26i2.2084

Hamdani, D., & Junaidi, J. (2020). Modifikasi karakter kode pada cipher Hill menggunakan kode ASCII. Eigen Mathematics Journal. https://doi.org/10.29303/Emj.V3i1.54

Hasan, P., Yunita, S., & Ariyus, D. (2020). Implementasi Hill Cipher pada kode telepon dan five modulus method dalam mengamankan pesan. Sisfotenika, 10(1). https://doi.org/10.30700/Jst.V10i1.521

Hasibuan, Y. W., Isnarto, I., & Veronica, R. B. (2022). Perancangan dan implementasi aplikasi kriptografi algoritma Hill Cipher dalam dekripsi enkripsi data keuangan nasabah Bank Sampoerna menggunakan kode ASCII. Unnes Journal of Mathematics, 11(1). https://doi.org/10.15294/Ujm.V11i1.29356

Hasoun, R. K., & Khlebus, E. A. (2021). Enhancing Hill Cipher using dynamic key matrices. International Journal of Computer Science and Network Security, 21(3), 45–52.

Hasoun, R. K., Khlebus, S. F., & Tayyeh, H. K. (2021). A new approach of classical Hill Cipher in public key cryptography. International Journal of Nonlinear Analysis and Applications, 12(2). https://doi.org/10.22075/Ijnaa.2021.5176

Hidayat, M., Tahir, M., Sukriyadi, A., & Sulton, A. (2023). Penerapan kriptografi Caesar Cipher dalam pengamanan data. Jurnal Ilmiah Multidisiplin, 2(3), 35–41. https://doi.org/10.56127/jukim.v2i03.619

Kesuma, P. A. D., & Rahayuda, I. G. S. (2024). Pengembangan algoritma Caesar Cipher dalam game-based learning untuk pendidikan kriptografi pada anak. Jurnal Nasional Teknologi Informasi dan Aplikasinya (JNATIA), 2(3), 531–536.

Krisma Budi Ziliwu, A. M. (2022). Implementasi Caesar Cipher pada algoritma kriptografi dalam penyandian pesan Whatsapp. Jurnal Comasie, 117–125.

Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., & Mir, U. H. (2022). Cryptanalysis and improved image encryption scheme using elliptic curve and affine Hill Cipher. Mathematics, 10(20), 3878. https://doi.org/10.3390/math10203878

Mesran, M., & Nasution, S. D. (2020). Peningkatan keamanan kriptografi Caesar Cipher dengan menerapkan algoritma kompresi Stout Codes. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 4(6), 1209–1215. https://doi.org/10.29207/RESTI.V4I6.2730

Naidoo, J., & Reddy, S. (2023). Embedding sustainable mathematics higher education in the Fourth Industrial Revolution era post-COVID-19: Exploring technology-based teaching methods. Sustainability, 15(12). https://doi.org/10.3390/su15129692

Nurjamiyah. (2020). Implementasi algoritma Affine Cipher untuk keamanan data teks. Jurnal Sistem Informasi, 50–59.

Permata Dewi, N., Sembiring, D. J. M., Br. Ginting, R., & Br. Ginting, M. (2022). Pengamanan data dengan kriptografi hibrida algoritma Hill Cipher dan algoritma LUC serta steganografi chaotic LSB. Jurnal Syntax Admiration, 3(2). https://doi.org/10.46799/Jsa.V3i2.389

Rasudin, R., Zulfan, Z., & Rizki, P. (2022). Analisis perbandingan keamanan kriptografi klasik pada algoritma secure Hill Cipher berbasis kode ASCII dan monoalphabetic. Jurnal Teknologi Terapan dan Sains.

Rosas, G. A. P., Polo, M. J. A., Hermosilla, A. S., Delgado, A., & Huamaní, E. L. (2023). Development of a web system to improve and reinforce learning in mathematics. International Journal of Recent Innovations in Trends in Computing and Communication, 11, 51–58. https://doi.org/10.17762/ijritcc.v11i5s.6597

Setyawati, N. Y., Khofid, A. N., Rundi, A. U. B., & Wati, V. (2021). Modifikasi kriptografi klasik kombinasi metode Vigenere Cipher dan Caesar Cipher. Journal of Smart System, 1(1), 1–8. https://doi.org/10.36728/jss.v1i1.1601

Sujarwo. (2024). Key analysis of the Hill Cipher algorithm (Study of literature). Jurnal Mandiri IT, 12(3), 135–141.

