ISSN No:-2456-2165

Optimizing Data Security: A Literature Review on the Implementation of Beaufort Cipher for Vigenère Affine Cipher

Prema Adhitya Dharma Kusumah[1], Kusrini Kusrini[2], Kusnawi Kusnawi[3]
Magister of Informatics[12], Computer Science Faculty[3], Universitas AMIKOM Yogyakarta[123]
Sleman, Daerah Istimewa Yogyakarta, Indonesia[123]

Abstract:- This study does an in-depth examination of cryptographic methods, specifically focusing on Affine, Vigenère, and Beaufort ciphers. The analysis is based on a large collection of scientific articles published between 2019 and 2023. The study begins by studying the prevalence and trends of these encryption methods during the chosen period, revealing surprising patterns in their usage. The Affine Cipher has become a prominent subject of study in recent research, with a notable increase in its popularity, as indicated by a peak of eight articles published in 2023. Vigenère Cipher remains a regularly preferred approach, sustaining stable usage throughout the research period. Beaufort Cipher, initially absent in 2019, enjoys a strong reappearance, reaching seven pieces in 2023. The findings not only show the growing landscape of cryptographic research but also emphasize the rising relevance of specific methods. The research contributes to a detailed understanding of encryption preferences, offering a platform for future investigations into enhancing data security through the strategic integration of these cryptographic algorithms.

Keywords:- *Cryptography; Vigenère Cipher; Affine Cipher; Beaufort Cipher; Research Trends; Encryption Methods.*

I. INTRODUCTION

The advent of the communication technology era has facilitated the exchange of information across different entities[1]. Information may be confidential or intended for specific purposes, necessitating information security precautions[1]. For various reasons, data security and confidentiality are crucial[2]. The delivery of online data is highly susceptible to hacking attempts, emphasizing the need for robust security measures[3]. To secure data conveyed over the internet, cryptography is essential for transmitting information securely between two parties[4]. Proper safeguarding of sensitive data, especially in the field of data security, is essential to thwart unwanted access and potential breaches. Cryptography is a recent subject of research now since it might be important to give protection to highly delicate and sensitive documents from criminal wrongdoings during transmission across the network[5]. Cryptography, an integral component of information security, is crucial for protecting data by converting the original text into an almost impenetrable form that can only be accessed with the appropriate decryption key. Cryptography, as a mathematical technique, covers security elements such as secrecy, data integrity, authentication, and non-repudiation[6]. Cryptography, derived from the Greek word meaning the art of securing information by changing it into a complicated and unreadable format, combines a combination of mathematics and computer technology[7].

The value of data has increased significantly in the current era of information technology. particularly if the information is highly private and only a select few have access to it. In this instance, digital or electronic data is the type that is protected[8]. With the rapid advancement of digital data interchange via electronic means, information security is becoming increasingly crucial for data transmission and storage on public communication networks[9].

Prior studies have recommended the utilization of traditional cryptographic methods, such as the Vigenère Cipher, Affine Cipher, and Beaufort Cipher, to enhance data security. The implementation of these procedures has resulted in heightened security levels, with certain studies suggesting greater security against brute force attacks and other decoding methods. The performance cipher with varying sizes demonstrate that the encryption and decryption processes are influenced by the file size, with larger files requiring more time for these operations[10]. These find extensive use in secure communications and network data transfer.

A prominent research endeavor conducted by [11] investigated the combination of Vigenère Cipher and Zig-Zag Cipher to enhance security, highlighting the need to protect text-based data with traditional cryptographic methods. [12] conducted a study on using a combination of the Triangle Chain Cipher and Vigenère Cipher to safeguard data in databases. Their research demonstrated the effectiveness of cryptographic approaches in ensuring the security of digitally stored information. [13] conducted a study that endorsed the utilization of a blend of Affine Cipher and Caesar Cipher for safeguarding textual data. The study emphasized the need for more intricate encoding methods to ensure the security of sensitive information.

The study conducted by Syahputra[14] examined the application of the Vigenère Cipher at Mom's Kitchen Medan, emphasizing the significance of safeguarding wage data as a crucial element of firm functioning in the realm of payroll data security. The produced data bears no relation to the original record, and users have the autonomy to determine the key creation[15].

