International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(15s) 2026 pp. 638-650
https://doi.org/10.70917/ijcisim-2026-4442
Article

Design and analysis of Symmetric Cipher for Mobile Device Encryption Based on Extended Classical Techniques: VIgPLAY

Sarita Singh1, Y.D.S. Arya2, Akash Sanghi3*, Laxmi Shanker Maurya4

1Department of Computer Science & Engineering, Invertis University, Bareilly UP, India, er.sarita2014@gmail.com
2Department of Computer Science & Engineering, Invertis University, Bareilly UP, India, vc@invertis.org
3*Department of Computer Applications, Invertis University UP, India, sanghiakash@gmail.com
4Department of Computer Science & Engineering, Ashoka Institute of Technology and Management, Varanasi, UP, India, lsmaurya@gmail.com

Abstract: Nowadays, huge data concerning every human is travelling in all directions. So, data is crucial for everyone's life. We need to secure this data. There are many scientists and researchers who have used various approaches for data security. We are well aware of the Cipher approach which converts message into an unreadable format (Cipher Text). In cryptography there are two types of Cipher's: Substitution Cipher and Transposition Cipher. In this paper we have implemented a new symmetric cipher which has dual nature of Security along with this we have enhanced the structure of the matrix of Playfair Cipher (6*6) and Vigenère Cipher (36*36) which is supported for alphanumeric encryption in mobile app and LCG method for generate the random numbers. The VigPlay Cipher is built for speed and efficiency. In our results, it encrypted data in 1.63 ms and decrypted it in 0.98 ms, achieving a massive throughput of 200,231.48 KB/s on a lean 72.2 MB memory budget. Compared to heavyweights like AES, DES, and Blowfish, as well as classic ciphers like Playfair and Vigenère, VigPlay proves to be a faster, more lightweight alternative tailored perfectly for mobile app security. We combined Vigplay cipher with a dynamic substitution method (using an LCG) to create a much harder defense against common hacking methods, including brute-force attacks and frequency analysis. This hybrid approach makes the encrypted data far more random and highly sensitive to key changes, all while keeping things running fast. Our tests and charts prove that this model successfully delivers the best of both worlds: robust security that doesn't drag down execution speed or memory. This study provides a new dual-layer symmetric encryption technique that combines an enhanced 6x6 Playfair cipher and an enlarged 36x36 Vigenère cipher to permit alphanumeric input. Improved security against frequency analysis and brute-force attacks. The proposed method is suitable for mobile applications and resource-constrained environments and can be further extended using post-quantum cryptographic techniques and secure key distribution mechanisms for future secure communication systems.

Keywords: Playfair Cipher, Vigenère Cipher, Plain text, cipher text, Encryption.

1. INTRODUCTION

The exponential increase in data transfer and storage in the digital age necessitates the implementation of strong security measures for sensitive data within mobile applications. To produce strong security systems appropriate for contemporary uses, the fundamentals of classical cryptography can be expanded upon and integrated. Traditionally applied over a 26×26 matrix (alphabet only), the Vigenère cipher is a polyalphabetic substitution cipher. It applies several Caesar shifts to plaintext using a keyword.

Until the 19th century, Kasiski's key repetition method for determining key length made it seem unbreakable. Military communications employed the playfair cipher, which is a digraph substitution cipher that uses a 5x5 matrix to encrypt letter pairings, usually by combining "I/J" or omitting "J," but bigram frequency analysis can detect it. These ciphers have been extended.

This has been achieved by recent research. In a 6x6 Playfair matrix, for example, the character set is expanded to 36 by including numerals (0, 9) in addition to alphabets; this expansion allows for a fuller representation of the data. Since the Vigenère encryption has been modified to use randomized key generation to prevent cryptanalysis and wider matrices to accommodate alphanumeric characters, it has improved security features.

2. RELATED WORK

The writers of this paper focused on researching a type of substitution cipher. Playfair cipher and examine three enhanced iterations of the 3D Playfair cipher. After then, a conclusion was reached regarding these three enhanced Playfair cipher variants. Lastly, it anticipates the advancement of cryptography and the Playfair cipher in the future [1].

In this study, the authors proposed an enhanced key security of Playfair cipher algorithm using Playfair cipher 16x16 matrix, XOR, two's complement, and bit swapping. The result of the study shows that the processing time for encryption and decryption processes are linearly proportional. It means the longer characters of the key; the more significant times needed to encrypt and decrypt the key. Also, the proposed method is faster than the existing key security of Playfair cipher algorithm [2].

In this research, a modified Advanced Encryption Standard (AES) cipher system with Cipher Block Chaining (CBC) mode based on a one-time pad (OTP) cipher is used to encrypt and decrypt classified text files in the Kurdish alphabet. Additionally, the given method transmits randomly generated secret keys for both AES and OTP via unreliable channels using a modified RSA cipher system. Instead of using two huge prime numbers, the modified RSA cipher system selects two large co-prime numbers at random under the constraint that each have a maximum of two factors [3].

The goal of this thesis is to use the RSA technique to secure the key of the new extended size 16x16 play fair procedure. There are two stages to the algorithm. I utilized matrix 5x5 rules to create a matrix and cipher text at the first stage at the sender's end. Both lowercase and uppercase alphabets, numbers, and special characters are used to form the matrix's contents. The matrix is then rotated using shifting values.

In the second stage, the play fair ciphers' key is safely transmitted using the RSA public key encryption technique, and the receiver end creates a play fair matrix using this key [4].

In this Paper the author’s proposed Playfair cipher highlights the integration of randomly generated numbers and color substitution techniques that further strengthens the encryption process, which leads to improved data privacy [5].