Sujjada, A., & Juniar, E. (2022). Implementasi algoritma Hill Cipher untuk proses enkripsi data menggunakan media citra digital. Jurnal Restikom: Riset Teknik Informatika dan Komputer, 3(1). https://doi.org/10.52005/Restikom.V3i1.76

Sujarwo. (2024). Penerapan algoritma Hill Cipher dalam pengamanan data teks. Jurnal Teknologi Informasi, 15(2), 55–63.

Supiyanto, & Mandowen, S. A. (2021). Advanced Hill Cipher algorithm for security image data with the involutory key matrix. Journal of Physics: Conference Series, 1899(1). https://doi.org/10.1088/1742-6596/1899/1/012116

Sylviani, S., Kartiwa, A., Permana, F. C., Hadi, A. N., Kadir, M. P., & Wilopo, R. (2023). Aplikasi matriks untuk meningkatkan keamanan proses kriptografi Caesar, Vernam, dan Hill Cipher. Jurnal Sains dan Teknologi, 12(2), 502–515.

Thanh-Giang, N. T. (2023). Applications of linear algebra in encryption. HPU2 Journal of Natural Sciences and Technology, 2(1), 46–52. https://doi.org/10.56764/hpu2.jos.2023.1.2.46-52

Wasil, M. (2023). Implementasi matriks dalam kriptografi Hill Cipher dalam mengamankan pesan rahasia. Zeta - Math Journal, 8(2). https://doi.org/10.31102/Zeta.2023.8.2.71-78

Widia Asiani, R., & Yanti, I. (2022). Penerapan kriptografi Caesar Cipher dan Hill Cipher dalam pengiriman pesan rahasia sebagai media pembelajaran matematika realistik pada materi modulo. Baitul 'Ulum, 6(1).

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all researchers whose studies were included in this systematic literature review. Their contributions have provided valuable insights into the application of linear algebra concepts in cryptographic systems and mathematics education. The authors also appreciate the support of their affiliated institution and colleagues who provided constructive feedback throughout the preparation of this manuscript. Their assistance contributed significantly to the completion of this study.

AUTHOR CONTRIBUTION STATEMENT

AAYT was responsible for conceptualizing the study, developing the research objectives, designing the systematic literature review framework, conducting data analysis, and drafting the initial manuscript. VER contributed to the literature search process, study screening and selection, data extraction, and organization of the reviewed materials. PEAT assisted in the synthesis of findings, interpretation of results, and critical evaluation of the educational implications of hybrid Hill–Caesar cryptosystems. RP contributed to manuscript revision, validation of the research findings, and refinement of the final draft. All authors reviewed and approved the final version of the manuscript and agreed to be accountable for the accuracy, integrity, and coherence of the research.

AI DISCLOSURE STATEMENT

The authors used artificial intelligence (AI)-assisted tools, including Microsoft Copilot and QuillBot, during the preparation of this manuscript for language refinement, sentence paraphrasing, improvement of academic writing style, and organization of the overall structure of the article. The AI tools were utilized solely as writing support instruments and were not involved in the generation of research data, analysis, interpretation of findings, or formulation of conclusions. Following the use of these tools, the authors independently reviewed, verified, revised, and refined all content to ensure its accuracy, originality, academic integrity, and suitability for publication. The authors take full responsibility for the content of this manuscript.

***Auriel A. Y. Tuerah (Corresponding Author)**
Universitas Negeri Manado,
Jalan Kampus Unima, Kelurahan Tonsaru, Kabupaten Minahasa, Provinsi Sulawesi Utara 95618, Indonesia
Email: aurieltuerah7@gmail.com

Vivian E. Regar
Universitas Negeri Manado,
Jalan Kampus Unima, Kelurahan Tonsaru, Kabupaten Minahasa, Provinsi Sulawesi Utara 95618, Indonesia
Email: vivian.regar@gmail.com

Philoteus E. A. Tuerah
Universitas Negeri Manado,
Jalan Kampus Unima, Kelurahan Tonsaru, Kabupaten Minahasa, Provinsi Sulawesi Utara 95618, Indonesia
Email: philteusea@gmail.com

Regina Pakpahan
Universitas Negeri Manado,
Jalan Kampus Unima, Kelurahan Tonsaru, Kabupaten Minahasa, Provinsi Sulawesi Utara 95618, Indonesia
Email: reginapakpahan@gmail.com