

A secure cryptographic framework: Leveraging Fermat's two squares theorem and trigonometric transformations for enhanced encryption

Ranjith Kumar

*School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India,
Vidyabharathi Dakshinamurthi*

Computer Science and Engineering, Sona College of Technology, Junction Main Road, Salem, India

M Marimuthu, Aryaman Tamotia and Dhruv Shantu Karmokar

School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India

P Revathi

Department of Computer Science and Engineering, C. Abdul Hakeem College of Engineering and Technology, Melvisharam, India

ABSTRACT: The rapid growth of cybersecurity challenges demands faster and stronger cryptographic algorithms for text and image encryption. This study introduces a new encryption algorithm based on the concept of the Fermat theorem and the use of trigonometric functions and transformations and the current cryptographic tools. The proposed approach will improve the security of data, as it is a more robust approach to saving sensitive information that combines the characteristics of transcendental number and trigonometric transformations. A prime number that is congruent to one, modulo four defines two secret keys which Fermat has established in his Theorem. The keys are then applied during the trigonometric transformation phases of encryption process. The protocol uses the decimal representation of a transcendental number to encode the plaintext characters to unique numerical values adding resistance to frequency and brute force attacks. Tangent and arc-tangent functions are trigonometric transformations that are used in both encrypting and decrypting the messages, which transform the integers into floating point numbers, and bring great non-linearity in the communication medium. The characteristics of trigonometric function and transcendental number lay a mathematically sound system guaranteeing a high entropy and accurate reversibility. Experimental verification spells out that the decryption protocols recover the original secret message with perfect fidelity, which makes the accuracy and reliability of the proposed method.

Keywords: Fermat's two squares theorem, Trigonometric Transformations, Diffie-Hellman algorithm, Transcendental number, Encryption and Decryption

1 INTRODUCTION

The security of information transmission has become a key issue in the contemporary digital age. The dramatic increase in internet-related communications and cybersecurity risks has necessitated the need to come up with new cryptographic schemes to safeguard sensitive information against unauthorized access or information leaks. Secure communication relies on the modern cryptographic techniques that ensure the confidentiality, integrity, and

authenticity of the information being transmitted or stored [1]. The success of these cryptographic protocols however is based on their resistance to a number of cryptanalytic attacks in addition to being computationally efficient. The traditional cryptographic functions such as AES and RSA are still at the core of securing digital communication systems [2], but their scalability and inability to withstand emerging complex attacks/threats are increasingly challenged by the modern development of advanced mathematical methods and quantum computing [3]. Most of these implemented algorithms are strongly based on proximate factorization and discrete logarithm tasks, which are secure in the existing world of computation constraints, but could be weaker in the future as the new models of computation change [4]. This scenario highlights the dire necessity of powerful methods that will embrace fresh mathematical rules in enhancing security flexibility to counter the fast-paced developments of all traditional existing attacks [5].

In order to tackle these arising issues, the current paper suggests a new encryption algorithm named as a multiplication of Fermat Two Squares theorem, trigonometric transformation, and transcendental number as an improvement to the data security. By the use of the theorem of Fermat, one can construct unique pairs of keys based on the prime numbers in an easy, reproducible and random manner. Diffie-Hellman key exchange protocol is a key exchange between parties that are sure without any common secrets which have been agreed on previously [5]. Using the non-repeating, infinite, decimal expansion of the transcendental number, and, as a result, increasing resistance to frequency and multi-brute force attacks [6]. The introduction of trigonometric functions also brings with them non-linearity and diffusion of more resistance to the cryptanalytic attack and thus more resistant to the readability of the ciphertext [7] and [8]. This layered design does not only enhance the general encryption process, but also provides a mechanism that takes care of the fact that the original message can be effectively recovered by decryption in a manner that is secure and reliable [9].

2 RELATED WORK

In this section, there are five critical studies on the relevant literature about cryptographic techniques and their applications in reference to the problem findings and their merits and demerits of creating robust encryption algorithms. The enhanced cryptography method suggested by Ali and others in [5] adapts the classical method of Diffie-Hellman key exchange algorithm in WSNs. The authors find some drawbacks of the traditional Diffie-Hellman algorithm in a resource-constrained setting by optimizing computational performance and reducing the energy usage. The scheme proposed enhances key management and authentication activities in the WSNs that guarantee high resilience against different attacks, especially man-in-the-middle attacks and replay attacks [10].

