A Literature Review on the Role of Mathematics in Enhancing Cyber Security Through Data Encryption

Nur Laily Shodiq [1)], **Ammar Hawari** [2)], **Nabilla Andini Putri** [3)], **Maira Nurul Faizah**[4], **Wahyunengsih**[5]

[1-5)] Departement of Mathematics, State Islamic University Syarif Hidayatullah Jakarta

Correspondence Author: nabillaandinip16@gmail.com

Article Info :	**ABSTRACT**
Article History : Received : 11-07-2024 Revised : 17-09-2024 Accepted : 12-01-2025 Available Online : 29-01-2025 **Keyword :** **Cybersecurity, Mathematics, Algoritma, Bilangan Biner, Aljabar Boolean**	*This article discusses the important role of mathematics in enhancing cyber security in the data encryption process. The research problem investigates the benefits of applying mathematical principles in maintaining data security amid increasingly complex cyber threats. The study focuses on four main criteria: protecting sensitive information, verifying user identity, preventing intrusions, and protecting network integrity. Mathematical algorithms, binary numbers, and boolean algebra are essential in effectively encrypting data. They not only protect sensitive information from unauthorized access but also verify user authenticity, preventing identity theft and unauthorized system access. By utilizing mathematical theories and algorithms, binary numbers, and boolean algebra, cyber security systems can guarantee data confidentiality, integrity, and availability. In conclusion, the integration of mathematics in cyber security systems is essential to mitigate risks and protect critical digital assets from increasingly sophisticated cyber threats.*

1. INTRODUCTION

Developing a strong security system requires the role of math to help. For example, the mathematical foundations of number theory and linear algebra are used to create encryption algorithms that scramble data and cannot be read by anyone without the key. Undergraduate programs also have math courses often seen in cybersecurity programs, such as College Algebra, Probability and Statistics, and Discrete Mathematics Applications. Number Theory and Boolean Algebra can also help develop security systems to secure online transactions and digital signatures. In these courses, there are concepts such as prime factorization and modular arithmetic that make it difficult to break encryption without a secret key (Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019), in L Magas, Yuliia Koziuk 2023).

The definition of cybersecurity given by several experts shows that it is a very important topic in the technological era. Because these systems are connected to the internet and have the potential to be the target of cyber attacks, it is expressed by Amoroso (2006) that cybersecurity is an important procedure designed to protect against cyberattacks on systems connected to the internet, including data, software and hardware. In addition, Lewis (2006) points out that cybersecurity also plays an important role in maintaining the security of information or data of a company. The overall conclusion is that cybersecurity is a critical factor in maintaining information security.

ISSN Print : 1979-7141
ISSN Online : 2541-1942

Cybersecurity has security devices that are usually physical hardware or virtualized hardware. One example of a device involved in a cybersecurity system is a firewall. Firewalls function as supervisors, control the sending and receiving of all traffic to pass unless there are events that raise suspicious alerts (SM Bellovin, WR Cheswick, 1994 in Johanna Ullrich, Jordan Cropper, Peter fruhwirt, edgar Weippl, 2016). Another example is an Intrusion Detection System (IDS), which is a device used to detect any unauthorized activity (Kemmerer and Vigna, 2002, Ingham, 2003 in Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, 2005).

The review of previous research on why math is important in cybersecurity especially in binary math and cryptography. Binary math is used to indicate computer operations and distinguish negative or positive states in cyber security. This is because binary is at the core of all machine languages and software. This research also uses cryptography, which is the foundation of information security and data confidentiality. Cryptography uses algorithms that are indispensable in computer science and cyber security to perform calculations, data processing, and so on. This makes math an indispensable component of cybersecurity, as the basis of encryption techniques, algorithms, and security protocols. Understanding mathematics can help in creating secure systems, analyzing, detecting anomalies, and mitigating threats effectively (Steven Bowcut, 2024).

