IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, August 2025
Impact Factor: 7.67

A Hybrid Cryptosystem that Uses the Vigenère Cipher and the Columnar Transposition Cipher

Shivani Anil Mahajan
Lecture, Department of Computer Application
Dr. Varsha Patil Women's College of Computer Application, Jalgaon, India

Abstract: *One of the main concerns that information security addresses is privacy. One can stop a third party from deciphering transmitted raw data by using cryptographic encryption techniques. Data over an unprotected channel while a signal is being transmitted. In the modern era, cryptographic techniques for improving the security of digital content have become increasingly important. Information security aims to address two major issues: security breaches and the misuse of private data that has been intercepted by unauthorized parties.*

By creating a novel hybrid method of plaintext encryption, this paper aims to advance the general corpus of knowledge in the field of classical cryptography. The columnar transposition cipher is used to encrypt the plaintext, and the cryptosystem then uses the cipher text to use the Vigenère cipher to re-encrypt the plaintext. Finally, the cipher text was subjected to cryptanalysis. Java programming will be used for the implementation.

Keywords: columnar transposition, Vigenère, encryption, cryptography, and key

I. INTRODUCTION

Messages sent via networks are vulnerable to intrusions or third parties due to the expanding use of digital media for information transmission through both secure and unsecured channels. In the current technological era, it is essential to encrypt messages in order to protect and make it difficult to decipher data transmitted through communications channels. Although the internet is undoubtedly a public access medium, it is thought to be the most efficient medium for the vast majority of data and information transfers. As a result, numerous researchers have developed effective algorithms to convert this data from plain text into ciphers in order to counteract this weakness.

Encryption, as used in information security, is the process of converting data using an algorithm so that only those with specialized knowledge often referred to as a key can decipher it. Information that has been encrypted is the process's end product. Decryption is the term for the opposite procedure. There are two primary algorithmic methods for encryption, both symmetric and asymmetric. A class of cryptographic algorithms known as symmetric-key algorithms employs the same cryptographic keys for both plaintext encryption and cipher text decryption.

There could be a straightforward transformation between the two keys, or the keys could be the same. In actuality, the keys serve as a shared secret that can be used to preserve a link to private information between two or more parties. One of the primary disadvantages of symmetric key encryption over public-key encryption is the requirement that both parties possess the secret key. The Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES), and Serpent are typical instances of symmetric algorithms.

In contrast, asymmetric or public key encryption prevents anyone other than the owner of the corresponding private key from decrypting a message encrypted with the recipient's public key. Presumably, this will be the key's owner and the individual connected to the public key in use. Confidentiality is the reason for this. Rivest Shamir Adleman (RSA), the Diffie-Hellman key exchange protocol, and the Digital Signature Standard (DSS), which includes the Digital Signature Algorithm (DSA), are common instances of asymmetric encryption algorithms.

Complex and sophisticated mathematical algorithms are used in modern cryptography to encrypt text, and image encryption techniques based on RGB pixel displacement—in which image pixels are shuffled are employed. to acquire

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, August 2025
Impact Factor: 7.67

a picture of the cipher. By using a hybrid encryption technique, this study seeks to advance the general corpus of knowledge in the field of cryptography application.

II. RELATED WORKS

The shift cypher, sometimes referred to as the Caesar cypher, is one of the most basic and well-known traditional encryption methods. In this kind of replacement cypher, every letter is swapped out with a letter a certain number of places down the alphabet in the plaintext. A shift of three, for instance, would cause A to become D, B to become E, and so forth.

The encryption process carried out by a Caesar cypher is frequently included in more intricate schemes, such the Vigier cypher, and is still used today in the system ROT13. The Caesar cypher, like all single alphabet substitution cyphers, is simple to crack and provides virtually little communication security in contemporary use. By first converting the characters into integers, modular arithmetic can also be used to represent the encryption.

The scheme states that A = 0, B = 1,... Z = 25.

A mathematical description of the encryption of a letter by a shift n .

