JCBI
Journal of Computing & Biomedical Informatics Volume 11 Issue 01
ISSN: 2710 - 1606 2026

Research Article
https://doi.org/10.56979/1101/2026/1292

A Secure Taylor Expansion–Based Data Encryption Algorithm Using Effective Permutations

Asad Shakoor[1], Muhammad Usman[2*], Syed Mudassar Alam[3], Rao Umer Farooq[4], and Ayesha Ayub[5]

[1]National University of Modern Languages (NUML), Faisalabad, 38000, Pakistan.
[*]Corresponding Author: Muhammad Usman. Email: shk.usman.su@gmail.com

Received: January 06, 2026 **Accepted:** May 01, 2026

Abstract: The paper proposes a lightweight exploratory encryption framework to explore the substitution of dynamic permutation based on Taylor-series for the encryption of text. The proposed method inputs plaintext and a key value. In the next step the key value is converted into dynamic key value (DKV) and the plaintext is converted into its corresponding ASCII sequence which is finally transformed using Taylor's series-based operations to produce cipher text. The security and speed of the proposed method were evaluated by measuring encryption and decryption times along with plaintext and key based avalanche effects. The observed results showed computational efficiency of 11 characters of plaintext with a variable length of numeric key setup. Under experimental conditions, the time spent for encryption was 0.0005 seconds and the time spent for decryption was 0.0001 seconds. The experimental conditions employed led to promising avalanche characteristics to the proposed technique: key-based changes - 83.75%, plaintext-based changes - 55.45%. The hybrid structure has been optimized by means of both permutation and nonlinear substitution operations, which are well suited for lightweight exploratory encryption applications as it is optimized for confusion and diffusion for such applications. The proposed solution shall be viewed in this context as another pioneering lightweight encryption scheme for research in academia and simple level text-encryption research.

Keywords: Encryption; Taylor series; dynamic key; permutation; substitution; avalanche effect

1. Introduction

Encryption is the process of transforming data from a visible form known as plaintext into an encoded message known as cipher text. Over wired and wireless networks, including the Internet and e-mail, data sent and saved on servers, desktops, laptops, tablets, cellphones, and other portable devices can be secured using encryption. Encryption converts readable plaintext into unrecognizably cipher text using a mathematical technique. The opposing operation, decryption, employs the same technique to transform plaintext from incomprehensible cipher text into a readable form. A key is nothing more than a line or collection of data that is used with the technique to encrypt and decode data. Security is provided by using the method with the particular key/keys. Secret key or symmetric key encryption is the process of encrypting and decrypting the data using the same secret key and method. While using secret key encryption, the secrecy of the key must be maintained because anyone with access to it can use it to decrypt the data as shown in figure 1.

Permutation and substitution functions [8] are very important components of encryption algorithms as they provide distinct yet complementary roles in ensuring the security and effectiveness of the encryption process. Substitution functions aid in maintaining confusion by replacing or substituting elements of the plaintext with different elements based on specific rules or mappings.

The difficulty of the process of recognizing direct relationships between plaintext and ciphertext patterns is increased. By using substitution functions, encryption algorithms achieve a higher level of data obfuscation and non-linearity, increasing the complexity of the cipher and enhancing its resistance to cryptographic attacks. Permutation functions help create diffusion by shuffling the order or position of elements within the data. This reordering effect spreads out statistical patterns in the original text so that even a little change in the input data leads to a significant change in the encrypted output. Permutation operations help diffusion within the encrypted data by shuffling statistical attributes. The combination of substitution and permutation functions in an encryption algorithm results in a well-balanced algorithm that achieves both confusion and diffusion [9-10]. Taylor series mathematically represent a formula as a summation of infinite terms that computed from the derivatives of the functions [1-2].