There is another study of using cryptography to secure village information. In tackling the essential issue of data security for village information, especially considering the sensitivity of the data involved, a standard Vigenère cipher cryptographic technique is applied. This cryptographic solution attempts to strengthen the security and confidentiality of village information, prohibiting illegal access and adjustments. To apply this strategy, a desktop-based application is written using the Java programming language within the NetBeans IDE[16]. Cryptography also can be used in different medium like image. In tackling the risks associated with image media modification, cryptography appears to increase image security, assuring secrecy and preventing unauthorized access. In the current digital era, where sensitive data and information are frequently saved in image form, digital image security is becoming more and more important[17]. This study employs the Affine Cipher and Merkle Hellman algorithms for encryption and decryption processes. The results reveal that this combination of algorithms efficiently encrypts photos, rendering them fuzzy and incomprehensible to unauthorized individuals[18]. Addressing the issues of maintaining confidentiality, integrity, authenticity, and non-repudiation during the storage and transmission of images over unsecured networks[19]. In the context of Internet of Things (IoT) systems, data exchanged between linked devices typically contains sensitive information. To preserve this data, cryptography plays a critical role, guaranteeing that only authorized parties can access its contents[20]. In data security, the strength of an algorithm not only relies on its complexity but also on the unpredictability and complexity of the key utilized[21]. To solve these difficulties, a security solution has been developed to preserve important data by encoding it, making it challenging for unauthorized parties to identify[22].

This study builds upon the aforementioned information and specifically examines the utilization of the Beaufort Cipher to enhance the Vigenère Affine Cipher for the purpose of improving data security. By summarizing the contributions and discoveries from past research, this article tries to enhance existing security measures by employing a combination of standard cryptographic algorithms. This implementation is predicted to make a substantial contribution to preserving data confidentiality and lowering the possible hazards of information breaches.

II. RESEARCH METHODS

A. Research Questions

To carry out a systematic literature review (SLR) study, it is essential to follow a predetermined set of processes and criteria known as PICOC. The abbreviation PICOC outlines the fundamental components necessary for a thorough analysis in research, including population, intervention, comparison, outcomes, and context. Table I concise summary table that outlines the key elements of PICOC for successful adoption in the systematic literature review (SLR) process.

TABLE I. PICOC ELEMENTS

Population	*Cryptography, Data Security*
Intervention	*Datasets, Models and Methods*
Comparison	*Security Level*
Outcome	*Encrypted Data*
Context	*Database, Vigenère Affine and Beaufort Cipher*

To conduct research utilizing the systematic literature review (SLR) technique, it is necessary to formulate a set of research questions (RQs). These questions in Table II serve to provide a more targeted, purposeful, and streamlined approach to the research process.

TABLE II. RESEARCH QUESTION

ID	Research Question	Purpose
RQ1	Where does the research source used as a reference for cryptography using Vigenère Affine Beaufort come from?	Identification of research sources as references.
RQ2	What is the research on cryptography especially on hybrid method like in the last 5 years?	Identification of research developments on cryptography, especially on using Vigenère, Affine or Beaufort Cipher.
RQ3	What and how does the Vigenère Cipher work?	Identify the concepts and how the Vigenère Cipher works
RQ4	What and how does the Affine Cipher work?	Identify the concepts and how the Affine Cipher works
RQ5	What and how does the Beaufort Cipher work?	Identify the concepts and how the Beaufort Cipher works

B. Study Selection

During the study selection phase, this systematic literature review (SLR) includes research published during the past 5 years, specifically in the form of journal articles or conference papers. The study employs important search phrases, particularly cryptography, data security, Vigenère, Affine, and Beaufort Cipher. The literature gathered falls into two broad categories: experimental and survey research. The representation of the literature search process, illustrating the numerous phases leading to the discovery of relevant research.

Fig. 1 shows the steps that have been taken in this research, starting from journal collection until journal exception. An exception was made to eliminate some appropriate journals that did not have any connection with this research.