Belazi *et al.* [3] introduced an enhanced chaotic map algorithm that combines the sine and tangent functions for medical image encryption. The approach suggested relies on the sensitivity of chaotic systems to the initial condition to achieve high security [11]. The research attains a high encryption algorithm of image information, which has high resistance to statistical and differential attacks. High-order chaotic maps enhance more randomness and uncertainties to sensitive information like medical images [12]. In another study, Liestyowati [13] gave a detailed introduction to the concept of the public key cryptography, explaining its fundamental concepts and most of the algorithms, such as ECC and RSA.

Wang [4] talks of applying the Fermat Little Theorem in cryptographic applications, and how the theory can be applied in modular arithmetic. The paper demonstrates that the theorem can be used to further the number theory based encryption/decryption algorithms. The piece is still quite theoretical, as it has not been experimentally tested or applied to practice. Other research studies of similar type [14] and [15] also contain theoretical discussions and lack a proof of the behavior and practicality of the suggested work. In a homomorphic encryption scheme, it was proposed by Harmon *et al.* [6] that the encoding of

arithmetic operations is done using a p-adic integer encoding (PIE) scheme. PIE scheme is more accurate in such computations and is useful in privacy preserving applications, including secure multiuser computation and machine learning [16] and [17]. The encoding with p-adic numbers can be highly complicated and intensive computational cost which has an impact on the execution speed and capacity of encryption machine [18] and [19]. Its practicality is limited by the fact that the need to control defects requires specific accuracy, which is not always feasible in a resource-constrained setting.

3 PROPOSED METHODOLOGY

The proposed encryption/decryption scheme incorporates a number of complicated mathematical principles to provide a secure, efficient and reversible cryptography scheme. The general framework presented in Figure 1 is a combination of Two Squares Theorem by Fermat, Diffie-Hellman Key Exchange protocol, π -digit-based encoding, and trigonometric transformations. Both the development of the methodology and its presentation have been done in a way that is easy to understand and reproduce, which is why implementation is not paramount and does not need any exhaustive computational efforts.

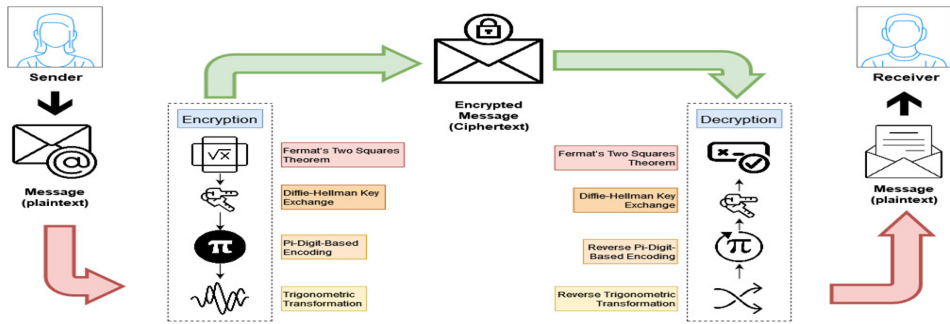


Figure 1. The proposed algorithm.

3.1 Key generation

A number p randomly chosen prime number such that $p \equiv 1 \pmod{4}$ (i.e., p is a term in the expression of $4n + 1$, where n is some). The prime number p is the base of generation of the primary keys, where the primary key takes advantage of the mathematical characteristics of the prime number to achieve greater security. According to Fermat in his two squares theory,

“Let $p > 2$ be a prime number, then the equation $x^2 + y^2 = p$ has a solution in integers iff $p - 1$ is a multiple of 4, i.e. $p \equiv 1 \pmod{4}$ ”.