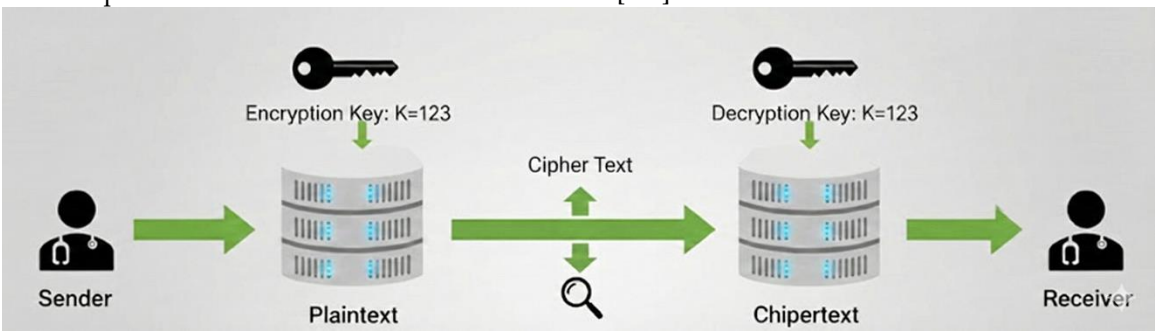

Figure 1. Encryption and Decryption

The proposed method operates using an input key and plaintext that is meant to encrypt textual data. The proposed method first converts the plain text (character by character) into ASCII code and the user-input key to dynamic key value using modulo function. In the next step the permutation function, which shuffles the plain text's characters into other characters using the dynamic key value (DKV). After this step, the ASCII values of each character get substituted with extended digits using the Taylor's series function to create the final cipher text.

The work proposed is a light-weight new encryption method suitable for research purposes that studies the use of Taylor series based nonlinear substitution combined with permutation operations that change with time. The study is not designed to supplant with the industrial standard (AES, ECC) but rather to examine the possibility of achieving a substitution method for lightweight applications of text encryption using a mathematical-series approach.

2. Related Work

Many encryption algorithms have used and explored mathematical and classical ciphers to increase data protection. Noaman et al. [3] proposed a Taylor series–based cipher that substitutes plaintext ASCII codes into a polynomial formula but used a static key and lacked permutation functions, lacking diffusion properties. Abed et al. [4] introduced a McLaurin series encryption but uses a fixed key value 0, which makes the algorithm predictable. Arroyo et al. [5] introduced a Polybius-Square cipher with ASCII mapping which also lacked permutation layers, which results in weak diffusion. Hameed and Sadeeq [6] modified the Vigenère cipher by using hybrid key generation, although it introduced complexity without proportional gains in speed. Viswanathan et al. [7] combined elliptic-curve cryptography with Euler and Gamma functions to secure group communication, but it resulted in computational cost. [11] Provides a systematic review of cryptanalytic studies on substitution–permutation network (SPN) based image encryption schemes. Many of these schemes exhibit weak diffusion, too few encryption rounds, and excessive dependence on basic chaotic maps, leaving them open to chosen-plaintext and chosen-cipher text attacks. [12] Proposes a lightweight, block-cipher encryption scheme using a custom substitution-permutation network and an improved S-box. The algorithm relies only on simple operations to keep complexity low. This technique is good for implementation in low resource equipment like security camera. Author proposes in [13] a new "Secured Asymmetric Image Cipher (SAIC)" algorithm based on permutation and substitution, and demonstrates strong security properties. We used the scheme with unconstrained key length and showed its good performance when it encrypts and decrypts binary image data for image transmission applications. Their tests show a very high sensitivity to plaintext. The study [14] introduces a novel text-

encryption scheme that uses Elliptic Curve Cryptography (ECC) to map message characters to elliptic-curve. The algorithms pass through multiple checks to perform its efficiency. The algorithm has good computational performance in encrypting and decrypting time cipher text size and plain text size. The study [15] reviews numerous symmetric and asymmetric cryptographic algorithms, organizing them based on their architectural style as well as their key sizes, block sizes, and round structures. The authors also discuss key research challenges, emphasizing the need for adaptable symmetric-key algorithms, improved key-exchange methods, and lightweight encryption solutions for constrained and distributed environments like IoT.