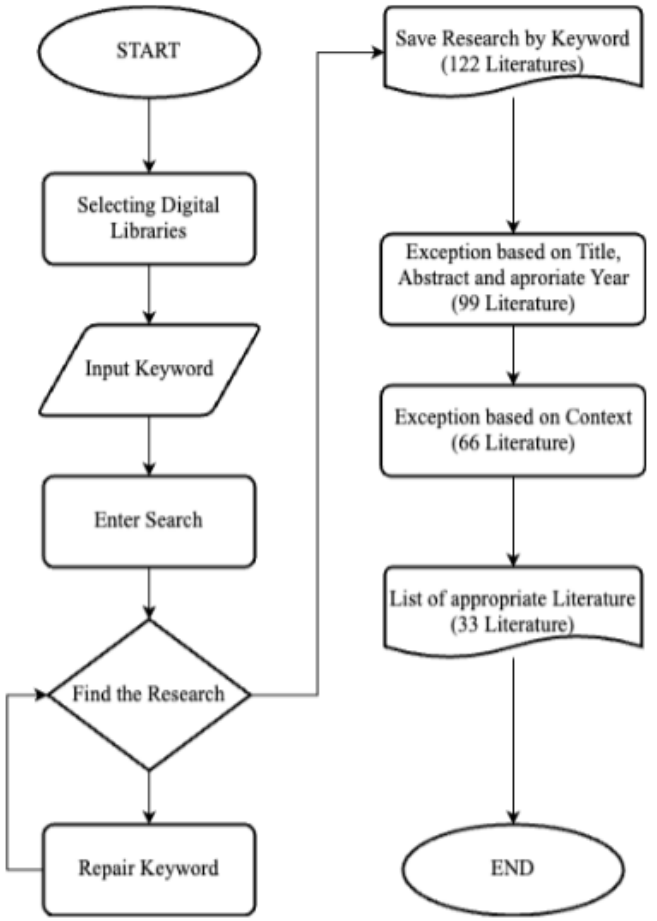

Fig. 1. Research Search Flowchart

III. RESULTS AND DISCUSSION

The Systematic Literature Review (SLR) methodology was chosen as the ideal research method due to its availability of a systematic and complete framework for discovering, analyzing, and synthesizing relevant literature. The structured and instructive character of the SLR technique fits with the obligation to deliver material clearly and systematically, achieving the high-quality criteria necessary in this research.

A. Research Years

The annual publishing rates of academic articles on data security from 2019 to 2023 are examined in this long-term study as shown in Fig. 2. The percentages varied, with 2020 seeing a notable spike to 21%, signifying a notable rise in scholarly contributions. In 2022, there was a further fall to 12%, indicating a possible shift in research priorities, while in 2021 there was a modest decline to 15%, suggesting likely stabilization. With a publication rate of 43% in 2023, there was a notable revival that suggests fresh interest and possibly innovative viewpoints in the discipline. Throughout the designated period, this detailed research sheds light on how academic engagement with data security has changed over time.

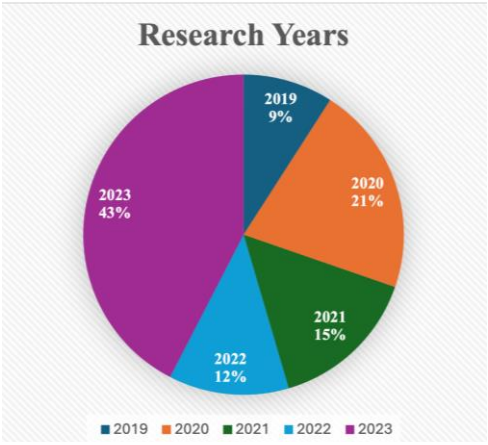

Fig. 2. Research Years

The research entails analyzing a dataset of journals, which are divided by year. Fig. 3 reveals a pattern in the growth of the number of journals focused on data security. In 2019, three journals made significant contributions that formed the foundation of this study. In 2020, the number of journals climbed to 7, demonstrating a boost in interest and attention towards data security. In 2021, the trend persisted with 5 journals being cited. Although there was a minor decline to 4 journals in 2022, it nevertheless suggested ongoing interest. The peak occurred in 2023, with the number of journals reaching 14, suggesting a major increase in academic interest in the topic of data security.