A study presented a new hash function called SHA-3. Based on mathematical concepts and permutations, this research shows that SHA-3 is more secure than previous hash functions and can be used to ensure data integrity and authenticity. Hash functions are an important component of cyber security systems, as they ensure data integrity and authenticity (Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. 2017).

A review of previous research introduces an innovative cryptographic system based on mathematical concepts such as elliptic curves and modular shapes. This research confirms that the system has a high level of security and can be used for data encryption and decryption processes. Cryptography is a key element in cyber security systems as it plays a role in protecting data from unauthorized access. However, conventional cryptographic systems such as RSA and elliptic curve cryptography have proven to be vulnerable to attacks (Boneh, D., & Silverberg, A. 2019).

This study has some differences from previous studies. The difference is that in the cryptographic algorithm or hash function, we use SHA-256, which plays an important role in improving data security and provides strong data integrity through complex encryption, making it difficult for intruders to tamper with the data. In this research, we also use boolean algebra to create an encoding that can be misleading to criminals to make the message more secure. Binary is used for plaintext conversion (message in its original form or readable and unlocked).

Cryptography is the science of securing information, messages and data by converting the original text or information (plaintext) into a form that cannot be understood or accessed without having the appropriate decryption key. Cybersecurity systems utilize mathematics through cryptography to maintain information confidentiality, message or data authenticity, and data integrity and also to guarantee digital transactions. Cryptography uses mathematical principles to keep data secure (Stallings, W. 2017).

Cryptography has an algorithm namely DES, RSA, SHA, MD. Cryptographic algorithms are used to secure information by transforming plaintext into ciphertext. The application of cryptography in encryption creates strong algorithms to protect data through complex transformations. First, DES or Data Encryption Standard, is an algorithm that uses math to keep data secure. Then there is RSA, a widely used public-key cryptography system that relies on mathematical principles to ensure data security. RSA uses modular exponentiation to create a secure encryption and decryption process. It ensures that the private key cannot be easily derived from the public key and provides strong data security.

Furthermore, SHA is one of a family of cryptographic hash functions that are important and widely used in data security. In mathematics, the encryption process uses SHA, which is to protect data. Then the last is MD5, its use is the same, namely to maintain data security in the encryption process. However, MD5 is used to generate the hash of the input data. Then, the hash generated by MD5 can be used to secure password storage by storing the hash password instead of the original password and guarantee the data's validity by creating a digital signature.

Using MD5, sensitive data such as secret messages can be converted into hash values that are difficult to break back into the original data (Stallings, W. 2017). The conclusion of some of these cryptographic algorithms is that their uses are similar, namely to maintain data security. However, they have different ways of working and can complement each other.

The research problem of the research "What are the benefits of applying mathematics in the encryption process to maintain data?" is to investigate the benefits of applying mathematics in the encryption process to maintain data security. Sensitive information is increasingly vulnerable to unauthorized access, theft, and tampering. Therefore, this research aims to explore the role of mathematical algorithms and techniques in maintaining data confidentiality, integrity, and authenticity and to fool adversaries when they want to break into data.

2. METHOD

The proposed research investigates the benefits of applying mathematics in encryption to protect data, using a literature study combined with qualitative methods like focus groups and reviews. By merging theoretical insights from existing literature with firsthand perspectives from qualitative data, the study aims to deepen understanding of math's role in encryption for data protection.

Focus groups will engage participants in structured discussions to explore diverse perspectives, while literature reviews and observations will gather detailed data. Conducted at the Faculty of Science and Technology, Syarif Hidayatullah State Islamic University Jakarta, the research will not involve specific populations but will rely on existing literature and observations.

The literature review will adhere to ethical guidelines, respecting copyright and licensing regulations, and considering the broader social, political, and economic implications of the research. The study aims to uncover practical applications of mathematics in encryption, such as protecting sensitive information, verifying identity, preventing intrusion, and securing networks.

Using content analysis and narrative techniques, the research will construct a detailed understanding of the subject. While the qualitative nature of the study may limit generalizability, it will provide valuable insights for future research and practical applications in cybersecurity.