3. Proposed Method

The proposed work aims to explore and present lightweight framework of encryption using Taylor Series based NONLINEAR SUBSTITUTION and DYNAMIC PERMUTABILIZATION for text encryption applications. The algorithm will run through two steps which are encryption and decryption. It takes in the plain text P and a variable length user-defined secret key K for practical secure deployment recommends minimum three-digit or greater keys, then calculates a Dynamic Key Value (DKV) and performs permutation and Taylor-series based substitution to obtain the cipher text C.

A. Encryption Phase

I. Convert plaintext characters to ASCII codes.

II. Compute Dynamic key value (DKV) using:

$$DKV = K \bmod 95$$

Where, K is the user specified key for the encryption, the number 95 is the sum of all the number of the printable ASCII characters.

III. Perform dynamic permutation by adding DKV to each ASCII value.

IV. Apply Taylor-series-based substitution on permuted values to obtain cipher text digits.

V. Concatenate results to form final Cipher text C.

B. Decryption Phase

The decryption process undoes the encryption operations with same secret key K.

I. Input C and K.

II. Recomputed DKV = K mod 95.

III. Apply inverse Taylor-series function to restore ASCII codes.

IV. Subtract DKV to reverse permutation from each restore ASCII codes.

V. Convert ASCII codes back to plaintext.

The framework of the proposed method is illustrated in Figure 2. A detailed explanation of the algorithm is provided below.

Phase 1: Encryption Phase

Step 1: Inputs

- Encryption key (K)

(Variable length numeric key e.g., 999)

- Plaintext (P)

(In character for e.g., ABCD7@XYZ)

Step 2: Conversions and Dynamic key generation

- Conversion of user entered plaintext into ASCII code

(E.g., ABCDEWXYZ = 65 66 67 68 55 64 88 89 90)

- Generation of key value (DKV) for dynamic permutation (DKV= K mod 95)

(E.g., DKV = 999 mod 95, DKV = 49)

Step 3: Operations

- Dynamic permutation operation is being applied by adding dynamic key value (DKV) to the ASCII code of each character of the plaintext.

$$X_i = ASCII\ (P_i) + DKV$$

(E.g., 65+49 66+49 67+49……90+49)

- Taylor's series-based substitution function is being applied.

Step 4: Taylor-Series Based Substotution

$$f(x) = \sum_{n=0}^{r} \frac{f^n(a)}{n!}(x-a)^n$$

Where:

- x is the permuted ASCII code,
- a is Dynamic Key Value (DKV),
- r is the truncation order of the Taylor expansion,
- f(n)(a) is the value of the derivative at a.

The proposed method expands a function with an infinite number of terms, but only truncated to the order r for reducing the computation cost factors for implementation and reconstructibility for decryption.

For each character, the ciphertext character is calculated based on the following:

$$C_i = \left(\sum_{n=0}^{r} \frac{(X_i - a)^n}{n!} \right) mod\ B$$

Where:

- C_i represents the generated ciphertext component,
- B represents the modulus boundary.

In our proposed implementation:

B=95

The proposed substitution method is based on the following truncated Taylor-series expansion (1).

$$f(x) = \sum_{n=0}^{r} \frac{f^n(a)}{n!}(x-a)^n \qquad \textbf{\textit{Eq. (1)}}$$

The lightweight encryption framework introduces nonlinear substitution mechanism based on Taylor series, which causes the output variation of the lightweight cryptographic system.