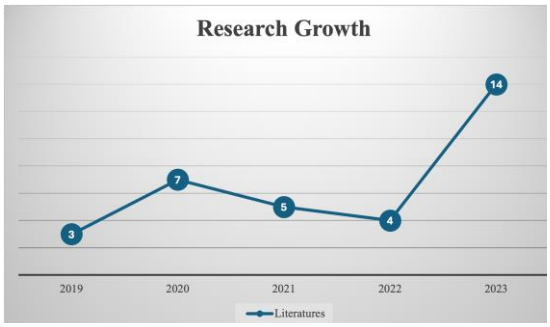

Fig. 3. Research Growth

B. Cipher Methods

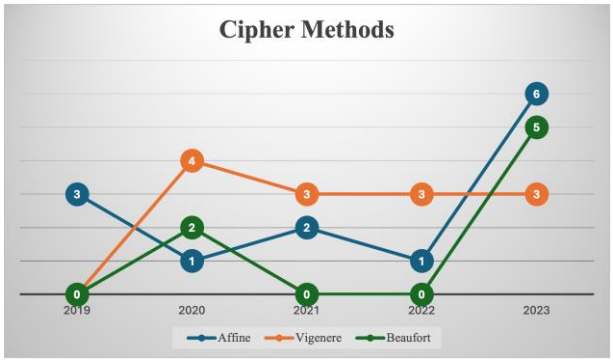

Fig. 4. Cipher Methods Growth

ISSN No:-2456-2165

The analysis of trends in the employment of data security approaches as shown in Fig. 4, notably Affine, Vigenère, and Beaufort, throughout the period from 2019 to 2023 uncovers remarkable conclusions. In 2019, the Affine approach was applied in 3 journals, whereas Vigenère and Beaufort were not featured in the study. The environment transformed in 2020, as Vigenère led with 4 journals, and Affine and Beaufort were also included in 1 and 2 journals, respectively. In 2021, Vigenère maintained its supremacy, yet Affine continued to gain interest with 2 journals. The year 2022 exhibited a continuous interest in Affine and Vigenère, both featuring in 1 and 3 journals, while Beaufort experienced a fall in utilization. The apex was reached in 2023, as the Affine approach had its maximum utilization with 6 publications, Vigenère sustained attention with 3 journals, and Beaufort experienced a major increase, being included in 5 journals. This analysis demonstrates the growth of research interests in certain data security approaches across the study period, with the Affine method being the dominant emphasis in the final year of the research.

Cipher, particularly in the field of data security, assumes a vital role in maintaining the confidentiality of information during storage and transmission across public communication networks[9].

C. Vigenère Cipher

Vigenère Cipher stands as a classical encryption method that involves a substitution mechanism, signifying a noteworthy leap beyond simpler methods like Caesar Cipher. Vigenère cipher is a cryptographic method that uses a word or phrase as the encryption key, with the key length adjusted to the length of the plaintext[11]. As an integral component of cryptographic history, the Vigenère Cipher is characterized by its capacity to solve the limitations of its predecessor and provide a more robust way of safeguarding textual information, however, its vulnerability rests in the additive cipher used in the encryption process, rendering it subject to frequency analysis assaults[23]. In some research version of the Vigenère cipher, normally used for text encryption, demonstrates its adaptability to image encryption with necessary changes[24].

The main premise of the Vigenère Cipher lies in the exploitation of a keyword or key phrase, where each letter of the keyword corresponds to a shift value for the substitution of letters in the plaintext. Unlike the Caesar Cipher, which applies a fixed shift for all characters, the Vigenère Cipher includes a variable-length key, offering better protection against frequency analysis.

The operating mechanism of the Vigenère Cipher involves repeating the keyword across the length of the plaintext. The key letters are then aligned with the corresponding plaintext letters, and the encryption is done by shifting each plaintext letter according to the matching key letter. This technique results in a ciphertext that exhibits a more complex pattern, rendering typical frequency analysis approaches less efficient.

The methodological intricacy of the Vigenère cipher is founded in the cyclical structure of its fundamental application. The repeated application of the keyword ensures a broad range of shifts, creating complexity and enhancing the overall security of the encryption. While the Vigenère cipher attracts attention, it poses issues due to a recurring encryption key[25]. Traditional cryptosystems like Caesar and Vigenère are considered obsolete because to developments in attack methods targeting key repetition[26]. The decryption process mirrors the encryption, with the key used to reverse the shifts done during encryption.

An excellent citation providing insight into the Vigenère cipher is taken from [13]. According to Gusmana, the Vigenère cipher proves its prowess as a technique for encrypting textual data, highlighting its relevance in contemporary cryptographic applications. This source provides a complete reference for understanding the subtleties and significance of the Vigenère cipher within the domain of data security.

$$C_i = (P_i + K_{i \bmod m}) \bmod 26 \quad \ldots(1)$$

C_i = encrypted letter
P_i = plaintext letter
$K_{i \bmod m}$ = key letter at position (i mod m)
m = length of the alphabet

$$P_i = (C_i - K_{i \bmod m} + 26) \bmod 26 \quad \ldots(2)$$

C_i = encrypted letter
P_i = plaintext letter
$K_{i \bmod m}$ = key letter at position (i mod m)
m = length of the alphabet

D. Affine Cipher

The affine cipher, as a symmetric cryptography algorithm, is integrated into a hybrid scheme in this research to enhance message security[27]. Affine Cipher is commonly applied in cryptographic applications due to its simplicity and efficacy in providing an additional layer of protection[28].