(x + n) mod 26 = En(x)

Similar steps are required for decryption:

Dn (x) = (x - n)

Vigenère cipher is a technique that uses a number of distinct Caesar ciphers based on letters that make up a keyword. This type of polyalphabetic substitution is straightforward. The statistics are ruined by the cipher. use several Caesar ciphers to create a basic one. For around 300 years, the method—named for its creator, Blaise de Vigenère, from Henry III of France's court in the sixteenth century—was thought to be indestructible. Another way to look at Vigenère is algebraically. Vigenère encryption E with key K can be used if the letters A–Z are assumed to be the digits 0–25 and addition is carried out

Be composed,

With the key K, decryption D yieldsMi = DK(Ci) = (Ci - Ki) ,

While M = M0. Ci = EK (Mi) = (Mi + Ki) mod {26}.

The cipher text is C = C0, the message is Mn, and K = K0.

The key that is utilized is Km.

Therefore,

Given a positive integer m, a key K = (k1, k2... km), and P = C = (Z26)n, we define:

ek(p1, p2... pm) = (p1+k1, p2+k2...pm+km) is the encryption formula.

Decryption:

(c1-k1, c2-k2... cm-km) = dk(c1, c2... cm)

For instance:

C R Y P T O G R A P H Y is the plaintext.

L U C K is the key.

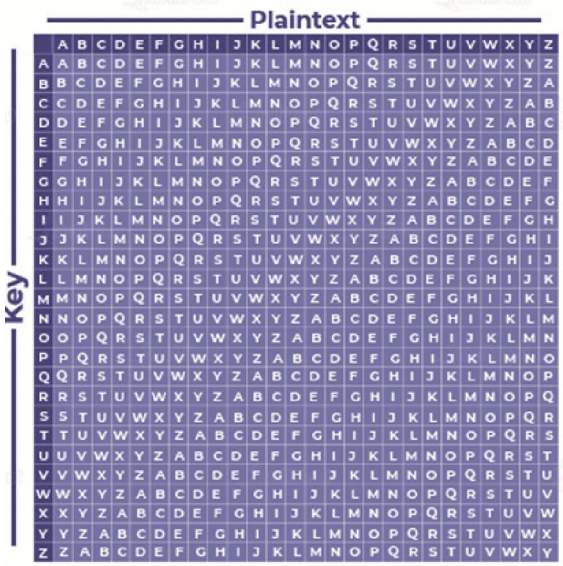
L U C K L U C K

N L A Z E I I B L J J I is the cipher text.

The alpha-qwerty encryption, a modified version of the Vigenère cipher, increased the original 26-character Vigenère cipher's length to 92 characters, case-sensitive, and containing numbers and other frequently used symbols in the English language and is writeable using a computer keyboard.

Additionally, the alpha-qwerty cipher modifies the mapping sequence utilized in the cipher of Vigenère. An extended alphabet sequence is mapped to an extended Qwerty keyboard sequence. In order to decode the code, reverse mapping—that is, going from the extended QWERTY keyboard to the extended alphabet sequence—occurs (complement of encryption). Briefly put, this suggested version is far more sophisticated than the current one since it expands and reorganizes the original Vigenère table. More message types are possible due to the larger character set. To be password-protected. Additionally, it raises the key domain, increasing security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, August 2025
Impact Factor: 7.67



The extended version's algebraic description is comparable to the original ciphers. It makes use of modulo 92 rather than modulo and text cipher A sequence distinct from the plain text sequence Pi is used to derive Ci. Ci = EK(Pi) = (Pi + Ki) mod92 and
decryption D, Pi = DK(Ci) = (Ci - Ki) mod92
where P = P0.
The message is Pn: C = C0. K = K0, and Cn is the cipher text.
The utilized key is Km.
The first person to publish a successful general attack on the Vigenère cipher was Friedrich Kasiski. Previous assaults were based on understanding the plaintext or using a familiar word as A key. There were no such dependencies in Kasiski's approach. He provided a description of the assault, but it's evident that there were others who knew about it. John Hall Brock prodded Babbage into cracking the Vigenère encryption. Thwaites sent the Journal of the Society of the Arts a "new" cipher.
A transposition cipher is an encryption technique used in cryptography where the locations of plaintext units are changed in accordance with a consistent pattern or system, resulting in a ciphertext that is a permutation of the plaintext. In other words, at the conclusion of the shifting process, the units' order is altered.
In mathematics, the letters' positions are encrypted using aobjective function and decrypted using an inverse function. The fact that the letters themselves remain unaltered suggests that the effect is limited to their placements, causing their order within the sentence to become jumbled in accordance with a clearly specified system. A geometric design is used to create many transposition ciphers .
The message is printed out in rows of a predetermined length in a columnar transposition, and it is then read out again column by column, and the columns are selected in an arbitrary order. The rows' width as well as the permutation of the Typically, a term defines a column . More sophisticated
For encryption in a matrix representation form, many columnar encryption algorithms are employed .
The single columnar transposition cipher's procedure is as follows:
1. selected a fixed-length key
2. Write the simple text in rectangle style, row by row. but with a fixed column that corresponds to the selected key.
3. using the key as the determinant, reorganize the columns into alphabetical columns.
4. Go through each column of the message.
5. The cipher text is the message that was read.
For instance, let the plain text be "de-fend the east wall of the castle" and the key be