The algorithm uses this the above theorem to determine the keys x and y so that p is the sum of their squares, i.e., $p = x^2 + y^2$. This encryption/decryption scheme is based on the following keys x and y ; these keys are different, strongly mathematically correlated, computationally infeasible when p is large enough. Moreover, determinism of the scheme also provides consistency in the generation of keys, which enhances both randomness and reliability in the scheme. Assume $x < y$, the users will select their own private keys in such a way that the sender has his/her private key, which is x , and the receiver has its private key, which is y . In the case of every message transmission, a new prime number of the form $4n+1$ greater

than the previous p is selected, with users being able to produce fresh keys of x and y . It provides per-session key renewal; therefore, the process possesses forward secrecy and enhances the general cryptographic security. These numbers are then applied in the following step of key exchange. Diffie Hellman Key Exchange is used to exchange a common key p between the users over a secure channel.

3.2 Encryption process

Upon completion of key generation protocol and exchange phase, plaintexts are encrypted by means of the decimal expansion of the transcendental number π (π). The non-terminating and non-repeating nature of π assures a high degree of randomness and unpredictability. The Pi-digit encoding brings in a sense of uniqueness, which increases resistance of the algorithm to attacks of frequency analysis. Each character in the plaintext is assigned to a numerical value: $A=0, B=1, \dots, Z=25$. The number of required π digits is determined by the sum of the sender's private key x and the message length: *Required Digits* = $x + \text{Length of Message}$. For each character, the corresponding π digit π_{x+i} (where i is the character's position in the message) is added to its numerical value and taken modulo 26: $m'_i = (m_i + \pi_{x+i}) \bmod 26$.

3.3 Trigonometric transformation

After encoding with π -digits, additional obfuscation with trigonometric transformations is performed. The ciphertext numerical values m_i are added as a string and divided into 4 digit blocks. All the segments are translated to a floating-point value by pre-stating them with the value 0. in radians: $\theta_i = 0.$ *segment*. The tangent of every θ_i is then calculated to bring non-linearity and complexity: $t_i = \tan(\theta_i)$. The tangent values make the final encrypted data and they are now non-linearly transformed and which gives another security.

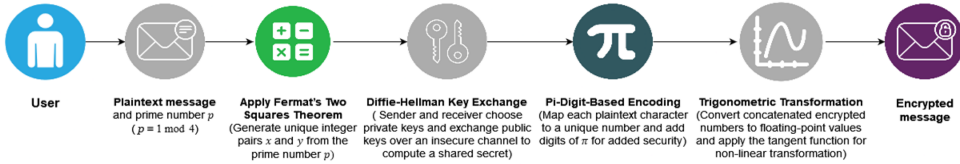


Figure 2. Encryption process.

3.4 Decryption process

Figure 3 shows the encryption stages during the decryption process that is reversed. It begins with the arctangent function because this will convert the value of tangent into its original radians using $\theta_i = \arctan(t_i)$, each θ_i scales it by 10,000, after which it will pull out the decimal portion, followed by separating these into two-digit numbers. To retrieve the original numerical values m_i subtract corresponding digits from π modulo 26: $m_i = (m'_i - \pi_{x+i}) \bmod 26$. Finally, the numerical values are converted back into alphabetic characters to reconstruct the plaintext.

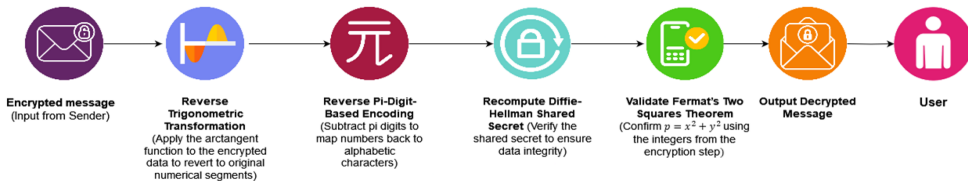


Figure 3. Decryption process.

3.5 Bidirectional communication

To establish two-party secure communication, the receiver can apply the same encryption process to send a reply to the sender using their own secret key y . In the initial stage both users exchange the prime key p through the Diffie-Hellman protocol and then construct their secret keys x and y using Fermat's theorem. No further key transmission is required. For every subsequent communication new key pair (x, y) is generated from a newly chosen prime number p' of the form $4n+1$ larger than p . It ensures that the keys are dynamic in each transmission and gives higher security.