The study suggests a modified Playfair encryption method for RGB image encryption that makes use of the Block Cipher encryption principle. It consists of three steps: first, a 4x4 Playfair matrix is created instead of the traditional 5x5 matrix; second, image pixels are encrypted using the modified Playfair matrix in conjunction with the Cipher Block Chaining (CBC) mode of operation; and third, round keys are generated from a single 160-bit key during the key generation stage. A 160-bit key can have 2160 potential values because a bit can be either 0 or 1. It would be necessary to try every possible combination of the 2160 keys in a brute force attack. It would take years to crack the encryption method, even with a cutting-edge computer, making it nearly impossible. The suggested method passes several security criteria, including Avalanche effect, Entropy, Correlation, Histogram Analysis, MSE, and SSIM, and is safe against brute force attacks. The method can be applied to a variety of multimedia systems to securely encrypt images [6].

The modification of the Playfair cipher is the topic of this work. The m x n matrix playfair cipher, which incorporates the two symbols "+" and "#," is a modification of the classic 5x5 matrix playfair cipher. By adding these two symbols to the matrix, the plain text and the cipher text have a one-to-one correlation, making encryption and decryption simple and clear. When these symbols show up in the final cipher text, the text becomes more secure. With the right size matrix, the suggested approach can be used to encrypt and decrypt texts in any natural language [7].

This paper examines a number of hybrid cryptosystems that make use of the public asymmetric cryptosystem RSA and the simpler symmetric cryptosystem Playfair. Many methods are being used to make this hybrid cryptosystem better. While some of them are able to understand it, others do not.[8]

In this study the authors propose a novel symmetric encryption method based on the polygon scheme, which is simpler than contemporary ciphers and exhibits higher security when compared to classical methods due to its vast key space and strength against frequency analysis attacks.[9]

In this paper, the authors aim to improve resistance to frequency-based assaults and increase the complexity of character mappings, the system introduces a dynamically created Playfair table that is derived from MACG-based keys. The hybrid model creates a multi-layered encryption with strong diffusion and excellent resistance to cryptanalysis by combining Autokey encryption with this improved Playfair Cipher. Extensive security analysis, which includes measures like entropy, Avalanche Effect, and Index of Coincidence, shows that the suggested methodology is better at producing highly randomized ciphertexts. 4.27761 is the proposed model's entropy value.

The Index of Coincidence value is 0.01818, while the Avalanche effect value is 45.5%. The system is also appropriate for real-time applications since it maintains effective encryption and decryption times. Future developments in secure and adaptive encryption techniques will be made possible by this study's strong remedy for major flaws in conventional cryptographic systems.[10]

To increase the security of playfair cipher by using 6*6 playfair cipher and vignere 26*26 cipher and generate the random numbers.[13]

The classical Playfair cipher is relatively easy to break because it still leaves much of the structure of the plaintext language. This method of incorporating random sequences can also be applied to other ciphers [14].

3. MATERIALS AND METHODS

The proposed VigPlay Cipher was implemented and evaluated using both software tools and computer resources. The encryption method was developed using the Java programming language, which provides platform independence and efficient execution. Python's robust libraries for numerical visualization were used for data analysis and performance assessment. To evaluate the proposed cipher's real-time applicability, an Android-based mobile device and a standard computer system were part of the experimental setup. The performance of encryption and decryption was assessed using a variety of alphanumeric plaintext datasets of varying sizes.

3.1 Methods

This section explores the various methods.

3.1.1 Overview of VigPlay Cipher

The Proposed Viaplay Cipher is combination of the Vigenère Cipher and the Playfair Cipher. Linear Congruential Generator (LCG) to introduce a dynamic replacement process that produces pseudo-random numbers to increase encryption unpredictability, it improves on traditional methods.

3.1.2 Key Generation

The suggested Vigplay cipher's encryption process begins with two user-defined secret keys, K1 and K2, which are used for the playfair and vigenere ciphers, respectively. To make sure a secure and efficient data transformation, these keys will be integrated into the encryption process.

3.1.3 LCG-Based Random Number Generation

The suggested VigPlay Cipher uses the Linear congruential generator (LCG) which is used to generate pseudo-random integers for dynamic replacement. It has to do with:

$X_{n+1} = a*(X_n) + c* \bmod (m)$

where a, c, and m are constants and X_n represents the present value. The generated sequence is key-dependent since the original seed is obtained from the secret key.

To increase randomness and lessen vulnerability to statistical attacks, character mappings are dynamically modified during encryption using the LCG-generated values. Because LCG has a low computational complexity, it can be used in mobile encryption systems.

3.1.4 The Process of Encryption

1. Preprocessing involves changing the plaintext to uppercase and, if necessary, removing spaces and special characters.

2. Initial substitution dependent on the key is introduced using the Vigenère cipher technique (36*36).

3. Playfair cipher (6*6) rules for digraph substitution are then applied to the output.

4. At each stage, character mappings are dynamically modified using values generated by LCG.

5. The final ciphertext is generated.

3.1.5 The Decryption Process

The decryption procedure proceeds in the opposite order:

1. LCG values are used for reverse dynamic mapping.

2. Use the inverse Playfair transformation.

3. Use the same key to apply Vigenère decryption.

4. Get the original plaintext back.

3.1.6 Performance Assessment

The following criteria are used to assess the suggested cipher's performance:

Memory usage, throughput, encryption time, decryption time

Python is used to create graphs and statistical analysis.

3.1.7 Analysis of Security

The VigPlay Cipher's security was examined in comparison to:

- Brute-force assaults
- Analysing frequency
- Cryptanalysis, both linear and differential

Resistance to these attacks is strengthened by the addition of hybrid structure and dynamic substitution.