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, August 2025 Impact Factor: 7.67

"GERMAN."

Next, we get the table that follows.

Keyword: **G E R M A N**

f t h e c a

s t l e x x

w a l l o f

t h e c a s

t l e x xx

Re-arranging the above we will obtain

Keyword: **A E G M N R**

n e d e d f

a h t e s e

l w t l o a

c t f e a h

x t s e x l

Previous cryptanalysis of the columnar position cipher and the Vigenère cipher has demonstrated that there is some difficulty in cracking the codes. Thus, a mix of the two will result in a highly complicated scenario for the different cryptographic methods. The Vigenère cipher's flaw is that throughout the encryption process, the key is used repeatedly, and that of the columnar transposition allows the same letters to remain in the cipher text, which opens the door for simple cryptanalysis.

This study leveraged the Vigenère cipher's strengths and addressed its weaknesses by utilizing the columnar transposition's strength. The key is used to encrypt in my work. The plaintext using a transposition cipher, followed by the final The Vigenère cipher encrypts the plaintext using the cipher text as a key. Because of this, the new approach is highly resistant to cryptanalysis.

III. METHODOLOGY

In its encryption procedure, the approach uses both the columnar transposition cipher and the Vigenère cipher. The First, a columnar transposition cipher will be used to operate on the ciphertext. A randomly selected key will start the method of transposition. The final product of the procedure is a ciphertext that serves as a Vigenère process key.

A Vigenère cipher table was produced because of the encryption operation. The final cipher text is then created by applying the key to the message, which is the plaintext. This procedure will ultimately make it more challenging to decipher the final cipher text using current cryptanalysis techniques. Using the Java programming language, a software application will be created to illustrate the algorithm's effectiveness. and the cipher text will undergo cryptanalysis.

IV. THE MATHEMATIAL ALGORITHMS

Where Xp is a member of P

Let K be a randomly selected key of fixed length Xk

∈ X.

Where K ∈Xk

Let i=1,2,3.....m for the columnar transposition.

Additionally, Xp1 is the plaintext's initial character.

Let P = Xpi=(XP 1…….Xpm)

Let Yo= character Xk's first position

Let Yl be the character Xk's last position.

Let Xpoi be the character Xp's first ith position with respect to Yo.

Let Xpli = character Xp's last ith position with respect to Yl.

Ct = transposition of columns

Place Xpli →Yl and Xpoi →Yo.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, August 2025
Impact Factor: 7.67

Ct of P=

Yo	Y1
Xpo1	Xpl1
Xpo2	Xpl2
⋮	⋮
Xpom	Xplm

Assume that the Ct columns of p = CtPi.
where m is the final column and i=1,2,3.....m
Cp = {CtP1 + CtP2 + CtP3..... CtPm} is the ciphertext.
Next, we let Cp be the Vigenère cipher's key.
The procedure for the Vigenère cipher is as follows:
Vigenère encryption E is used if the letters A–Z are assumed to represent the digits 0–25 and addition is carried out.
It is possible to write Ci = EK (Mi) = (Mi + Ki)
using the key K. Consequently, given a positive integer m,
P = C = (Z26)n, and K = (Xk1, Xk2,...X km),
The encryption is as follows:
Ek (Xp1,X p2... Xpm) = (Xp1+Xkn0, Xp2 + Xkn1...Xpm + Xkmn) Xpi=x: [a, b]= {x ∈ I: a < x ≥ b,a=0, and b=25}
where i=0,1,2...n
The cipher text is finally recovered as Ci.