Step 5: Ciphertext

- Ciphertext (C) after Taylor's series-based substitution:

519875290353827547594326751079566475569954759

Phase 2: Decryption phase

In the decryption phase these inverse substitution mapping and substitution operations are performed to retrieve the original plaintext. The inverse permutation is used to get the original ASCII values back:

$$ASCII\ (P_i) = X_i - DKV$$

Once the ASCII values are recovered, the plaintext characters are reconstructed by comparing the recovered ASCII value to the table provided to convert ASCII to character.

Plaintext (P) recovered from Cipher text (C): ABCD7@XYZ

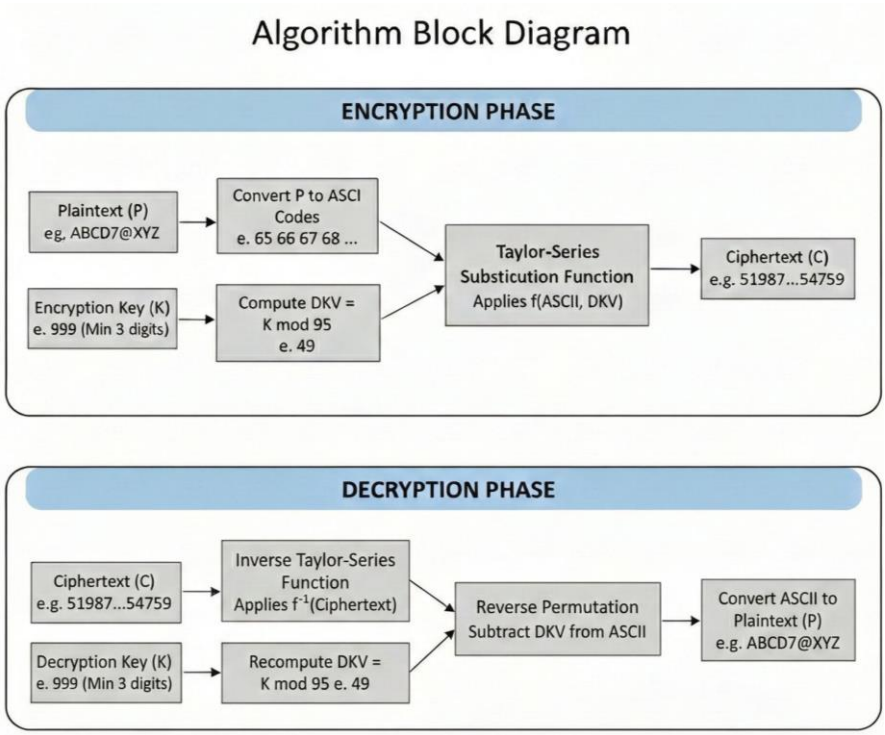

Figure 2. Proposed Methodology

The proposed method was implemented using DEV-C++ 6.30 running on Microsoft Windows 10 64-bit OS. The desktop PC was built with 8 GB Random Access Memory (RAM) and an Intel Core i5 2.30 GHz Central Processing Unit (CPU).

Avalanche effect is a cryptographic property where a small change in Plain text or in encryption produces a substantial change in the cipher text. Equation 2 presents the Avalanche effect.

$$Avalanche\ Effect(\%) = \frac{Number\ of\ Changed\ Bits}{Total\ Number\ of\ Bits} \times 100 \qquad \textbf{Eq. (2)}$$

The avalanche effect was tested using a binary representation performed on either the original or modified ciphertext outputs, followed by a bit-by-bit comparison, as a measure of the number of bits that differ. A variety of plaintext and key modification tests were performed and the avalanche percentages listed are the average experimental results from all the tests.

4. Results and Discussion

Data on comparative performances shown in Table 1 were copied from the original published studies. As a result, the testing environments used, the size of the plaintexts, the hardware used, the implementation platforms and the length of the key may vary between the methods involved. The comparison is made mainly for showing the relative performance of this lightweight text-encryption scheme against other similar schemes, not for creating a fully standardized performance environment. All comparative values were reported as presented in the cited references [16-24].