4. PROPOSED METHODOLOGY / ENCRYPTION PROCESS

Figure 1 shows Encryption Process of VIgPlay Cipher is given in this section. And Table 1 shows how plaintext is transformed into the final encryption using the suggested VigPlay cipher.

Vigenère encryption, Playfair cipher transformation, and coordinate-based mapping are used to create the ciphertext, as shown in the table. The suggested system's resilience and key sensitivity were assessed using various alphanumeric keys for every test case.

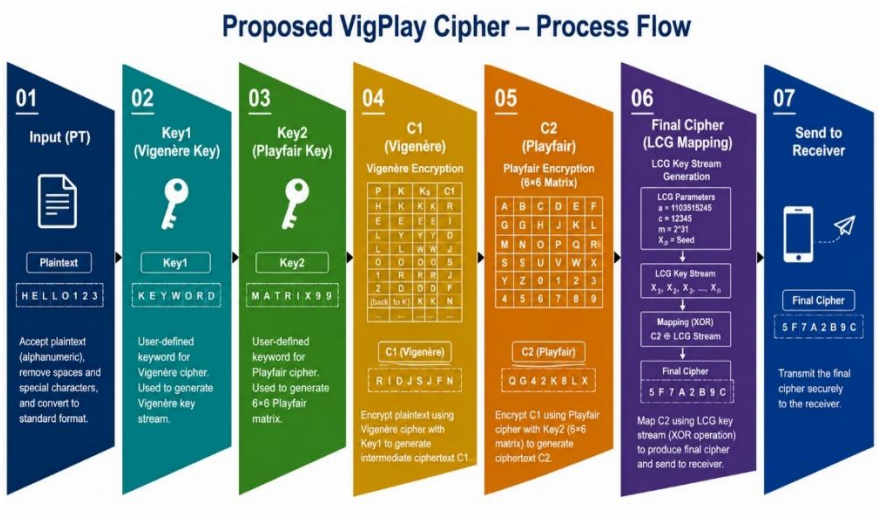

Figure 1: Proposed Vigplay cipher-process flow

TABLE 1: Transformation from Plaintext to Ciphertext

Input (pt)	Key1	Key2	C1(Vigenere)	C2(Playfair)	Final Cipher
SESSION 1089	Wonder689	art12345	ES5VM5JZZUN	FQUNLXYVPV	(4,6), (17,8), (27,28), (15,16), (7,16)
CRYPTOGRAPHY IS BEST POLICY OF SECURITY	HELLO1992WONDER899	CIPHER986	JV907FFQ2BVBLWSCRSWSWTQPNEK0Q7UMAW	FXJVT7Z4GZMEETY0ZOOHSIJSCU5Y	(7,3),(12,2),(29,13)(9,31)(18,9),(30,15)(15,29)(1,6)(9,6)(6,22)(19,16)(12,19)(11,24)(23,1)
CRYPTO123 SECURITY456 BEST789 POLICY	KEY123	Wonder456	MVMGLHB6RJ654V6KQXFAZ5KMHCXGGESGM	VNVMPFJ2ZLSUHBYLPIFVHYDMJPV	(13,5)(13,8)(26,14)(31,11)(10,22)(21,2)(20,18)(30,3)(21,26)(35,14)(13,18)(3,7)(8,31)(26,13
MOBILE2024 SAFE99 DATA88 ENCRYPTION77	SECURE456	ENCRPTION786	4SD22IWVYMWCZVD386BEASVR6MU7XK84B1	W97UXCLXPVWB9C9UWCJXVMFV	(14,25)(36,21)(10,19)(5,10)(4,22)(14,31)(25,19)(25,21)(14,19)(18,10)(22,32)(8,22)
USER1 LOGIN2 AUTH3 TOKEN4 VERIFY5	AUTH789	MECH687	UCXYYJNG2697SSHNCVHCM4FXYFDX5	WMYZWKGIRY8KEW6H85YZ5FYY	(32,13)(14,20)(32,11)(8,2)(7,14)(35,11)(23,32)(24,1)(35,3)(14,20)(3,36)(14,14)
VIGPLAY1 TEST2 CASE3 INPUT4 OUTPUT5	VIG123	PLAY654	GQMGD3J9Z5KMN KGJ6W3VVLLX92ZGMMQ	INNFJR5SNOFHIXWZ6UZTFNWR	(20,31)(31,6)(29,3)(26,17)(31,35),(6,9)(20,8)(22,16),(34,4)(16,5)(6,31)(22,3)
DATA9 CONFIDENTIAL8 INTEGRITY7 CHECK6	DATA456	SECURE888	GACA37KQF1D8IPLA48CIPHGAINT3FHXCE1	I7U9QZK6JOO6UHNJI7HOSLIWUC	(12,22)(34,21)(29,5)(9,14)(30,31)(31,14)(34,13)(36,30)(12,22)(13,31)(28,23)(12,27)(34,2)
ALGO121 DESIGN248 ANALYSIS343 RESULT444 GRAPH555	ALGO789	METRICS65433	AWM2Y00DPYWDL14JG17JXSTYH11QE30ZQ234RXOMF45G	7ZIUHLZXLVBHGZ5MIPLCCZ4RKRGH	(21,4),(30,14)(24,6)(4,8)(6,9)(20,24)(18,4)(16,33)(30,23)(6,10)(10,4)(7,5)(34,5)(18,24)
KEY123 VALUE456 PAIR789 MATCH000 TEST	PAIR786	ANALYSIS986	ZE6IZ1RPL2V1324AQ84651A1TEYWFTM9Q	UJ2IKQ6LSK9AGNVGUKXS	(28,6),(18,30),(36,10),(12,14)(33,36),(26,16)(31,22)(4,31)(28,36)(2,33)
PASSWORD121 HASH242 SALT343 VERIFY454 LOGIN595	PASS789	LOG666	4AAATMQS1KJE8RW2MKP8K83MLSCQXFGM22K3G05274	CVZRITYSMCQXFMHF1RDRWILFM6W	(3,32)(15,22)(9,18),(16,30)(23,3)(33,26),(24,33),(30,8)(24,2)(22,34)(22,5)(9,21)(24,23)(28,5)

Different alphanumeric keys were used for each test case to evaluate the robustness and key sensitivity of the proposed VigPlay cipher.