Research Object Article	Finding
Ariandi, W., Widyastuti, S., Haris, L. (2020) *Implementation Of Block Cipher Electronic Codebook (ECB) For Employee Data Security.* Jurnal Ilmiah Intech : Information Technology Journal of UMUS 67-68	To protect sensitive employee data from unauthorized access, the Electronic Codebook (ECB) algorithm can be implemented using mathematical concepts such as ASCII conversion, XOR operations, and 8-bit binary representation. By utilizing these methods, the ECB algorithm enhances the security of sensitive employee data. This approach is crucial for preventing unauthorized access and maintaining the confidentiality of the information.
Bryan Bernigen, (2020) *Analisis Penerapan Aljabar Boolean Dalam Kriptografi Pada Masa Perang Dunia II.*	The author discusses applying Boolean algebraic coding to secure information. This method ensures that secret messages cannot be deciphered without knowing the specific encoding used. By resembling international codes like Baudot but with different configurations, Boolean algebra coding effectively outwits criminals.

Pratama, A., Arif, M. N., Nazir, M., Dannaun, Z., & Dara. (2023). *Algoritma DES (Data Encryption Standard) untuk Keamanan Digital.* Jurnal SITEBA, 2(1), 15-26.	The author uses descriptive-analytical research to discuss the DES Algorithm and its application in data security. DES employs a symmetric-key encryption approach, using the same 56-bit key for both encryption and decryption. However, the effective key length is 48 bits, as 8 bits are used as parity bits.
Sulastri, S., & Putri, R. D. M. (2018). *Implementasi Enkripsi Data Secure Has Algorithm (SHA - 256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan*. Jurnal Teknik Elektro, Vol. 10 No. 2, 71-73.	This study combines SHA-256 and MD5 encryption for enhanced security. During key generation, the user's password is first transformed into MD5 format. The first and last characters of the MD5 result are added to the original password, one at the start and one at the end. The enhanced password is then encrypted using SHA-256, and the resulting hypertext is stored in the database.

3. RESULTS AND ANALYSIS

The categorization of this instrument revolves around the benefits of applying mathematics in the encryption process to maintain data security. These categories include protecting sensitive information, verifying user identity, preventing intrusions, and protecting network security. Each category was analyzed through various articles and research papers to determine how mathematical principles improve data encryption. The focus is on converting plaintext to ciphertext using binary numbers, using Boolean algebra to obscure information, the DES algorithm's effectiveness, and applying hash functions such as SHA-256 and MD5 to ensure data integrity and security. (Ariandi dkk., 2020; Bernigen, 2020).

Data from various articles reveal that mathematical principles, such as binary conversion, Boolean algebra, and cryptographic algorithms (DES, SHA-256, MD5), are essential in improving data security. For example, converting plain text into binary numbers ensures that only verified users with the correct keys can access sensitive data, effectively verifying user identity and preventing unauthorized access (Ariandi et al., 2020). Using hash functions such as SHA-256 and MD5 provides strong data integrity through complex encryption, making it difficult for intruders to tamper with data (Sulastri & Putri, 2018). These mathematical techniques are fundamental in creating robust encryption methods that protect against data breaches. **Additionally**, the complexity of this mathematical process acts as a barrier to potential attackers, further securing the data.

Comparing the different approaches, it is evident that while all methods aim to secure data, their mechanisms and levels of effectiveness vary. Binary conversion methods are straightforward and effective for simple encryption tasks, whereas Boolean algebra provides a more sophisticated approach suitable for susceptible information (Bernigen, 2020). **Although** historically significant, the DES algorithm may not be as secure as modern algorithms, but it still offers substantial protection for many applications (Pratama et al., 2023). The combination of SHA-256 and MD5 hash functions offers the highest level of security by ensuring that small changes to the input will result in a significantly different encrypted output, thus improving data integrity and security. (Sulastri & Putri, 2018).