Table 1. Comparative Encryption Time Analysis with Referenced Lightweight Encryption Methods

Sr. No	Existing Solutions	Methods	Plaintext Length (Characters)	Key Length	Encryption Time (Seconds)	Permutation	Substitution
1	[16]	DES	40	40	0.0672	Yes	Yes
2	[16]	Fixed Key Length	40	40	0.0035	No	No

3	[16]	ASCII Value Based Optimized Text Encryption System	40	40	0.0032	No	Yes
4	[17]	ASCII Value-Based Data Encryption Algorithm	10	10	0.5543	No	Yes
5	[18]	Elliptic Curve Cryptography for Secured Text Encryption	-	-	0.08	No	Yes
6	[3]	Taylor Expansion Based Encryption Model	21	1	-	No	Yes
7	[19]	SHSED Algorithm	-	-	0.0706	No	Yes
8	[5]	Traditional Polybius Square	11	Variable	0.0031929	No	Yes
9	[20]	Modified Playfair Cipher	40	40	5.257	Yes	Yes
10	[21]	Enhanced Polybius Square	11	Variable	0.0005	No	Yes
11	Proposed Method	Enhanced Taylor-Series Based Encryption Algorithm	40	Variable	0.002996	Yes	Yes
12	Proposed Method (Experimental Lightweight Configuration)	Enhanced Taylor-Series Based Encryption Algorithm	11	Variable	0.0005	Yes	Yes

The suggested approach was found to offer promising computational characteristics compared to some of the popular light-weight encryption techniques. The evaluation results of the experiments showed that the encryption time of the experiment in the condition of performing it was 0.002996 seconds when the length of the plaintext was 40 characters and 0.0005 seconds when the length of the plaintext was 11 characters.

Table 2. Decryption Time Comparison of Proposed Method with Similar Encryption Algorithms

Sr. No	Existing Solutions	Methods	Decryption time in seconds
1	[19]	Simple and highly secure encryption decryption (SHSED) algorithm	0.02
2	[18]	Elliptic Curve Cryptography for Secured Text Encryption	0.06
3	Proposed Method	Enhanced Taylor's series-based encryption algorithm.	0.0001

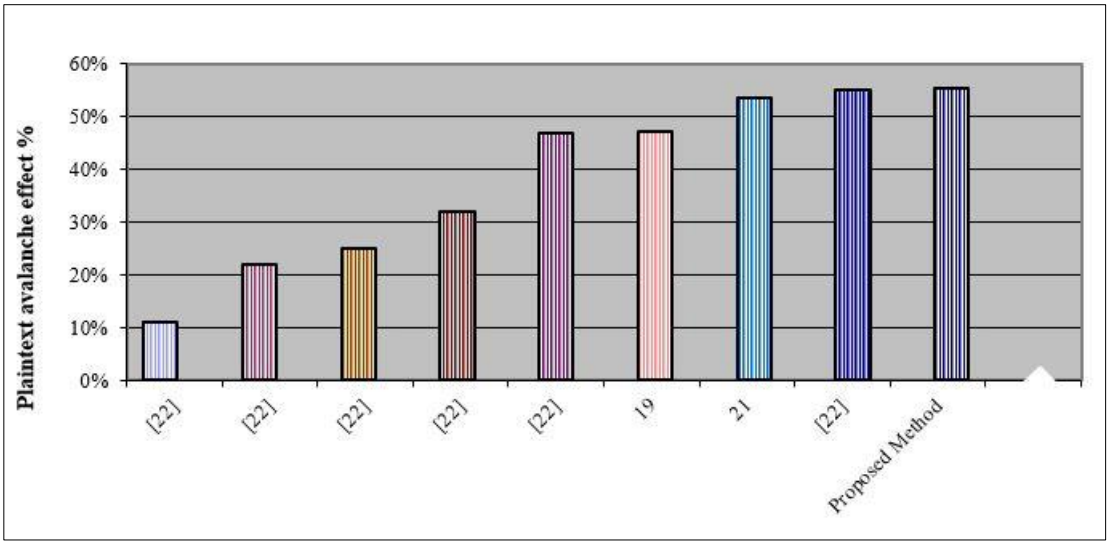

Figure 3. Graphical Comparison of Plaintext Avalanche Effect of Proposed Method with Others

