Revisiting the Vigenère Cipher: Security Evaluation and Modern Relevance

Oorjitha B, Chevuri Sri Bhavani, Nyneisha Baratam, Sagar Basavaraju
Department of Electronics and Communication Engineering
Amrita School of Engineering, Bengaluru
Amrita Vishwa Vidyapeetham, India
{bl.en.u4eac22040@bl.students.amrita.edu,
bl.en.u4eac22081@bl.students.amrita.edu,
bl.en.u4eac22038@bl.students.amrita.edu,
b_sagar@blr.amrita.edu}

***Abstract*—The foundation of today's cryptography is secure mathematical algorithms like AES and RSA. Nevertheless, before computers became widespread, classical polyalphabetic ciphers, including the Vigenère cipher, were thought to be secure because of their ability to mask simple frequency-based analysis. This paper re-evaluates the Vigenère cipher and some of its variations, namely Beaufort, Gronsfeld, and Porta ciphers, analyzing the historical significance, structure, and weaknesses associated with these methods. Specifically, this paper will discuss the factors that made these ciphers secure at some point, the way they were broken using statistical cryptanalysis techniques like Kasiski examination and index of coincidence. Additionally, a comparative implementation using AES-CBC to understand why modern cryptographic systems are better than classical ciphers. The paper evaluates the relevance of these ciphers in the modern world.**

***Index Terms*—Vigenère cipher, Beaufort cipher, Porta cipher, Gronsfeld cipher, AES-CBC, Kasiski Examination, Index of Coincidence, frequency analysis, polyalphabetic encryption, cryptanalysis**

I. Introduction

Cryptography has evolved from simple manual enciphering techniques to highly sophisticated mathematical techniques ensuring computational security. Before the development of the latest cryptographic systems, confidentiality in communications was achieved mainly through classical cipher techniques that sought to mask the presence of any patterns in plain English text. The Vigenère cipher system is one of the important achievements in this evolution of cryptography characterized by the use of a polyalphabetic cipher technique that employs different substitution alphabets based on a key.

The Vigenère cipher contrasts with monoalphabetic ciphers like the Caesar cipher because it uses several alphabets instead of one. For instance, the use of different alphabets ensures that the frequencies of characters are spread out. In turn, the method is less prone to frequency attacks [5]. Over the years, several variations of the cipher have been created to change the encryption process without altering the underlying idea of substituting characters based on a key. Examples include the Beaufort, Gronsfeld, and Porta ciphers.

The effectiveness of these ciphers was finally put under scrutiny by means of statistics-based cryptanalysis techniques. The Index of Coincidence of Friedman served as a mathematical way to uncover the frequencies involved in the cipher, while Kasiski's Test allowed estimating the length of the key by making use of recurring ciphertexts [1]. In summary, these techniques have proven that using repetitive keys leaves a pattern which allows dividing the ciphertext into several monoalphabetic segments. Shannon's information-theoretic approach has shown that this technique cannot achieve absolute secrecy due to language redundancy [2].

The introduction of computer-based technology has made apparent the weaknesses of traditional polyalphabetic ciphers. With today's cryptanalytical approaches, like automatic cryptanalysis and machine learning, quick analyses of ciphertexts are possible, making repeating-key ciphers obsolete for securing communications in the contemporary era. In comparison, recent cryptographic functions like AES and RSA rely on computational difficulty, large keyspace, and randomization processes apart from the statistical security that traditional systems depend on. This paper applies empirical evidence by using the AES-CBC function to conduct an analysis of its ciphertexts with respect to traditional statistical cryptanalysis methods.

Despite the ineffectiveness of classical encryption systems in modern times, they still play important roles in illustrating some fundamentals of cryptography such as substitution techniques, key management, entropy, and statistical attacks. While past studies have mostly focused on one particular system or specific types of attacks on classical ciphers, there is a lack of literature analyzing different polyalphabetic systems comparatively under statistical cryptanalysis. Therefore, this study will revisit the Vigenere cipher along with its variants (Beaufort, Gronsfeld, and Porta) in order to analyze the weaknesses under statistical cryptanalysis techniques while considering the role of key lengths and ciphertexts sizes.