5. RESULTS AND DISCUSSION

An alphanumeric dataset made up of capital letters and numerical values was used to assess the security and performance of the suggested VigPlay encryption. To evaluate the system's resilience and effectiveness, a variety of input scenarios with different sizes and levels of complexity were taken into account.

5.1 Performance Analysis

Table 2 shows the performance analysis of every component of the proposed system, including the encryption and decryption times for Vigenère and Playfair. It is discovered that both encryption techniques increase the overall computing cost based on the quantity and format of the input.

TABLE 2: Transformation from Plaintext to Ciphertext

	Input Plain Text	**Vigenere Encryption Time**	**Vigenere Decryption Time**	**Playfair Encryption Time**	**Playfair Decryption Time**
1	SESSION 1089	0.556847 ms	0.180923 ms	0.298154 ms	0.312000 ms
2	CRYPTOGRAPHY IS BEST POLICY FOR SECURITY	1.022462 ms	0.351385 ms	1.218846 ms	0.905000 ms
3	CRYPTO123 SECURITY456 BEST789 POLICY	0.640308 ms	0.258462 ms	0.594538 ms	0.940846 ms
4	MOBILE2024 SAFE99 DATA88 ENCRYPTION77	0.302692 ms	0.473923 ms	.460846 ms	0.495924 ms
5	USER1 LOGIN2 AUTH3 TOKEN4 VERIFY5	0.866077 ms	0.480692 ms	0.777231 ms	0.453154 ms
6	VIGPLAY1 TEST2 CASE3 INPUT4 OUTPUT5	.704539 ms	0.332692 ms	0.594692 ms	0.530231 ms
7	DATA9 CONFIDENTIAL8 INTEGRITY7 CHECK6	0.340307 ms	0.330154 ms	0.773770 ms	0.830846 ms
8	ALGO121 DESIGN248 ANALYSIS343 RESULT444 GRAPH555	1.455154 ms	0.459385 ms	1.020692 ms	0.584539 ms
9	KEY123 VALUE456 PAIR789 MATCH000 TEST	0.913538 ms	0.354231 ms	0.451385 ms	0.531385 ms
10	PASSWORD121 HASH242 SALT343 VERIFY454 LOGIN595	2.127923 ms	0.362154 ms	1.141769 ms	0.648308 ms

5.1.1 Overall System Performance

Table 3 presents the VigPlay cipher's encryption, decryption, throughput, and memory utilization. The results indicate that the proposed system is still capable of effectively processing data in a variety of alphanumeric input parameters.

TABLE 3: VigPlay cipher's encryption, decryption, throughput, and memory utilization

S. No.	**Input Plain Text**	**Encryption Time**	**Decryption Time**	**Throughput**	**Efficient Memory Usage**	**Total Memory Usage**
1	SESSION 1089	0.855001	0.492923	112280.6	24	48
2	CRYPTOGRAPHY IS BEST POLICY FOR SECURITY	2.241308	1.256385	142773.8	80	160

3	CRYPTO123 SECURITY456 BEST789 POLICY	1.234846	1.199308	233227.5	72	144
4	MOBILE2024 SAFE99 DATA88 ENCRYPTION77	0.763538	0.969847	387669	74	148
5	USER1 LOGIN2 AUTH3 TOKEN4 VERIFY5	1.643308	0.933846	160651.6	66	132
6	VIGPLAY1 TEST2 CASE3 INPUT4 OUTPUT5	1.299231	0.862923	215512.1	70	140
7	DATA9 CONFIDENTIAL8 INTEGRITY7 CHECK6	1.114077	1.161	265690.8	74	148
8	ALGO121 DESIGN248 ANALYSIS343 RESULT444 GRAPH555	2.475846	1.043924	155098.5	96	192
9	KEY123 VALUE456 PAIR789 MATCH000 TEST	1.364923	0.885616	216862.1	74	148
10	PASSWORD121 HASH242 SALT343 VERIFY454 LOGIN595	3.269692	1.010462	112548.8	92	184

5.2.1 Graphical analysis of the proposed VigPlay cipher

Various graphs illustrating the relationship between data size and key performance parameters are shown in Fig. 2.

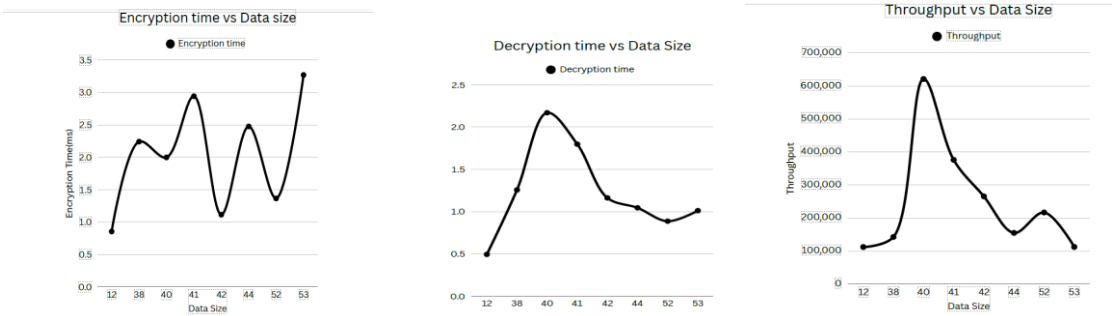

Figure 2 (a) encryption time vs data size, (b) decryption time vs data size (c) throughput vs data size

Different alphanumeric keys were used for each test case to evaluate the robustness and key sensitivity of the proposed VigPlay cipher.