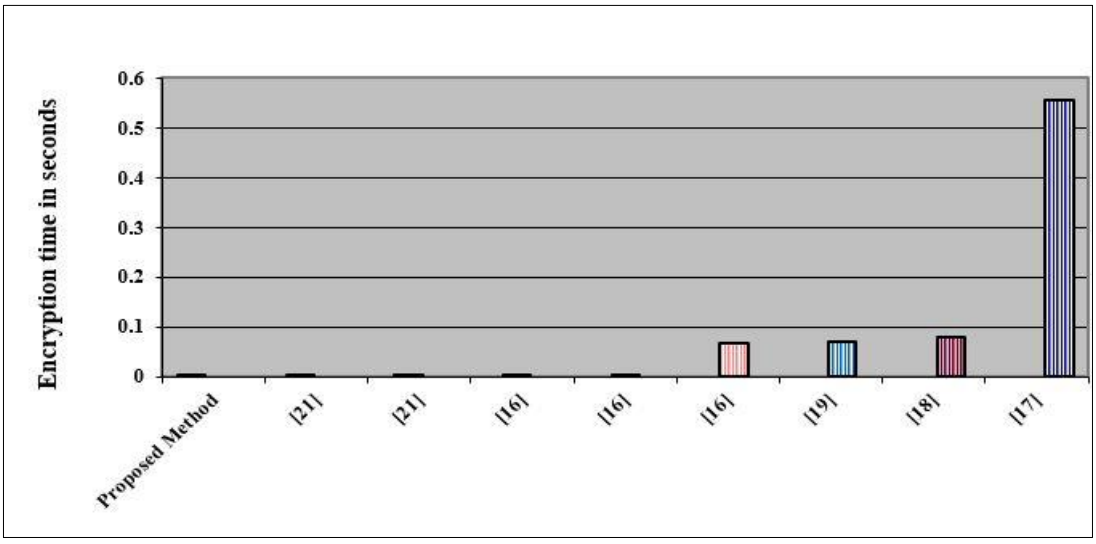

Figure 4. Encryption time comparison with other algorithms

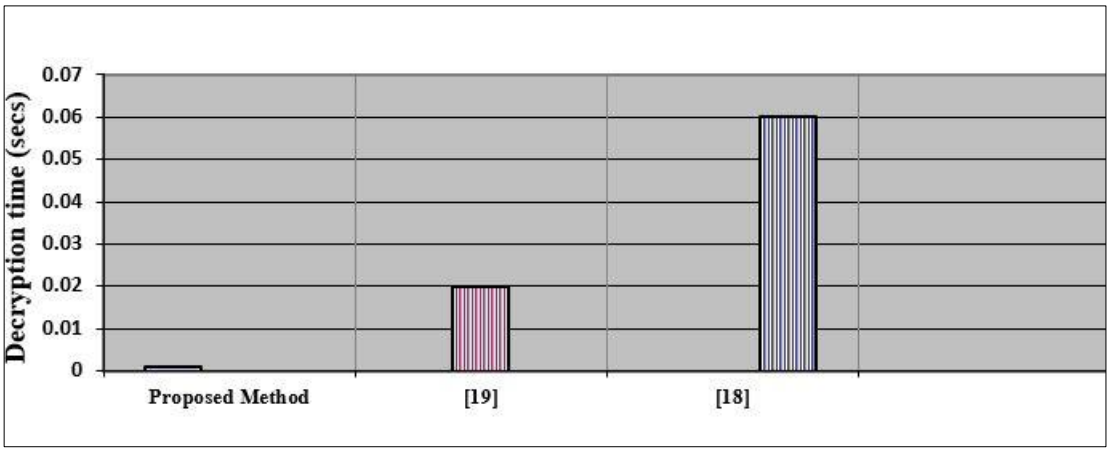

Figure 5. Decryption time comparison with other algorithms

The proposed framework has been benchmarked with the considered light-weighted encryption algorithms and is found to show promising avalanche effect and competitive computational time in the considered experimental scenarios. The use of dynamic permutation and the Taylor-series substitution adds to the diffusion and nonlinear transformation behavior of the encryption process. The results are shown in Figures 3, 4, and 5, respectively.

5. Security Discussion

A. Key Space Analysis

The proposed method is able to contain variable-size numeric keys. If the key has n digits, then the size of the keyspace is approximately: 10^n

The answer is that a longer key means that there are more computations for the brute force key search to try. The minimum key length is recommended as 3 digits and more for increasing the diversity of keys (practical secure deployment).

B. Plaintext Sensitivity

Experiments show that changing a small bit of the plaintext can dramatically affect the output of the ciphertext. This feature showcases desirable diffusion properties in the suggested lightweight encryption scheme.

C. Key Sensitivity

The proposed method demonstrates some important sensitivity properties, namely, small changes in the encryption key produce significantly different results in terms of ciphertext output. This property is a factor to be confused in the encryption procedure.

D. Ciphertext Characteristics