Affine Cipher stands as a pivotal cryptographic technique, presenting a particular method for encrypting textual data. Rooted in mathematical principles, the Affine Cipher leverages modular arithmetic to increase complexity and enhance the security of encrypted information. This narrative tries to go into the fundamental mechanics and operational technique of the Affine Cipher, providing a full understanding of its application in data security.

The core notion behind the Affine Cipher is the mathematical transformation of each character in the plaintext by a pair of mathematical functions—commonly. The simplicity and success of the Affine Cipher rest on its ability to mix multiplication and addition operations, creating diversity and preventing vulnerabilities associated with basic substitution ciphers.

$$E_{(x)} = (ax + b) \bmod m \quad \ldots(3)$$

E = encrypted letter
x = plaintext letter
(a & b) = key letter
m = length of the alphabet

The operational framework of the Affine Cipher comprises selecting adequate values for the key components a and b. The values used must adhere to specific constraints to guarantee the encryption is both reversible and secure. Specifically, the values for a and m must be coprime, and b should be within the range of the alphabet size. The encryption procedure entails applying the mathematical transformation to each character in the plaintext, creating the appropriate ciphertext.

$$D_{(x)} = a^{-1}(x - b) \bmod m \quad \ldots(4)$$

D = decrypted letter
x = plaintext letter
a^{-1} = Invers a
b = Key Letter
m = length of the alphabet

A major characteristic of the Affine Cipher is its reversibility, allowing for the decryption of the ciphertext to get the original plaintext. This inverse transformation ensures the recovery of the original message while keeping the security elements introduced by affine encryption. But Affine Cipher can be modified by the new method boosts the cipher's capability and complexity in disguising plaintext, which has led the way to more secure and dynamic data encryption[29]. Modification of Affine Cipher has goals to solve limitations noted in the original design, giving enhanced resistance against brute force assaults and aligning with both Shannon's primitive operations of cryptography and Kerckchoff's principle[30].

Another method also can be used in strengthening the robustness of keystreams for secure transaction data, this work employs the use of affine cipher with rainbow antimagic as a cryptosystem key[31]. Different study also have research in this work, by the use of an upgraded Caesar Cipher and Affine Cipher cryptographic approaches[32].

According to Fadlan[33], the employment of the Affine Cipher in combination with the Beaufort Cipher illustrates its efficacy in strengthening the security of encrypted data through multilayer encryption. This scholarly work serves as a great reference for learning the subtleties and significance of the Affine Cipher in the landscape of cryptographic algorithms.

E. Beaufort Cipher

The Beaufort Cipher, a cryptographic mechanism that traces its origins to the Vigenère Cipher, acts as a strategic way to enhance the security of textual information. This tale seeks to provide a deep analysis of the Beaufort Cipher, illuminating its underlying processes, operational approach, and applicability in contemporary data security. Despite its simplicity and history, the Beaufort cipher remains a popular choice for safeguarding data[33].

Beaufort Cipher also can be combined with another Cipher method like Vigenère Cipher to strengthen its ability. The usage of Beaufort Cipher, in conjunction with Vigenère cipher and Fibonacci, aids to establishing high levels of picture security in research by Atika Sari, et al[34].

$$C_i = (K_{i \bmod m} - P_i + 26) \bmod 26 \quad \ldots(5)$$

C_i = encrypted letter
P_i = plaintext letter
$K_{i \bmod m}$ = key letter at position (i mod m)
m = length of the alphabet

At its foundation, the Beaufort cipher operates on the notion of reciprocal substitution, bringing a new twist to the classic encryption methods. The Beaufort technique is regarded simple and fast in operations, although the key length that follows the file length can compromise security[35]. The procedure involves employing a keyword, like the Vigenère Cipher, but takes a separate approach to the encryption process. Instead of shifting the plaintext characters forward like in the Vigenère Cipher, the Beaufort Cipher utilizes a backward shift, creating a distinct yet effective encryption strategy.

$$P_i = (K_{i \bmod m} - C_i + 26) \bmod 26 \quad \ldots(6)$$

C_i = encrypted letter
Pi = plaintext letter
$K_{i \bmod m}$ = key letter at position (i mod m)
m = length of the alphabet

The operational approach of the Beaufort cipher begins with aligning the keyword with the plaintext, repeating the keyword as needed to cover the complete length of the message. The encryption procedure involves determining the distance between each plaintext character and its associated keyword character. The encrypted message, or ciphertext, is then generated by identifying the relevant letter in the reversed alphabet based on the estimated distance.