The credibility of the sources and the rigor of the research methodology support the Credibility of these findings. The sources include well-known texts and research papers from reputable authors and institutions, ensuring a detailed and nuanced understanding of how mathematics is applied in encryption. Moreover, document analysis allowed for a comprehensive examination of the existing literature, providing a solid basis for the conclusions drawn (Stallings, 2017; Bos, 2019).

In conclusion, the application of math in data encryption is multifaceted and significantly enhances data security. The conversion of plaintext to binary, the use of Boolean algebra, the DES algorithm, and the combination of SHA-256 and MD5 hash functions each contribute uniquely to protecting sensitive information, verifying user identity, preventing intrusions, and securing networks, these results are supported by Ariandi et al. (2020), Bernigen (2020), Pratama et al. (2023), Sulastri & Putri (2018). These findings underscore the importance of mathematical principles in developing strong encryption techniques to protect data from unauthorized access and tampering. These techniques are particularly important in the contemporary digital landscape, where data security is paramount.

3.1. The Conclusion of The Finding

Mathematical applications for data encoding are very diverse and significantly improve data security. In addition to plaintext conversion, other techniques include Boolean expressions, DES algorithms, and the combination of hash functions SHA-256 and MD5, each of which has a unique contribution to make when it comes to protecting sensitive data, verifying user identities, preventing intrusions, and securing networks. The whole thing emphasizes the importance of mathematical principles in developing strong encoding techniques to protect sensitive data from unauthorized access and unscrupulous businesses. These technologies are very important in today's digital landscape, where data security is one of the most important factors.

3.2. Comparison with Existing Theory

The comparison of the various approaches in this study also shows that while all methods aim to secure data, their mechanisms and levels of effectiveness vary. Binary conversion methods are simple and effective for basic encryption tasks, while Boolean algebra provides a more sophisticated approach suitable for highly sensitive information (Bernigen, 2020). Although historically significant, the DES algorithm may not be as secure as modern algorithms such as RSA, but it still offers substantial protection for many applications (Pratama et al., 2023). Stallings (2016) also mentioned that RSA, as a widely used public key cryptography system, uses mathematical principles to ensure data security through modular exponentiation, which ensures that private keys cannot be easily derived from public keys. Overall, the findings support existing theories and show that applying mathematical principles in cryptography can significantly improve information security. Strong cryptographic algorithms such as DES, SHA-256, and MD5 protect data through complex transformations that are difficult to disassemble without the right key.

3.3. Theoretical and Practical Implications

There are significant theoretical and practical implications for applying mathematics in cybersecurity. Theoretically, to protect sensitive information, prevent intrusions, and verify user identities, Boolean algebra can be used by utilizing bitwise XOR, NOT, and AND operations that can be used to fool intruders by generating codes as similar as possible to international codes (Bernigen, 2020). In addition, the DES algorithm can protect information by utilizing 56 bits in the encryption process using permutations on the substitution results to scramble the data. Hence, it is not easily readable (Pratama et al., 2023). Other algorithms, such as SHA-25 and MD5, utilize mathematics in the form of hash functions that can identify small changes in data by including the algorithm equation h = H(M), linear functions, and arithmetic modulo 232 (Sulastri and Putri, 2018). The application of binary math is also carried out by Plaintext to ASCII is converted by converting characters into decimal numbers. The decimal number of the plaintext is converted into an 8 bit binary, which contains 0 and 1. The 8 bit binary is encrypted with XOR logic, and the result of the XOR operation of the plaintext and the key is converted back into decimal form (Ariandi et al., 2020).

This study demonstrates that mathematical encryption techniques can be used in different situations to improve the protection of confidential data. Organizations can apply the DES algorithm and a blend of hash functions like SHA-256 and MD5 to safeguard employee data, financial information, and consumer data from illegal access. For instance, within the banking industry, the utilization of the DES algorithm can safeguard customer transaction data, while hash functions like SHA-256 can guarantee data integrity throughout the identity verification procedure. Moreover, in the healthcare industry, these encryption techniques can be utilized to ensure the confidentiality of patient data, which is essential for upholding the privacy of medical information.