A. Contributions of the Paper

The main contributions of this paper are as follows:

- C1: A unified study of the Vigenère cipher and its variants—Beaufort, Gronsfeld, and Porta—highlighting their structural similarities.

- C2: Implementation of classical polyalphabetic encryption and decryption mechanisms along with statistical cryptanalysis techniques such as Kasiski Examination and Index of Coincidence.
- C3: Experimental evaluation using real-world text datasets to analyze key length detection and cipher behavior.
- C4: Demonstration that structural modifications do not eliminate vulnerabilities arising from periodic key repetition.
- C5: A comprehensive analysis linking the weaknesses of classical cryptography to the evolution and necessity of modern cryptographic systems.
- C6: Comparative evaluation of AES-CBC against classical statistical cryptanalysis to demonstrate the elimination of exploitable periodic structures in modern cryptographic systems.

B. Organization of the Paper

The rest of this document will be structured as follows. In Section II, literature review on theories and developments on classical cryptography and cryptanalysis will be made. Section III covers the methodology used in this study, which includes the dataset creation process, the ciphers to be implemented and the evaluation procedures. The experimental findings and discussion thereof will be presented in Section IV. Lastly, conclusions drawn from the experiments as well as future directions in this field will be given in Section V.

II. Literature Survey

The contributions made by Friedman to the Index of Coincidence (IC) represent one of the earliest applications of mathematics to cryptanalysis. It represents the development of a mathematical criterion that differentiates between monoalphabetic and polyalphabetic ciphers. He used the probability of having repetitive characters to show that a message encrypted using a periodic key has identifiable features. He divided the ciphertext into several columns based on the period lengths and identified spikes in IC values, which revealed the period lengths of the ciphertext. This means that messages encrypted using polyalphabetic ciphers, such as Vigenère ciphers, could be reduced to monoalphabetic ciphers after determining the periods [1].

Shannon's theory of secrecy systems provides a strict mathematical description of the constraints of classical cryptography techniques. Through the use of entropy and equivocation measures, Shannon established that perfect secrecy can be achieved only if the length of the key is equal to the length of the message. From his theory, it is evident that repeated key systems cannot provide any secret information because of the nature of language, whereby the uncertainty of the message reduces as more and more lengthy messages are deciphered [2].

Mohan et al. conducted an extensive evaluation of classical cryptosystems, examining the advantages and disadvantages of substitution cryptosystems. The authors described how polyalphabetic cryptosystems have an advantage over monoalphabetic cryptosystems in terms of reducing frequency occurrences but still become vulnerable to Kasiski Examination and index of coincidence attacks. Additionally, the authors presented their own version of Vigenère cryptosystem, utilizing non-repetitive keys by employing different transformations. It has been concluded that the greatest weakness of classical cryptosystems is not complexity but repetition of keys [3].

Omran et al. proposed a systematic cryptanalytic approach using genetic algorithms for the cracking of the Vigenère cipher. In this process, a genetic code is generated from each candidate key, and its fitness is calculated based on the degree of similarity of the frequencies of this code to natural language. With the help of selection, crossover, and mutation operations, the key of the message is identified by this algorithm effectively. The work demonstrates that the proposed approach can find the key length and values faster than any other traditional brute force approach [4].

The work by Aliyu and Olaniyan provides an in-depth historical and critical analysis of the Vigenere cipher and its different versions. This includes a discussion about the history of the cipher, starting from Bellaso up to its latest iterations, and explains why the cipher has been considered secure for hundreds of years due to the fact that it can hide the frequency distribution. It also analyzes existing attack methods like Kasiski Examination and Index of Coincidence while highlighting the importance of repeated periodic key in reducing the cipher's strength [5].

Purwanti et al. reassess the Vigenère cipher in light of modern applications, determining whether it can be considered a reliable option for current use in securing sensitive information. The research identifies the encryption and decryption process based on the use of the tabula recta and evaluates its efficiency in terms of protecting sensitive information. While this cipher continues to remain relatively simple and easy to implement, the paper identifies the vulnerability of the code when used in conjunction with short key strings [6].