According to Hammad[1], the integration of steganography with cryptography, integrating Vigenère Cipher, Caesar Cipher, and periodic table conversion, indicates a strategic strategy to strengthen data resilience against potential brute force attacks. Another research propose different hybrid methodology entails the processing of input text messages and keys, resulting in the generation of two new keys for encryption using the Beaufort and Vigenère methods[36]. This scholarly effort serves as a vital reference for appreciating the subtleties and significance of the Beaufort cipher within the world of data encryption and security.

IV. CONCLUSION

The study examined current research sources and trends in cryptography with an emphasis on the Affine, Vigenère, and Beaufort ciphers. Regarding the research issue, it turned up a variety of sites that covered cryptography using various ciphers, demonstrating a broad spectrum of knowledge.

Analyzing recent cryptographic advances, particularly hybrid methods such as Affine, Vigenère, and Beaufort Cipher, revealed interesting trends in data security over the past five years. The popularity of the Affine approach peaked in 2023, pointing to a change in the focus of study.

The goal of the study was to comprehend how the Vigenère, Affine, and Beaufort ciphers worked, shedding light on the subtleties of each method, and offering an understanding of its underlying ideas. Up until now, the system's lack of data security has forced researchers to keep advancing science[37].

Finally, the work provides a thorough grasp of evolving trends in cryptography research. The suggested algorithm successfully breaches the security and exhibits applicability over a broad range of schemes[38]. The increased attention being paid to the Affine Cipher indicates a change in the direction of research, maybe because of its perceived efficacy in resolving data security concerns. various results not only address the problems raised by the study, but they also open new avenues for investigation into how best to apply various cryptographic techniques in tandem for enhanced information security. The Vigenère method stayed consistent, suggesting ongoing interest, and Beaufort saw a significant increase in use in 2023, furthering our comprehension of the dynamics of data security.

REFERENCES

[1]. R. Hammad et al., “Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message,” J. Phys. Conf. Ser., vol. 2279, no. 1, p. 012006, May 2022, doi: 10.1088/1742-6596/2279/1/012006.

[2]. Moch. H. Purwidiantoro and D. F. K. Saputro Wibowo, “Super Encryption Concepts using Vigenere Cipher Modification to Produce Color Imaginary as Ciphertext:,” in Proceedings of the 1st International Conference on Recent Innovations, Jakarta, Indonesia: SCITEPRESS - Science and Technology Publications, 2018, pp. 3029–3035. doi: 10.5220/0009946230293035.

[3]. E. Mendrofal, E. Y. Purba, B. Y. Siahaan, and R. W. Sembiring, “Manipulation Vigenere Cipher Algorithm with Vernam Cipher through Matrix Table Rotation:,” in Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology, Medan, Indonesia: SCITEPRESS - Science and Technology Publications, 2018, pp. 179–186. doi: 10.5220/0010040201790186.

[4]. H. Noman Abed, Z. Mohammed Ali, and A. Luay Ahmed, “A Robust Encryption Technique Using Enhanced Vigenre Cipher,” Int. J. Nonlinear Anal. Appl., vol. 12, no. 2, Jul. 2021, doi: 10.22075/ijnaa.2021.5071.

[5]. Department of CSE, Comilla University, Cumilla, Bangladesh, K. Nahar, P. Chakraborty, and Department of CSE, Comilla University, Cumilla, Bangladesh., “A Modified Version of Vigenere Cipher using 95 95 Table,” Int. J. Eng. Adv. Technol., vol. 9, no. 5, pp. 1144–1148, Jun. 2020, doi: 10.35940/ijeat.E9941.069520.

[6]. A. Abiyuda and L. Nababan, “Rancang Bangun Aplikasi Chatting Dengan Wireless LAN Menggunakan Metode Beaufort Cipher,” no. 02.