3.4. Alternative Explanation and Suggestion for Future Research

It is important to acknowledge that this research has certain limitations. A primary constraint is the dependence on qualitative data and pre-existing literature without empirical verification using experimental or real-world data. This technique may restrict the applicability of the findings, as theoretical insights may only sometimes be practically feasible. Furthermore, the emphasis on particular cryptographic algorithms like DES, SHA-256, and MD5 might not encompass newer advancements in cryptography, such as AES or ECC, which may provide superior security capabilities and extra performance advantages.

In order to address these constraints and make progress in the field of cybersecurity, future research should incorporate empirical investigations to validate theoretical discoveries through practical implementations and testing. The scope should also encompass contemporary cryptographic methods like AES and ECC, as well as the incorporation of supplementary security measures like multi-factor authentication, blockchain technology, and anomaly detection based on machine learning. Furthermore, it is crucial to assess the impact of quantum computing on current cryptography algorithms and develop encryption methods that are impervious to quantum attacks.

4. CONCLUSION

This study effectively addressed many crucial inquiries regarding using mathematics in the encryption procedure to enhance data security. Initially, it was discovered that mathematical techniques, such as Boolean algebra, binary conversion, DES algorithm, and SHA-256 and MD5 hash functions, significantly impact safeguarding confidential information. These techniques guarantee the security and integrity of data and create obstacles for unauthorized parties trying to get access. This discovery strengthens the hypothesis that mathematical principles play a crucial role in the creation of robust encryption techniques, as explained by Stallings (2016) and corroborated by recent research conducted by Ariandi et al. (2020), Bernigen (2020), Pratama et al. (2023), and Sulastri & Putri (2018).

5. ACKNOWLEDGEMENTS

This paper is the result of a student final project research for an English Lecture from the Department of Mathematics, Faculty of Science and Technology, State Islamic University Syarif Hidayatullah Jakarta, class of 2023.

6. DECLARATION OF COMPETING INTEREST

We declare that we have no conflict of interest.

7. REFERENCES

Bowcut, S. (2024, March 7). *Why Math Matters in Cybersecurity*. Cybersecurity Guide. Retrieved April 30, 2024.

Johanna Ullrich, Jordan Cropper, Peter Fruhwirt, & Edgar Weippl. (n.d.). *How Is Math Used in Cybersecurity?* edX. Retrieved April 30, 2024.

Koziuk, Y. (2023, June 26). *(PDF) APPLICATION OF MATHEMATICS IN CYBER SECURITY*. ResearchGate. Retrieved April 30, 2024.

Ozgur Depren, Murat Topallar, Emin Anarim, & Ciliz, M. K. (2005). *An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks*, *29*.

William Stallings. 2017. Cryptography and Network Security: Principles and Practice

Ariandi, W., Widyastuti, S. & Haris, L., 2020. Implementation of Block Cipher Electronic Codebook (ECB) for Employee Data Security. *Jurnal Ilmiah Intech: Information Technology Journal of UMUS*, pp. 67-68.

Bergen, B., 2020. Analisis Penerapan Aljabar Boolean dalam Kriptografi pada Masa Perang Dunia II.

Pratama, A., Arif, M.N., Nazir, M., Dannaun, Z. & Dara, 2023. Algoritma DES (Data Encryption Standard) untuk Keamanan Digital. *Jurnal SITEBA*, 2(1), pp. 15-26.

Sulastri, S. & Putri, R.D.M., 2018. Implementasi Enkripsi Data Secure Has Algorithm (SHA - 256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. *Jurnal Teknik Elektro*, 10(2), pp. 71-73.

Jonathan Katz and Yehuda Lindell. *Introduction to Cryptography, Modern Second Edition.* University Maryland, College Park, 2010.

Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press

Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.

Boneh, D., & Silverberg, A. (2019). A Cryptographic System Based on Elliptic Curves and Modular Forms. Journal of Mathematical Cryptology, 13(1), 1-23.

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The first collision for full SHA-1. In Advances in Cryptology (pp. 570–596).