Kusumah et al. undertook a systematic review on the Beaufort Cipher and its relationship to other cipher algorithms like the Vigenere and Affine cipher. In this analysis, which employed structured literature review techniques, the researchers observed recent trends in the research and an emerging trend in classical cryptography. According to their results, while the structure of the Beaufort can vary as in the case of its self-reciprocal nature, the cipher is still vulnerable to repeating keys [7].

Ketha presented a comprehensive overview of the evolution of cryptography from classical substitution systems to modern encryption algorithms. The study compares different cryptographic approaches based on security, efficiency, and resistance to attacks, emphasizing that classical ciphers fail due to predictable patterns and limited key spaces. In contrast, modern systems rely on computational complexity and large key sizes. This work provides a broader context for understanding the transition from classical to modern cryptography [8].

Park et al. propose a deep learning methodology involving the application of a generative adversarial network (GAN) for cracking classic cryptographic algorithms. The network automatically learns the mapping between ciphertext and plaintext without any need for pre-existing knowledge about the statistics of the language used in encoding the message. Tests performed show a high degree of accuracy above 97%, suggesting that classic cryptography systems can easily be cracked through modern AI algorithms. [9].

Classical cryptography in the existing literature is based on the Index of Coincidence proposed by Friedman and information theory propounded by Shannon, along with research on specific ciphers and attack algorithms on them. However, most of the literature on cryptography either concentrates on specific ciphers, theory of cryptography or on the specific attack algorithms used. The current paper aims to provide a single framework of study for the Vigenère cipher and related ciphers like Beaufort, Gronsfeld, and Porta.

III. Methodology

A. Experimental Design and Dataset Preparation

The study evaluates the resistance of four classical polyalphabetic ciphers (Vigenère, Beaufort, Gronsfeld, and Porta) against standard statistical cryptanalysis techniques. Experiments used realistic natural-language plaintext to preserve linguistic properties such as letter frequencies, digraph/trigraph repetitions, and redundancy that these attacks exploit.

Plaintext was drawn from the NLTK Gutenberg corpus (literary works in standard English). Samples of four sizes were prepared: 1000, 3000, 6000, and 10,000 characters. This range allowed assessment of how ciphertext length affects attack success. Preprocessing steps were applied uniformly:

1) Remove spaces, punctuation, digits, and special characters.
2) Convert to uppercase.
3) Retain only A–Z letters.
4) Map letters to integers: $A = 0, B = 1, \ldots, Z = 25$.

This produced clean alphabetic streams suitable for modular arithmetic and statistical analysis.

B. Key Generation

To ensure unbiased evaluation, keys were generated randomly for each run. Tested key lengths were 3, 4, 6, 8, and 12. These represent short to moderately long periods.

C. Cipher Implementations

All ciphers were implemented in a unified Python framework using periodic repeating keys. The pseudocodes are as follows:

Algorithm 1 Vigenère Encryption

Require: Plaintext P, Key K
Ensure: Ciphertext C
for $i = 0$ to $|P| - 1$ **do**
  $k \leftarrow K[i \bmod |K|]$
  $C[i] \leftarrow (P[i] + k) \bmod 26$
end for

Vigenère Cipher – A polyalphabetic substitution cipher that encrypts plaintext using repeated alphabetic key shifts.

Algorithm 2 Beaufort Encryption

Require: Plaintext P, Key K
Ensure: Ciphertext C
for $i = 0$ to $|P| - 1$ **do**
  $k \leftarrow K[i \bmod |K|]$
  $C[i] \leftarrow (k - P[i]) \bmod 26$
end for

Beaufort Cipher – A variant of Vigenère where encryption is performed using reverse subtraction of plaintext letters from key letters.

Algorithm 3 Gronsfeld Encryption

Require: Plaintext P, Digit Key D
Ensure: Ciphertext C
for $i = 0$ to $|P| - 1$ **do**
  $d \leftarrow D[i \bmod |D|]$
  $C[i] \leftarrow (P[i] + d) \bmod 26$
end for

Gronsfeld Cipher – A simplified Vigenère cipher that uses numeric digits as the repeating key instead of letters.