[7]. S. Vatshayan, R. A. Haidri, and J. K. Verma, “Design of Hybrid Cryptography System based on Vigene`re Cipher and Polybius Cipher”.

[8]. M. I. Harahap, S. Suherman, and R. W. Sembiring, “Three Pass Protocol for Key Security Using Affine Cipher Algortima and Exclusive-or (Xor) Combination,” sinkron, vol. 8, no. 4, pp. 2602–2614, Oct. 2023, doi: 10.33395/sinkron.v8i4.13051.

[9]. University of Computer Studies, Yangon, (UCSY), Myanmar, T. M. Aung, H. H. Naing, and N. N. Hla, “A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher: (Vigenère-Affine Cipher),” Int. J. Mach. Learn. Comput., vol. 9, no. 3, pp. 296–303, Jun. 2019, doi: 10.18178/ijmlc.2019.9.3.801.

[10]. A. Aryanti and I. Mekongga, “Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System,” E3S Web Conf., vol. 31, p. 10007, 2018, doi: 10.1051/e3sconf/20183110007.

[11]. F. A. E. Fardianto, F. Yanto, and I. Iskandar, “Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks,” vol. 4, no. 1, 2023.

[12]. A. Arif, A. Perdana, and A. Budiman, “Implementation Combination Cryptographic Algorithm Triangle Chain Cipher And Vigenere Cipher In Securing Data In Database,” vol. 7, no. 1, 2021.

[13]. R. Gusmana, H. Haryansyah, and F. Fitria, “IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN CAESAR CIPHER DALAM MENGAMANKAN DATA TEKS,” Sebatik, vol. 26, no. 2, pp. 517–524, Dec. 2022, doi: 10.46984/sebatik.v26i2.2084.

[14]. Y. H. Syahputra and L. A. Girsang, “Pengamanan Data Penggajian Menggunakan Vigenere Chiper Pada Mom’s Kitchen Medan,” vol. 5, no. 1, 2022.

[15]. D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, “Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi,” J. Sains Dan Teknol. JSIT, vol. 3, no. 1, pp. 47–52, Jan. 2023, doi: 10.47233/jsit.v3i1.483.

[16]. E. Irianti, D. F. Surianto, Ainun Zahra Adistia, Muh. Juharman, and Jumadil Ahmad Safi’i, “Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa,” Progress. Inf. Secur. Comput. Embed. Syst., vol. 1, no. 1, pp. 8–15, Mar. 2023, doi: 10.61255/pisces.v1i1.24.