5.2 Statistical Analysis of VigPlay Cipher

The statistical study of throughput, memory utilization, encryption time, and decryption time is shown in Table 4. The average encryption and decryption times are 1.6262 and 0.9816, respectively, according to the statistical analysis, suggesting that decryption is relatively quicker and more reliable. With an average value of 200231.48, the throughput shows effective data processing capability.

Additionally, the average memory utilization of 72.2 shows moderate resource consumption appropriate for contexts with limited resources. In comparison to encryption time and throughput, decryption time and memory consumption show less fluctuation, according to the standard deviation values. All things considered, the suggested VigPlay cipher strikes a fair mix between resource use, speed, and efficiency.

TABLE 4: Statistical Analysis of Encryption Time, Decryption Time, Throughput, and Memory Usage

Metric	Encryption Time	Decryption Time	Throughput	Memory Usage
Mean	1.6262	0.9816	200231.48	72.2
Standard Deviation	0.7570	0.2060	79589.64	18.9
Variance	0.5731	0.0424	6334510612.39	357.2
Minimum	0.7635	0.4929	112280.60	24
Maximum	3.2697	1.2564	387669.00	96

5.3.1 Encryption Time and Decryption Time analysis : The graphical analysis shows that the encryption time increases with input complexity, with minor fluctuations caused by variations in data patterns and alphanumeric input structures. In comparison, the decryption time remains relatively stable and consistent across different input cases, demonstrating the efficiency and reliability of the proposed VigPlay cipher during the reverse transformation process.

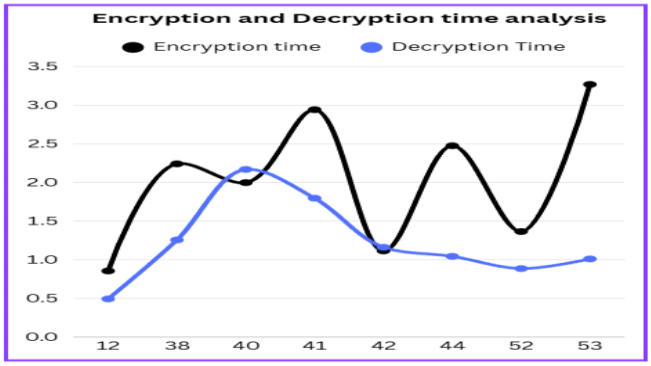

Figure 3: Encryption and Decryption time analysis

5.3.2 Throughput: The graph illustrates the throughput performance for varying input sizes. Higher throughput indicates efficient processing capability, while the observed variations depend on the structure and complexity of the input data.

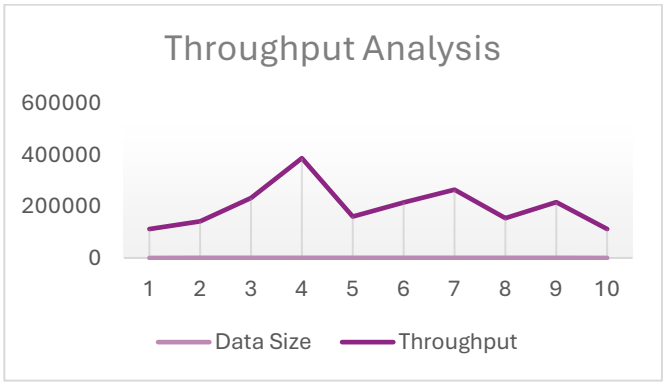

Figure 4: Throughput analysis

5.3.3 Memory Usage: Fig. 5 represents memory consumption across different input cases and remains within a moderate range, making the proposed encryption model suitable for resource-constrained environments.

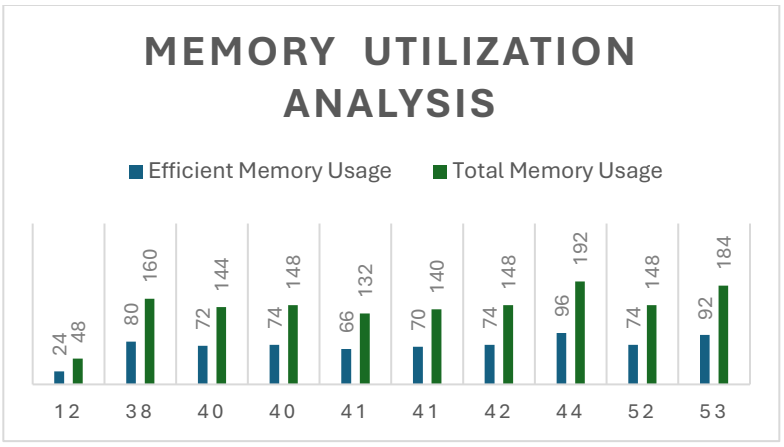

Figure 5: Memory Utilization analysis

5.4 Statistical Comparison of Encryption and Decryption Metrics

The statistical comparison of encryption and decryption metrics shown in Fig.6 display the computational performance and operational efficiency of the proposed VigPlay cipher. It analyses the statistical parameters such as mean, standard deviation, variance, minimum, and maximum values for encryption time and decryption time across different input cases. The analysis indicates that encryption time varies according to input complexity and data patterns, whereas decryption time remains comparatively stable and consistent. These results demonstrate the reliability, scalability, and lightweight execution capability of the proposed encryption model for mobile-oriented and resource-constrained.