4 IMPLEMENTATION

This section presents a detailed, step-by-step design of the introduced encryption and decryption algorithm. The plaintext message for this demo will be "ATTACK" and the prime number $p = 13$, satisfying $p \equiv 1 \pmod{4}$. Thus, we have found $x = 2$ and $y = 3$, since $13 = 2^2 + 3^2$, and assume the plaintext is: "ATTACK". To establish a shared secret between sender and receiver: Primitive Root: For $p = 13$, possible primitive roots are 2, 6, 7, 11. Let us choose $g = 2$.

- Private Keys: Choose private keys $a = 5$ (sender) and $b = 7$ (receiver).
- Public Keys: $A = g^a \pmod{p} = 2^5 \pmod{13} = 6$, $B = g^b \pmod{p} = 2^7 \pmod{13} = 11$.
- Shared Secret: sender computes $s = B^a \pmod{p} = 11^5 \pmod{13} = 7$. Similarly, the receiver computes $s = A^b \pmod{p} = 6^7 \pmod{13} = 7$. Thus, both parties have the common key $s = 7$.
- Pi Digit Calculation: To proceed, we need $(x + \text{message length})$ digits of π after the decimal point. Here, $x=2$ and the message length is 6, a total of 8 digits of π are needed. Extract digits: $\pi = 3.1415\dots$, so digits after decimal are: $\pi_{x+i} = 1, 4, 1, 5, 9, 2, 6, 5$.
- Plaintext m_i : $A \rightarrow 0$; $T \rightarrow 19$; $T \rightarrow 19$; $A \rightarrow 0$; $C \rightarrow 2$; $K \rightarrow 10$. For each character, compute the encrypted value using $m'_i = (m_i + \pi_{x+i}) \pmod{26} = 1\ 24\ 2\ 2\ 8\ 15$. Concatenate the encrypted numbers m'_i into a single string and form 4-digit segments (add leading zeros if necessary): [0124, 0202, 0815]. Convert each segment into a floating-point number by dividing by 10000: $\theta_1 = 0.0124$; $\theta_2 = 0.0202$; $\theta_3 = 0.0815$.
- Compute $t_i = \tan(\theta_i)$ (assuming θ_i is in radians): $t_1 \approx 0.0124009$, $t_2 \approx 0.0202034$ and $t_3 \approx 0.0817047$. The values t_i serves as the encrypted data segments. The decryption process is performed as the inverse of the encryption process, utilizing the operations *Arctangent*, *Segment Reconstruction*, and *Reverse Pi – Digit Encoding* to recover the original data.

5 RESULTS AND DISCUSSION

The theoretical analysis and practical implementation of the proposed approach dealt with the effectiveness and strength of the proposed approach. Various mathematical theories can be integrated into the security provisions.

- Uniqueness: Pi-digit-based encoding ensures that the characters do not have the same encryption, thereby creating some aspect of uncertainty.
- Non-Linearity: Exponential and trigonometric functions bring in non-linear changes and this constitute several layers of security.

5.1 Testing methodology

The overall benchmarking process was observed in order to measure the performance of the new encryption scheme. It tested small and medium-sized messages and showed encryption

time and decryption time in milliseconds and measured the memory used to assess the efficiency of the algorithm. The validity and repeatability of the results were guaranteed by the statistical analysis of the obtained information. Its results were compared with the familiar cryptographic algorithms, AES and RSA, to determine the performance of this suggested method, specifically in terms of speed and consumption of resources [20].

5.2 Comparative analysis

The efficiency of the proposed algorithm can however be compared in a number of aspects with standard encryption algorithms like AES and RSA as shown in Figure 4. It also gives a detailed comparison of the performance measurements, which are time taken to encrypt and decrypt, the complexity of computation, memory consumed and the level of security achieved. The algorithm is much faster in encrypting and decrypting data than the AES and RSA. This is mainly because of the Fermat, an addition of the Theorem of Two Squares, pi-digit encodings and the trigonometric transform it does not lose its security.