Algorithm 4 Porta Encryption

Require: Plaintext P, Key K
Ensure: Ciphertext C
for $i = 0$ to $|P| - 1$ **do**
  Select row using $K[i \bmod |K|]$
  Substitute $P[i]$ using Porta table
end for

Porta Cipher – A polyalphabetic substitution cipher that uses paired key letters and a lookup table for encryption instead of modular arithmetic.

D. AES-CBC Comparative Implementation

In order to contrast classical and modern cryptography techniques, the AES-CBC algorithm was tested in an identical experimental environment. AES does not operate like repeating-key polyalphabetic cryptosystems but employs substitution-permutation cycles and randomizes blocks through chaining [12]. This results in ciphertext that is indistinguishable from random noise. Different sized plaintext messages were encrypted using random AES keys, and their Base64 ciphertext was evaluated by calculating IC and utilizing the Kasiski test just as the classical cryptosystems. However, unlike the classical systems, there are no repetitive key cycles within AES.

Algorithm 5 AES-CBC Comparative Statistical Analysis

Require: Plaintext sample P, user-defined key K
Ensure: Statistical characteristics of AES-CBC ciphertext

Expand or repeat K to obtain a 128-bit AES key
Generate a random 128-bit initialization vector IV
Apply PKCS#7 padding to P
Encrypt padded plaintext using AES-CBC with key K and IV
Encode the binary ciphertext using Base64
Remove non-alphabetic symbols for compatibility with IC and Kasiski analysis
Compute the raw Index of Coincidence (IC)
Apply Kasiski Examination to detect repeated patterns
Record:
- Average IC value
- Kasiski output
- Execution time

Return the computed statistical measurements

E. Cryptanalysis Techniques

Two classic statistical cryptanalysis techniques were implemented in this study:

Kasiski Examination: The Kasiski Test detects key length from repetitions in ciphertexts, mainly trigrams. When identical segments of plaintext are encoded using identical key segments, then repetition in the ciphertext will occur at intervals that are related to the period of the key. The key length can be approximated from the GCD of these intervals.

Index of Coincidence (IC): The Index of Coincidence (IC) indicates the degree of closeness of ciphertext letter frequency distribution to that of standard English language. Each hypothetical value of key length k divides the text into k cosets, with calculation of mean IC. Higher IC means more probable key lengths because proper separation yields a monoalphabetic-like cipher. The values of k tested were between 1 and 15, for keys with lengths 3, 4, 6, 8, and 12 [5].

The IC is calculated as:

$$IC = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{N(N-1)} \tag{1}$$

where f_i is the frequency of letter i and N is the total number of letters.

F. Evaluation Procedure and Metrics

Fig. 1 illustrates the evaluation procedure followed in this study. Plaintext is first preprocessed and encrypted using the selected cipher with a randomly generated key of fixed length. The resulting ciphertext is then analyzed using Kasiski Examination and Index of Coincidence to estimate the key length. The predicted values are compared with the actual key length to evaluate accuracy, while execution time is recorded to measure computational efficiency.

Metrics:

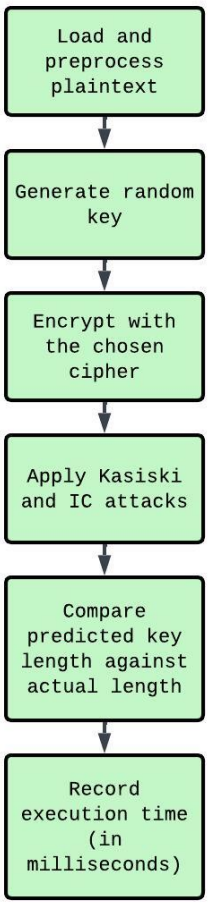

Fig. 1. Flowchart of the evaluation pipeline implemented in accordance with established methodologies in classical cryptanalysis.

- **Accuracy**: Fraction of runs where the correct key length was detected. In practice, IC-based estimation demonstrated higher stability and reliability than Kasiski Examination due to the latter's sensitivity to noisy repetition distances and accidental ciphertext alignments.
- **Execution Time**: Total time for encryption + cryptanalysis.