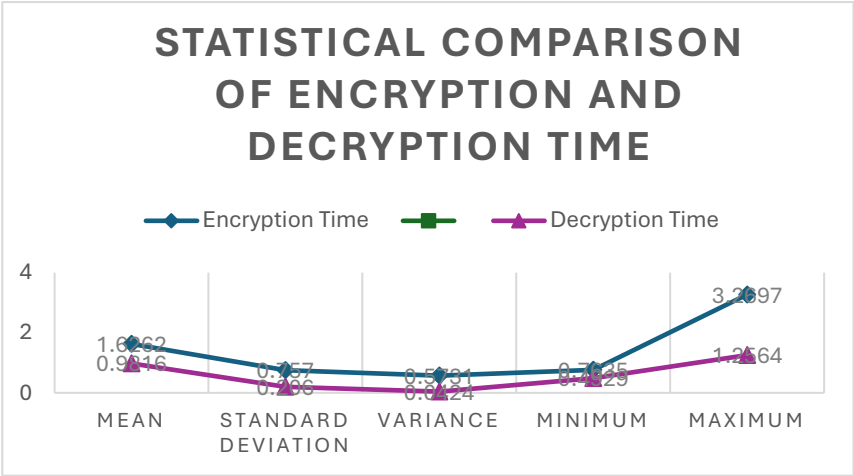

Figure 6: Statistical comparison of encryption and decryption time metrics

TABLE 5: Statistical Comparison with other Symmetric ciphers

Algorithm	Encryption Time (ms)	Decryption Time (ms)	Throughput (KB/s)	Memory Usage (MB)	Lightweight Suitability
AES	4.82	4.11	98500	128	Moderate
DES	3.76	3.44	110200	96	Low
Blowfish	2.91	2.68	142600	88	Moderate

Playfair Cipher	2.14	1.98	165400	62	High
Vigenère Cipher	1.89	1.54	178300	54	High
Proposed VigPlay Cipher	1.62	0.98	200231	72	Very High

5.5 Graphical representation of Statistical Comparison with other Symmetric ciphers

Comparative performance analysis of symmetric encryption algorithms illustrating (a) encryption time, (b) decryption time, (c) throughput, and (d) memory utilization for AES, DES, Blowfish, Playfair Cipher, Vigenère Cipher, and the proposed VigPlay Cipher in mobile-oriented environments are given in Fig. 7 to Fig. 10.

The graphical comparison demonstrates that the proposed VigPlay cipher achieves lower encryption and decryption times compared with conventional symmetric encryption algorithms while maintaining high throughput and moderate memory utilization. The results indicate that the proposed model provides efficient lightweight execution suitable for resource-constrained and mobile-device-based applications.

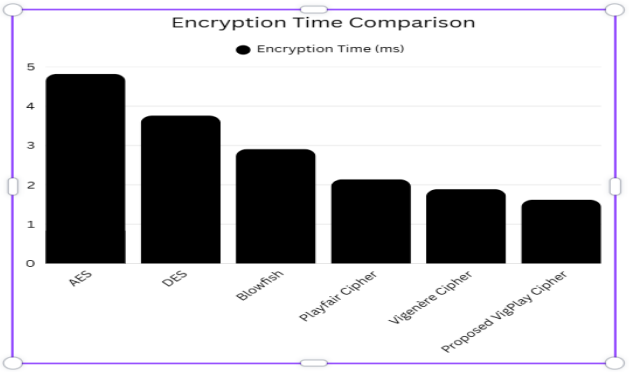

Figure 7: Comparative encryption time analysis of symmetric encryption algorithms

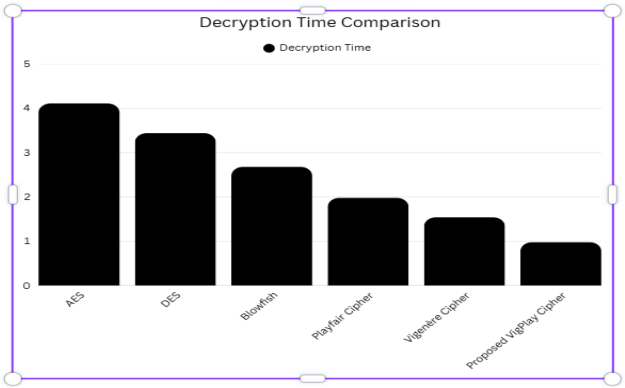

Figure 8: Comparative decryption time analysis of symmetric encryption algorithms