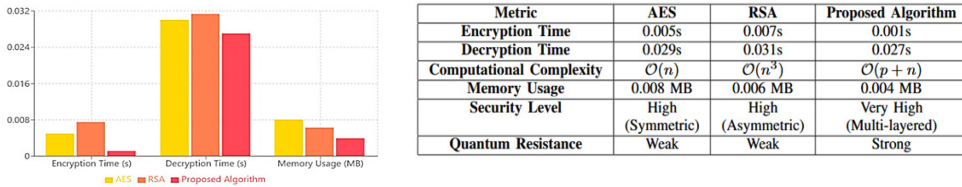


Figure 4. Comparison of proposed algorithm with existing methods.

6 CONCLUSION

The suggested encryption algorithm is an effective and safe system, which integrates Fermat theorem, encoding with π -digits, and the tangent. It is a promising and flexible application in cryptography in its dynamic key generation concept since it guarantees higher security, non-linearity, and limitness keys.

REFERENCES

- [1] Menezes A.J., P.C. Van Oorschot, and S.S. Vanstone, (2014). *Handbook of Applied Cryptography*, CRC Press, Boca Raton.
- [2] Shetty P., Ranjith Kumar M., Vyas T., Gehlot A.M, A. and Pant K. (2022). Application of cryptographic methods to blockchain technology to increase data reliability, *Inter. Conf. on System Modeling & Advancement in Research Trends*, IEEE, pp. 848–852
- [3] Belazi A. *et al.*, (2022). *Journal of Information Security and Applications* 66 103131
- [4] Gupta M. and Sinha A. (2021). Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks, *Inter. Jr. of Information Tech.*, 13, pp. 933–941.
- [5] Tang Y. (2020). Security design and application of internet of things based on asymmetric encryption algorithm and neural network for Covid-19, *Jr. of Intelligent and Fuzzy Systems*, 39 (6), pp. 8703–8711.
- [6] Harmon L. *et al.* (2023). *Inter. Conf. on Applied Cryptography and Network Security*, 425–450.
- [7] Dileep, M. Durairaj, S. Subudhi, Rao VVRM, J. Jayanthi, D. Suganthi, (2023). AI-driven drowned-detection system for rapid coastal rescue operations, *Spatial Information Research, SpringerNature*, 32,143–150.
- [8] Kumar M.R., Mani R., Revathi P., Sabarinathan S., and Govindan V. (2023). *International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, 1–5.

- [9] Shirazi S.A.R., Shah S.A., Wahab A., and Fatima M. (2024). *The Asian Bulletin of Big Data Management* 4 1 261–275.
- [10] Xiang G. and Cui Z. (2012). *2012 International Conference on Communication Systems and Network Technologies*, 978–981.
- [11] Goswami P.S., Chakraborty T., and Chattopadhyay A. (2021). *Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 1–8.
- [12] Arshad B. and Siddiqui N. (2020). *International Journal of Computer Science and Information Security* 18 4 109–122.
- [13] Tsafack N. *et al.* (2020). *Information Sciences* 515 191–217.
- [14] Chan H.L. (2022). *Proceedings of the 11th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2022)*, 251–264.
- [15] Li, Z., Yang, *et al.*, (2025). A remote sensing image encryption and compression scheme using novel hyperchaotic system and plaintext related random S-box. *Nonlinear Dyn* 113, 2769–2790.
- [16] Zhang B., Liu L. (2023). Chaos-based image encryption: review, application, and challenges. *Mathematics*, 11, 2585.
- [17] Trujillo-Toledo D.A., *et al.* (2021). Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps, *Chaos, Solitons & Fractals*, 153(2), 111506.
- [18] Ramya P., Karthik B. (2023), Word sense disambiguation based sentiment classification using linear kernel learning scheme, *Intelligent Automation and Soft Computing*, 36(2), 2379–2391.
- [19] Sharma T., M.R. Kumar, S. Kaushal, D. Chaudhary and K. Saleem, (2023). Privacy aware post quantum secure ant colony optimization Ad Hoc on-demand distance vector routing in intent based internet of vehicles for 5G smart cities, *IEEE Access*, 11, 110391–110399.
- [20] Kumar, M.R., Naik, D.A., Kapila, N. *et al.* (2024). A novel approach to detect, analyze and block adversarial web pages. *Int. J. Inf. Technol.* 16, 3617–3622.