Experiments were repeated multiple times for each configuration to ensure statistical reliability. The obtained results consisted of predicted key lengths from Kasiski Examination and Index of Coincidence, correctness of each prediction, and execution time measurements. These outputs were then used to compute overall accuracy, compare cipher-wise performance, analyze the effect of text size and key length, and generate summary statistics and visualizations.

This methodology ensures reproducibility, controls for confounding variables (text statistics, key randomness), and provides both quantitative metrics and visual insights into cipher behavior.

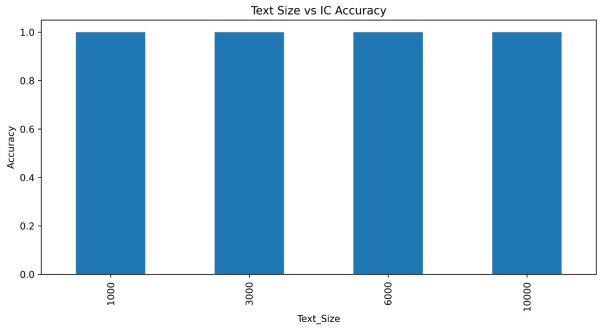

Fig. 2. Effect of Text Size on IC Accuracy

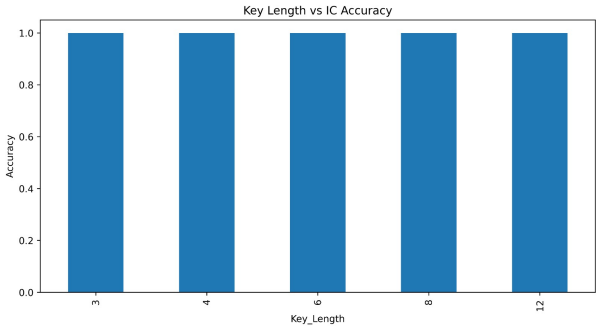

Fig. 3. Effect of Key Length on IC Accuracy

IV. Results and Analysis

The classic polyalphabetic ciphers such as Vigenère, Beaufort, Gronsfeld, and Porta cipher became an important stage in the development of cryptography. Polyalphabetic ciphers utilized a number of substitute alphabets, which would shift with periodicity according to the key. As opposed to the Caesar cipher and other monoalphabetic ciphers, the polyalphabetic ciphers could resist manual cryptanalysis with frequency analysis [5], [10]. However, these ciphers were rather vulnerable and required limited access to the ciphertext and insufficient cryptanalytic skills. The current part explores their vulnerability and discusses their replacement by more advanced ciphers.

A. Scenario 1: Effect of Text Length on Cryptanalysis

One of the primary objectives of this study was to evaluate the vulnerabilities of classical ciphers under statistical cryptanalysis. Results showed that ciphertext length significantly affects the success of Index of Coincidence (IC)-based attacks [1]. As shown in Fig. 2, shorter ciphertexts (≈1000 characters) produced unstable predictions due to insufficient statistical redundancy, whereas larger texts (up to 10000 characters) preserved stronger English-language frequency distributions and improved IC accuracy.

These results confirm that larger ciphertext samples make repeating-key periodicity more detectable [5]. Compared to Kasiski Examination, IC analysis produced more stable and reliable predictions because Kasiski relies heavily on exact repeated sequence alignment and GCD computation, making it more sensitive to noise and accidental repetitions in ciphertext.

B. Scenario 2: Effect of Key Length

Experiments evaluating the impact of key length revealed that while longer keys increase resistance marginally, they do not eliminate the fundamental vulnerability of periodic repetition. Moderate and long keys were successfully identified using IC analysis because the repeating cycle remains embedded in the ciphertext. Very short keys sometimes introduced harmonic peaks, causing temporary ambiguity between the actual key length and its multiples as shown in Fig. 3. Nevertheless, the effective search space was substantially reduced in all cases, allowing efficient segmentation into monoalphabetic streams.