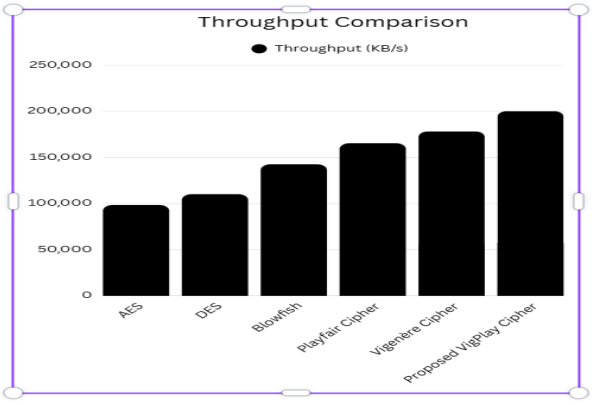

Figure 9: Comparative throughput analysis of symmetric encryption algorithms

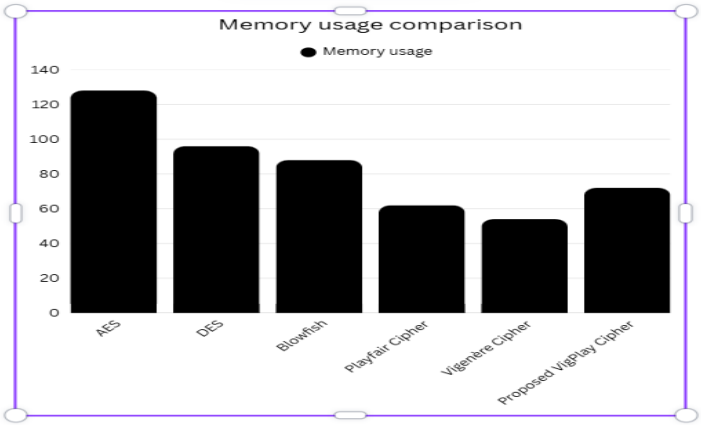

Figure 10: Comparative memory utilization analysis of symmetric encryption algorithm

5.6 Security Analysis of Vigplay Cipher

The suggested VigPlay cipher's security is assessed by examining how well it resists a number of traditional and contemporary cryptanalytic assaults. The assessment focuses on brute force attack, frequency analysis and other cryptanalytic techniques like linear and differential attacks. By using two separate keys and a multi-layered encryption framework, the suggested VigPlay cipher is made more secure. Let K1 and K2 be the key spaces for the Vigenère and Playfair ciphers, respectively, an estimate of the entire effective key space is as follows:

$$K_{TOTAL}=K1*K2*M$$

where M stands for the extra randomness brought about by permutation and coordinate-based mapping. The computational cost of a brute-force attack is greatly increased by this multiplicative expansion, which causes an exponential growth in key space. As a result, a high degree of cryptographic security against exhaustive search attacks is ensured because the time needed to exhaust all potential key combinations becomes infeasible.

5.6.1 Frequency Analysis

VigPlay cipher scrambles traditional cipher's frequency distribution. It uses a two-step technique: first, the Vigenère cipher shifts letters around to create confusion. Then, the Playfair cipher encrypts pairs of letters to spread the data out diffusion. On top of that, it maps everything into a 6×6 matrix; this process turns single letters and numbers into pairs of numbers. By the time it’s done, the original letter frequencies are so distorted that standard statistical attacks just won't work.

5.6.2 Linear Cryptanalysis

The goal of linear cryptanalysis is to find out the relationship that exist among the plain text, cipher text and key but the proposed cipher uses the multi-keys and multi layered encryption structure to reduce the linear relationship,

Coordinate mapping and Playfair's non-linear transformations provide complexity, which enhances protection against linear attacks.

5.6.3 Differential Cryptanalysis

"Differential cryptanalysis checks how changes in the input affect the output. The proposed VigPlay cipher prevents such attacks because even a small change in the plaintext leads to a significant change in the ciphertext during transmission. This phenomenon is known as the avalanche effect. A strong avalanche effect makes it difficult to identify patterns, thereby improving the security of the cipher."

TABLE 6: Security Comparison of VigPlay Cipher with Other Encryption Algorithms

Security Parameter	AES	DES	Blowfish	VigPlay
Dimensions of Key	128/192/256	56	32–448	Variable
Brute Force Resistance	Very High	Low	High	Moderate-High
Dynamic Substitution	No	No	No	Yes
Resistance to Frequency Analysis	High	Moderate	High	High
Lightweight Execution	Moderate	Moderate	Moderate	High
Mobile Friendly Environment	Moderate	Low	Moderate	High

6. CONCLUSION AND FUTURE SCOPE

"A lightweight and improved classical encryption and decryption scheme that supports alphanumeric data and keys and is optimized for effective performance on mobile platforms is proposed in this study."

In today's digital age, secure and efficient encryption of alphanumeric data is more crucial than ever, especially on mobile devices. This study provides a new dual-layer symmetric encryption technique that combines an enhanced 6x6 Playfair cipher and an enlarged 36x36 Vigenère cipher to permit alphanumeric input. Improved security against frequency analysis and brute-force attacks.

by this advancement. Using a Pseudo-Random Number Generator (PRNG) to provide a dynamic, unpredictable random numbers for strengthens the encryption process even more. On both ends, key matrices can be constructed thanks to the secure transmission of this random number, which guarantees synchronization. By ensuring that the encryption key is unique and challenging to decipher, this technique not only improves security. For mobile apps with constrained processing power and memory, the entire architecture provides a quick, easy, and safe encryption solution. Furthermore, to protect the PRNG seed or key over untrusted channels, the suggested method can be expanded with Quantum Key Distribution (QKD) or other post-quantum cryptography techniques, making it resistant to quantum attacks even.

To address secure key transmission over untrusted channels, the proposed technique can be extended using advanced techniques such as Quantum Key Distribution (QKD) or other post-quantum cryptographic methods, which focuses on key distribution and quantum-resistant algorithms typically using quantum mechanics to ensure secure communication will address the issue of this cipher's dependence on a key for both the Playfair and Vigenère matrices (e.g., Quantum Key Distribution (QKD) like BB84 protocol). Additionally, the proposed approach can be expanded to protect the PRNG seed or key over untrusted channels using Quantum Key Distribution (QKD) or dynamic S-Box generation, making it suited to mobile apps that have limited memory and processing power.