[17]. Ayudeviapertiwi, Achmad Fauzi, and Siswan Syahputra, "Application Of Super Encryption Using Rot 13 Algorithm Method and Algorithm Beaufort Cipher For Image Security Digital," J. Artif. Intell. Eng. Appl. JAIEA, vol. 3, no. 1, pp. 83–92, Oct. 2023, doi: 10.59934/jaiea.v3i1.263.
[18]. Muhammad Fadillah Azmi, Achmad Fauzi, and Husnul Khair, "Implementation Of Affine Cipher Combination And Merkle Hellman On The Process Digital Image Security," J. Artif. Intell. Eng. Appl. JAIEA, vol. 2, no. 3, pp. 107–122, Jun. 2023, doi: 10.59934/jaiea.v2i3.204.
[19]. S. Sabir, "Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map," Multimed. Tools Appl..
[20]. Permana Langgeng Wicaksono Ellwid Putra, C. A. Sari, and F. O. Isinkaye, "SECURE TEXT ENCRYPTION FOR IOT COMMUNICATION USING AFFINE CIPHER AND DIFFIE-HELLMAN KEY DISTRIBUTION ON ARDUINO ATMEGA2560 IOT DEVICES," J. Tek. Inform. Jutif, vol. 4, no. 4, pp. 849–855, Aug. 2023, doi: 10.52436/1.jutif.2023.4.4.1129.
[21]. T. Zebua, "Penerapan Multiply With Carry Generator pada Proses Pembangkitan Kunci Algoritma Beaufort Cipher," J. Inf. Syst. Res. JOSH, vol. 4, no. 2, pp. 607–613, Jan. 2023, doi: 10.47065/josh.v4i2.2928.
[22]. A. H. Hasugian, Y. R. Nasution, and N. A. Simanjuntak, "KOMBINASI ALGORITMA BEAUFORT CIPHER DAN LSB2BIT UNTUK KEAMANAN FILE TEXT," J. Inform., vol. 6, no. 1, 2023.
[23]. S. Agustini, W. M. Rahmawati, and M. Kurniawan, "Modified Vegenere Cipher to Enhance Data Security Using Monoalphabetic Cipher," Int. J. Artif. Intell. Robot. IJAIR, vol. 1, no. 1, pp. 26–32, Nov. 2019, doi: 10.25139/ijair.v1i1.2029.
[24]. V. V. K. Reddy and S. Bhukya, "ENCRYPT AND DECRYPT IMAGE USING VIGENERE CIPHER".
[25]. T. Hassan Hameed and H. Tariq Sadeeq, "Modified Vigenère cipher algorithm based on new key generation method," Indones. J. Electr. Eng. Comput. Sci., vol. 28, no. 2, p. 954, Nov. 2022, doi: 10.11591/ijeecs.v28.i2.pp954-961.
[26]. B. A. Esttaifan, "A Modified Vigenère Cipher based on Time and Biometrics features," J. Eng., vol. 29, no. 6, pp. 128–139, Jun. 2023, doi: 10.31026/j.eng.2023.06.10.
[27]. M. A. Budiman, Handrizal, and S. Azzahra, "An implementation of Rabin-p cryptosystem and affine cipher in a hybrid scheme to secure text," J. Phys. Conf. Ser., vol. 1898, no. 1, p. 012042, Jun. 2021, doi: 10.1088/1742-6596/1898/1/012042.
[28]. M. Jannah, B. Surarso, and Sutimin, "A combination of Rivest Shamir Adlemann (RSA) and Affine Cipher method on improvement of the effectiveness and security of text message," J. Phys. Conf. Ser., vol. 1217, no. 1, p. 012073, May 2019, doi: 10.1088/1742-6596/1217/1/012073.
[29]. J. C. T, "A Keystream-Based Affine Cipher for Dynamic Encryption," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 7, pp. 2919–2922, Jul. 2020, doi: 10.30534/ijeter/2020/06872020.
[30]. P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," Mathematics, vol. 10, no. 20, p. 3878, Oct. 2022, doi: 10.3390/math10203878.
[31]. R. Nisviasari, Dafik, I. H. Agustin, E. Y. Kurniawati, I. N. Maylisa, and B. J. Septory, "Improving the robustness of the affine cipher by using a rainbow antimagic coloring," J. Phys. Conf. Ser., vol. 2157, no. 1, p. 012017, Jan. 2022, doi: 10.1088/1742-6596/2157/1/012017.
[32]. K. R. Olayinka and S. Wilson, "Towards Securing Electronic Health Records using Ceasar And Affine Cryptographic Techniques," vol. 7, no. 12, 2022.
[33]. M. Fadlan, Suprianto, Muhammad, and Y. Amaliah, "Double Layered Text Encryption using Beaufort and Hill Cipher Techniques," in 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia: IEEE, Nov. 2020, pp. 1–6. doi: 10.1109/ICIC50835.2020.9288538.
[34]. C. AtikaSari, D. W. Utomo, and M. A. S. Doheir, "Visual Analysis Based on CMY and RGB Image Cryptography Using Vigenere and Beaufort Cipher," Kinet. Game Technol. Inf. Syst. Comput. Netw. Comput. Electron. Control, May 2023, doi: 10.22219/kinetik.v8i2.1664.
[35]. C. Irawan, E. H. Rachmawanto, C. A. Sari, and C. A. Sugianto, "SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM," 2020.
[36]. E. Sugiarto et al., "Securing Text Messages using the Beaufort-Vigenere Hybrid Method," J. Phys. Conf. Ser., vol. 1577, no. 1, p. 012032, Jul. 2020, doi: 10.1088/1742-6596/1577/1/012032.
[37]. L. B. Handoko and A. Abdussalam, "Text Security Using Vigenere Cipher and Hill Cipher," Bit Fak. Teknol. Inf. Univ. Budi Luhur, vol. 19, no. 1, p. 37, Apr. 2022, doi: 10.36080/bit.v19i1.1790.
[38]. P. Derbez, P.-A. Fouque, B. Lambin, and B. Minaud, "On Recovering Affine Encodings in White-Box Implementations," IACR Trans. Cryptogr. Hardw. Embed. Syst., pp. 121–149, Aug. 2018, doi: 10.46586/tches.v2018.i3.121-149.