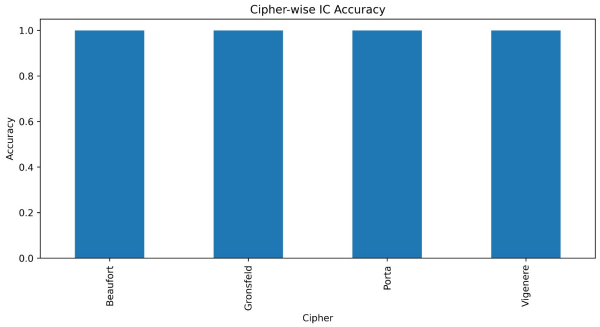

Fig. 4. Accuracy Comparison Across Ciphers

TABLE I
Comparative Structural Analysis of Evaluated Ciphers

Cipher	Key Type	Method	Core Weakness
Vigenère	Alphabetic	Addition mod 26	Repeating key
Beaufort	Alphabetic	Subtraction mod 26	Repeating key
Gronsfeld	Numeric	Digit shifts	Small key space & repetition
Porta	Alphabetic	Table substitution	Repeating key

These results highlight a key weakness: even extended keys cannot overcome the structural flaw of key repetition.

C. Scenario 3: Comparative Performance Across Ciphers

In line with the objective to study Vigenère, Beaufort, Gronsfeld, and Porta ciphers, a unified implementation and evaluation was performed. As observed in Fig. 4, all four ciphers exhibited remarkably similar performance under IC-based cryptanalysis, with only marginal differences observed, consistent with findings in recent security analyses [3], [4].

The experiments confirm that modifications in substitution methods or key type provide negligible improvement in security when the repeating-key mechanism remains unchanged [7]. This supports the conclusion that the dominant vulnerability is structural rather than algorithmic.

Table I summarizes the structural characteristics of the evaluated ciphers, highlighting that despite differences in key representation and substitution method, all variants share the same fundamental weakness of repeating keys.

TABLE II
WHY CLASSICAL CIPHERS FAIL IN MODERN SCENARIOS

Threat	Cipher Response	Outcome
Brute force	Small key space	Key recovered
Statistical attack	Repeating patterns	Key length detected
Known plaintext	No randomness	Plaintext exposed
Chosen plaintext	Predictable mapping	Key inferred
Interception	Offline analysis	Data broken
Tampering	No authentication	Undetected changes

TABLE III
STATISTICAL BEHAVIOR: CLASSICAL CIPHERS VS AES-CBC

Property	Classical Ciphers	AES-CBC
Repeating Key Structure	Present	Absent
Periodic Patterns	Detectable	Non-detectable
IC-Based Key Estimation	Effective	Ineffective
Kasiski Examination	Partially Effective	Unstable/Random
Ciphertext Statistics	Language-dependent	Near-random
Security Basis	Pattern concealment	Computational hardness

D. Failure of Classical Ciphers Against Statistical Attacks

Once the key size was estimated, the encryption could be divided into multiple monoalphabetic codes, which can be easily broken using frequency analysis methods. This demonstrates the concept proposed by Shannon, according to which language redundancy becomes a disadvantage when the same key is used multiple times. [2]. All stages of the cryptanalysis, including determination of the key size through IC and Kasiski analysis, up to decrypting the message, were demonstrated in the experiment [6], [9]. Nowadays, due to computerization, artificial intelligence, and genetic algorithms, the vulnerability of such systems becomes more evident [4], [9], [14].

Table II provides a consolidated view of common attack scenarios and illustrates how classical ciphers fail to provide adequate security under modern computational conditions.

E. Comparative Analysis with AES-CBC

AES-CBC, along with classical polyalphabetic ciphers, under the same circumstances, does not have any stable periodic patterns to detect key length based on statistical methods. Fig. 5 reveals that classical ciphers maintain a higher average IC due to redundancy of language, as well as repeating-key periodicity, whereas AES-CBC demonstrates significantly lower IC, which approaches randomness.

Similarly, Kasiski test also proves ineffective as repeated segments occur randomly without any correlation to cyclic key repetition. It thus appears that modern cryptography eliminates the use of repeating-key periodicity, which classical cryptanalysis exploits. Given the inclusion of random IVs, diffusion, and substitutions, AES-CBC avoids any predictable patterns, hence the transition from pattern-based cryptography to computational cryptography.