References

1. Y. Wang, "A classical cipher—Playfair cipher and its improved versions," in Proc. Int. Conf. on Electronic Information Engineering and Computer Science (EIECS), [Changchun, China.], 2021, pp. 123–126. DOI:10.1109/EIECS53707.2021.9587989
2. R. M. Marzan and A. M. Sison, "An enhanced key security of Playfair cipher algorithm," in Proc. 8th Int. Conf. on Software and Computer Applications (ICSCA), Penang, Malaysia, 2019, pp. 457–461. doi: 10.1145/3316615.3316677
3. S. Singh Chauhan, H. Singh, and R. N. Gurjar, "Secure Key Exchange Using RSA in Extended Playfair Cipher Technique," International Journal of Computer Applications, vol. 104, no. 15, pp. 13–19, Oct. 2014, doi: 10.5120/18284-9320.

4. A. C. Licayan, B. D. Gerardo, and A. A. Hernandez, “Enhancing Playfair cipher using seed-based color substitution,” in Proc. IEEE 16th Int. Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2020, pp. 242–246. doi: 10.1109/CSPA48992.2020.9068695
5. M. S. Yousif, R. K. Salih, and N. M. G. Alsaidi, “A new modified Playfair cipher,” in Proc. AIP Conf. Proc., vol. 2086, no. 1, p. 020026, Apr. 2019. doi: 10.1063/1.5095116
6. J. Kavedia, J. Shah, J. Dawre, and R. Mangrulkar, “A modified Playfair-based approach for secured RGB image encryption,” in Proc. Int. Conf. on Sustainability, Innovation & Technology (ICSIT), [City, Country], 2025, pp. 1–12. DOI:10.1109/ICSIT65336.2025.11294465
7. A. Alam, S. Ullah, I. Wahid, and S. Khalid, “Universal Playfair cipher using M×N matrix,” Int. J. Adv. Comput. Sci., vol. 1, no. 3, pp. 113–117, Sep. 2011. [Online]. Available: https://www.researchgate.net/publication/274709666_Universal_Playfair_Cipher_Using_MXN_Matrix
8. S. M. Suhael, Z. A. Ahmed, and A. J. Hussain, “A Review on Hybrid Methods Using Playfair and RSA Techniques,” in AIP Conference Proceedings, vol. 3169, no. 1, p. 030002, Feb. 2025, AIP Publishing LLC, doi: 10.1063/5.0250658.
9. Masadeh, S. R., and H. A. Al_Sewadi, “A Novel Polygon Cipher Technique Using Hybrid Key Scheme,” International Journal of Computer Science and Information Security (IJCSIS), vol. 14, no. 4, pp. 67–70, Apr. 2016, doi: 10.6084/M9.FIGSHARE.3362203.
10. M. Tummala, M. E. Malkhed, and S. Basavaraju, “Dynamic hybrid cryptographic system using modified additive congruential generator,” in Proc. 3rd Int. Conf. on Inventive Computing and Informatics (ICICI), Bangalore, India 2025, pp. 229–235. doi: https://doi.org/10.1109/ICICI65870.2025.11069780
11. S. Singh and A. Dixit, “An approach for enhancing the security of Playfair cipher,” Imperial J. Interdiscip. Res., vol. 3, no. 6, pp. 1–5, 2017. [Online]. Available: https://www.onlinejournal.in/IJIRV3I6/001.pdf
12. S.Singh, “A novel technique for enhancement of the security of Playfair cipher,” Int. J. Comput. Eng. Res. Trends (IJCERT), vol. 7, no. 1, pp. 1–6, 2020. [Online]. Available: https://ijcert.org/ems/ijcert_papers/V7I102.pdf
13. Singamaneni, K. K., Reddy, P. V. G. D., & Rao, K. S. (2025). “A novel lightweight hybrid cryptographic framework for secure smart card transactions in resource-constrained environments.” Cybersecurity, 8(1), 1–23. https://doi.org/10.1186/s42400-025-00204-8
14. Kumar, A., Sharma, R., & Gupta, S. (2025). “Hybrid cryptographic approach for strengthening IoT and 5G communication security.” Scientific Reports, 15, 11874–11891. https://doi.org/10.1038/s41598-025-12575-7
15. Ahmad, S. A., & Garko, A. B. (2019). “Hybrid cryptography algorithms in cloud computing: A review.” Proceedings of the 15th International Conference on Electronics, Computer and Computation (ICECCO), 1–6. IEEE. https://doi.org/10.1109/ICECCO48375.2019.9043254
16. Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). “Hybrid cryptographic approach for Internet of Things applications: A review.” Journal of Information and Communication Technology, 19(3), 279–319. https://doi.org/10.32890/jict2020.19.3.1
17. Gupta, P. K., Jaleel, U., & Vidya, R. (2023). “A Novel Hybrid Cryptographic Approach for Secure Device-to-Device Communication.” International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 412–420. Available at: https://ijisae.org/index.php/IJISAE/article/view/4118
18. Shivam Vatshayan, “Design of Hybrid Cryptography System Based on Vigenère Cipher and Polybius Cipher,” in Proc. 2020 International Conference on Computational Performance Evaluation (ComPE), Jul. 2020, pp. 350–354, IEEE, doi: 10.1109/ComPE49325.2020.9200050.
19. C. M. S. Tan, G. P. Arada, A. C. Abad, and E. R. Magsino, “A Hybrid Encryption and Decryption Algorithm Using Caesar and Vigenere Cipher,” in Journal of Physics: Conference Series, vol. 1997, no. 1, p. 012021, Aug. 2021, IOP Publishing, doi: 10.1088/1742-6596/1997/1/012021.
20. H. Touil, N. El Akkad, and K. Satori, “Text Encryption: Hybrid Cryptographic Method Using Vigenere and Hill Ciphers,” in Proc. 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Jun. 2020, pp. 1–6, IEEE, doi: 10.1109/ISCV49265.2020.9204065.