Applying dynamics of permutation and its substitution by a Taylor series make the generated right output more variable, thus decreasing visible statistical regularity in the ciphertext values. Ciphertext diversity during encryption is partially caused by the nonlinear substitution process.

E. Scope Clarification

The presented system serves as a tentative lightweight encryption system for investigating the use of the Taylor-series approach to nonlinear substitution and the dynamic permutation operations. The study is not meant to compete with standardized industrial cryptographic systems like AES or ECC. A formal defense against future advanced crypt analyzers, entropy analysis, and an adaptive attack study are all directions for future investigation.

6. Conclusions and Future Directions

In this study a lightweight exploratory text-encryption framework that combines dynamic permutation and Taylor series-based expansion was presented. The technique provides low-weight computational complexity and extensive and promising confusion and diffusion properties via a mix of permutation and substitution operations. Preliminary testing shows encouraging avalanche behavior, and competitive encryption speeds when compared to several of the referenced approaches based upon Taylor series and McLaurin series. The proposed framework is based on variable length numeric keys that will enable a

larger number of key configurations to be used, increasing key-space complexity. The proposed framework has added only as a means of exploration of mathematical-series based substitution mechanisms in light-weight research related to text-encryption. The framework can be expanded in the future with other randomness mechanisms, entropy measurement and more extensive cryptanalytical analysis.