Table III summarizes the key experimental differences between classical polyalphabetic ciphers and AES-CBC, highlighting how the absence of repeating-key periodicity and the use of computationally secure transformations render classical statistical attacks ineffective against modern cryptographic systems.

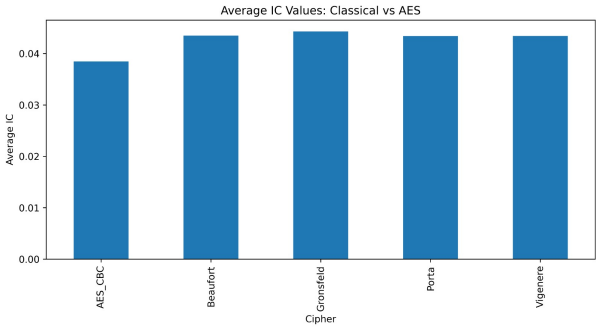

Fig. 5. Average IC Values: Classical Ciphers vs AES-CBC

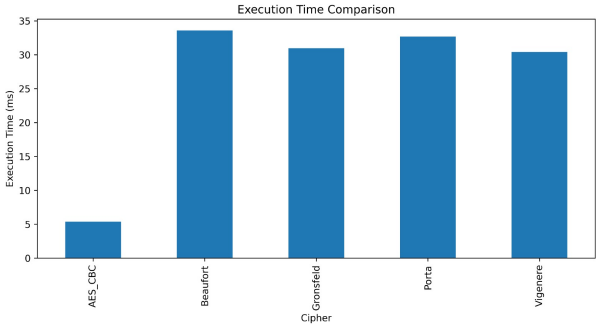

Fig. 6. Execution Time Comparison

TABLE IV
CLASSICAL VS MODERN CRYPTOGRAPHY

Feature	Classical Ciphers	Modern Cryptography
Security Basis	Pattern concealment & repetition	Computational hardness & randomness
Key Space	Small / repeating	Extremely large
Attack Type	Statistical & manual	Mathematical & side-channel
Randomness	Minimal	Strong (nonces/IVs)
Integrity Protection	None	MAC / AEAD
Speed	Very high	Moderate to high
Practical Security	Low	High

F. Computational Efficiency and Performance Analysis

All four ciphers demonstrated high computational efficiency, with encryption and decryption completed within milliseconds for all tested configurations. As shown in Fig. 6, Gronsfeld recorded the lowest execution time, while Porta showed comparatively higher runtime due to its substitution-table lookup mechanism. Although these classical ciphers are lightweight and suitable for low-resource environments, their simple repeating-key structure also enables rapid cryptanalysis using modern computational tools. Table IV highlights the transition from classical pattern-based security to modern cryptographic systems based on computational hardness, randomness, and advanced secure communication frameworks such as quantum key distribution [16].

G. Overall Statistical Summary

In terms of accuracy in estimation of the key length, experiments prove that the Index of Coincidence (IC) was superior to the Kasiski Examination approach in all cases. The use of longer text samples led to more accurate results for both IC and Kasiski approaches by increasing stability of frequency characteristics of ciphers. Distinctions between Vigenère, Beaufort, Gronsfeld, and Porta ciphers were not substantial, which means that variations in cipher structures are not very effective measures of adding additional security to ciphers with repeated keys.

H. Modern Relevance and Educational Value

Although classical polyalphabetic ciphers are obsolete for secure communication, they remain important for understanding fundamental cryptographic concepts such as substitution, modular arithmetic, key management, entropy, and statistical cryptanalysis [8]. They also provide historical insight into the evolution of cryptography and help illustrate why modern systems such as AES, RSA, ChaCha20, and elliptic curve cryptography were developed to achieve computational security through large key spaces, randomness, and mathematically secure designs [10], [13], [15].

I. Key Findings and Contribution Assessment

The experimental results validate all the contributions outlined in this study. The unified implementation and analysis of Vigenère, Beaufort, Gronsfeld, and Porta ciphers demonstrate that despite differences in structure, all exhibit similar vulnerabilities due to repeating key mechanisms. The application of Kasiski Examination and Index of Coincidence effectively enabled key length detection across varying text sizes and key lengths, confirming the influence of ciphertext length on attack success. Overall, the findings establish that structural modifications do not enhance security and reinforce the objective of highlighting the inherent limitations of classical polyalphabetic ciphers.

V. Conclusion

This study presented a unified experimental analysis of the Vigenère cipher and its variants—Beaufort, Gronsfeld, and Porta—to evaluate their resistance to statistical cryptanalysis. Experimental results showed that despite structural differences, all four ciphers remain vulnerable due to repeating-key periodicity. Techniques such as the Index of Coincidence successfully enabled key-length estimation and ciphertext analysis, confirming that the primary weakness of these systems lies in key reuse rather than substitution design.

The AES-CBC comparison further demonstrated the transition from classical pattern-based security to modern computational cryptography. Unlike classical ciphers, AES-CBC produced statistically randomized ciphertext resistant to classical cryptanalysis techniques such as IC and Kasiski Examination. Although classical polyalphabetic ciphers are no longer suitable for secure communication, they remain important for understanding the historical evolution and foundational concepts of cryptography. Future work may extend this analysis using automated or AI-based cryptanalysis methods.

VI. Acknowledgement

The authors gratefully acknowledge Sri Mata Amritanandamayi Devi (Amma), Chancellor, Amrita Vishwa Vidyapeetham, for her inspiration and for providing financial support.

References

[1] W. F. Friedman, *The Index of Coincidence and Its Applications in Cryptanalysis*. Technical Paper, 1928.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, 1949.

[3] M. Mohan, M. K. K. Devi, and V. J. Prakash, "Security analysis and modification of classical encryption scheme," *Indian Journal of Science and Technology*, vol. 8, no. S8, p. 542, 2015.

[4] S. S. Omran, A. S. Al-Khalid, and D. M. Al-Saady, "A cryptanalytic attack on Vigenère cipher using genetic algorithm," in *Proc. IEEE*, 2011, p. 59.

[5] A.-A. M. Aliyu and A. Olaniyan, "Vigenere cipher: Trends, review and possible modifications," *International Journal of Computer Applications*, vol. 135, no. 11, pp. 46–47, 2016.

[6] Purwanti, S. D. Nurcahya, and D. Nazelliana, "Message security in classical cryptography using the Vigenere cipher method," *International Journal of Software Engineering and Computer Science*, vol. 4, no. 1, pp. 350–357, 2024.

[7] P. A. D. Kusumah, K. Kusrini, and K. Kusnawi, "Optimizing data security: A literature review on the implementation of Beaufort cipher for Vigenere affine cipher," *International Journal of Innovative Science and Research Technology*, vol. 9, no. 2, pp. 681–682, 2024.

[8] A. Ketha, "The evolution of cryptography and a contextual analysis of the major modern schemes," 2023.

[9] S. Park, H. Kim, and I. Moon, "Automated classical cipher emulation attacks via unified unsupervised generative adversarial networks," *Cryptography*, vol. 7, p. 35, 2023.

[10] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication*. 1967.

[11] R. M. Jacob, P. K., and A. P. P., "Application of visual cryptography scheme in software watermarking," in *Proc. ICOEI*, 2020, pp. 1044–1048.

[12] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.

[13] K. J. Kumar *et al.*, "A comprehensive end-to-end solution for web security with cryptography, multi-factor authentication, and secure communication," in *Proc. IDCIoT*, 2025, pp. 325–332.

[14] K. Amit, G. S. S. Sravya, K. D. Sai, and S. Basavaraju, "Evaluating machine learning algorithms with feature selection for cybersecurity: A case study on Pegasus spyware," in *Proc. IEEE ICSC*, 2025, pp. 381–386.

[15] C. Ramakrishna *et al.*, "A secure authenticated image encryption scheme based on elliptic curve cryptography," *International Journal of Computers and Applications*, 2023.

[16] N. Jain *et al.*, "Attacks on practical quantum key distribution systems and how to prevent them," *Contemporary Physics*, vol. 57, 2015.