References

1. G. B. Thomas, R. L. Finney, M. D. Weir, and F. R. Giordano, Thomas' calculus: Addison-Wesley Reading, 2003.
2. C. Hooley, "Taylor series the University of St Andrews, 31st August 2006 2006
3. Noaman, Salam Abdulkhaleq, Basim Najim Al-din Abed, and Sameera A'amer Abdul-Kader. "A New Mathematical Model to Improve Encryption Process Using Taylor Expansion." *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*. IEEE, 2020.
4. Abed, Basim Najim Al-din, and Salam Abdulkhaleq Noaman."McLaurin series as a new technique to improve encryption process."*Journal of Physics: Conference Series*. Vol. 1294. No. 4. IOP Publishing, 2019.
5. Arroyo, Jan Carlo T., Ariel Roy L. Reyes, and Allemar Jhone P. Delima. "A Novel ASCII Code-based Polybius Square Alphabet Sequencer as Enhanced Cryptographic Cipher for Cyber Security Protection (APSAlpS-3CS)." *International Journal of Advanced Computer Science and Applications* 11.7 (2020).
6. Hameed, Thamer Hassan, and Haval Tariq Sadeeq. "Modified Vigenère cipher algorithm based on new key generation method." *Indonesian Journal of Electrical Engineering and Computer Science* 28.2 (2022): 954-961.
7. Viswanathan, S., et al. "Euler phi function and gamma function based elliptic curve encryption for secured group communication." *Wireless Personal Communications* 125.1 (2022): 421-451.
8. A. R. Narwal and S. Gill, "Hybrid Permutation–Substitution Cipher for Text Data," IJCS, 2022.
9. Farooq, Muhammad Shoaib, et al. "Design of a Substitution Box using a Novel Chaotic Map and Permutation." *VFAST Transactions on Software Engineering* 10.2 (2022): 01-08.
10. Khan, A., and H. Qazi. "Improving Text Cipher Security with ASCII Permutation." *International Journal of Computer Security*, 2018.
11. Dhall, Sakshi, and Khushboo Yadav. "Cryptanalysis of substitution-permutation network based image encryption schemes: a systematic review." *Nonlinear Dynamics* 112.17 (2024): 14719-14744.
12. Gupta, Tanisha, Arvind Selwal, and Ajay K. Sharma. "A Novel Lightweight Image Cryptographic Algorithm via Substitution-Permutation Methods." *Security and Privacy* 8.2 (2025): e70015.
13. Goel, Vikas, and Amit Kumar Goyal. "An Improved Analysis of Secured Permutation and Substitution based Image Encryption." *Journal of Cybersecurity & Information Management* 12.1 (2023).
14. Sharma, P. L., et al. "TEXCEL: text encryption with elliptic curve cryptography for enhanced security." *Multimedia Tools and Applications* 84.13 (2025): 11503-11531.
15. Salami, Yashar, Vahid Khajevand, and Esmaeil Zeinali. "Cryptographic algorithms: a review of the literature, weaknesses and open challenges." *J. Comput. Robot* 16.2 (2023): 46-56.
16. Sultana, Roofee, and T. Madhavi Kumari. "An ASCII value based optimized text data encryption system." *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 5.8 (2016).
17. Mathur, Akanksha. "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms." *International Journal on Computer Science and Engineering* 4.9 (2012): 1650.
18. Keerthi, K., and B. Surendiran. "Elliptic curve cryptography for secured text encryption." *2017 International conference on circuit, power and computing technologies (ICCPCT)*. IEEE, 2017.
19. Hendi, Amjad Y., et al. "A novel simple and highly secure method for data encryption-decryption." *International Journal of Communication Networks and Information Security* 11.1 (2019): 232-238.
20. Yousif, Madeha Shaltagh, Raghad Kadhim Salih, and Nadia Mohamed Ghanim Alsaidi. "A new modified playfair cipher." *AIP conference proceedings*. Vol. 2086. No. 1. AIP Publishing LLC, 2019.
21. Arroyo, Jan Carlo T., et al. "An enhanced playfair algorithm with dynamic matrix using the novel multidimensional element-in-grid sequencer (MEGS)." *International Journal of Engineering Trends and Technology* 70.3 (2022): 132-139.

22. Rajeswari, S., N. Ramya, and K. Saranya. "Avalanche effect based variants of playfair cipher for data security." *International Conference on Explorations and Innovations in Engineering & Technology, Issn*. 2016.
23. Hussain, T., Faiz, R. B., Aljaidi, M., Khattak, A., Samara, G., Alsarhan, A., & Alazaidah, R. (2023). Maximizing Test Coverage for Security Threats Using Optimal Test Data Generation. Applied Sciences, 13(14), 8252. https://doi.org/10.3390/app13148252.
24. Almaini, A., Al-Dubai, A., Romdhani, I. et al. Lightweight edge authentication for software defined networks. Computing 103, 291–311 (2021). https://doi.org/10.1007/s00607-020-00835-4.