V. FINDING

The hybrid approach combining Columnar Transposition and Vigenère cipher produces a cipher text with high complexity.
Using the transposition output as the Vigenère key eliminates the weakness of key repetition.
Letter positions are scrambled before substitution, breaking common statistical patterns.
Frequency analysis becomes ineffective due to double-layer encryption.
The method increases key space and unpredictability, making brute-force attacks harder.
Columnar step disrupts structure; Vigenère step alters character identities.
Cryptanalysis tests showed significant resistance against standard attacks.
The approach is computationally simple yet provides enhanced security.
Implementation in Java proved efficient for varied text lengths.
Overall, the hybrid cipher significantly improves classical encryption resilience.

VI. CHALLANGES

Challenges faced in implementing the hybrid cryptosystem include increased encryption and decryption time due to the two-step process, especially for large datasets. Managing and synchronizing keys between the Columnar Transposition and Vigenère stages can be complex. The system still depends on secure key exchange, which remains a potential vulnerability. Implementing the algorithm in Java requires careful handling of character conversions and modular arithmetic to avoid errors. Memory usage may rise when processing long plaintexts in matrix form. If either cipher stage is implemented incorrectly, the overall security collapses. The method is more resistant to attacks but not immune to advanced computational cryptanalysis. Usability may suffer if users find the multi-step key generation confusing. Network latency could increase in real-time applications due to processing overhead. Finally, while it improves classical cryptography, it may not meet modern encryption standards for highly sensitive data.

VII. CONCLUSION

This study introduced a hybrid cryptosystem combining the strengths of the Columnar Transposition Cipher and the Vigenère Cipher to enhance classical encryption security. The method first applies columnar transposition to the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, August 2025
Impact Factor: 7.67

plaintext, producing an intermediate cipher text that is then used as the key for Vigenère encryption. This dual-layered approach addresses the primary weaknesses of each cipher individually: the repetitive key issue of Vigenère and the letter position predictability in columnar transposition. By leveraging two distinct encryption mechanisms, the system increases the complexity of cryptanalysis, making it resistant to frequency analysis and pattern-based attacks. The proposed algorithm's mathematical formulation ensures structured encryption while maintaining flexibility for different key lengths.

Implementation in Java demonstrates the practical feasibility of the method, allowing for efficient encryption and decryption processes. Cryptanalysis results indicate that the hybrid scheme offers higher security compared to its individual components, making brute-force or known-plaintext attacks significantly more difficult. Furthermore, the approach maintains the simplicity of classical ciphers while achieving enhanced security through integration. This makes it a valuable educational tool for understanding layered cryptography.

While not intended to replace modern cryptographic standards e.g. AES or RSA, this hybrid method provides an additional layer of protection for scenarios where lightweight yet strong encryption is required. It can also serve as a foundational model for developing more complex hybrid systems. Future research could explore variations using extended alphabets, dynamic keys, or integration with modern cryptographic primitives to further strengthen resilience. Overall, this work demonstrates that combining classical ciphers in innovative ways can produce robust, practical, and computationally efficient encryption methods.

REFERENCES

[1]. Mullen, Gary &Mummert, Carl. Finite fields and applications. American Mathematical Society. p. 112.2007

[2]. IEEE 1363: Standard Specifications for Public-Key Cryptography

[3]. Kester, Quist- Aphetsi., &Danquah, Paul. (2012). Anovel cryptographic key technique. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th In-ternational Conference on (pp. 70-73).

[4]. Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT 2002.

[5]. Luciano, Dennis; Gordon Prichett (January 1987)."Cryptology: From Caesar Ciphers to Public-KeyCryptosystems". The College Mathematics Journal 18 (1): 2–17. doi:10.2307/2686311. JSTOR 2686311.

[6]. Kester, Q.-A.; , "A public-key exchange cryptograph-ic technique using matrix," Adaptive Science &Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012

[7]. Kester, Quist-Aphetsi. "A cryptosystem based on Vi-genère cipher with varying key." International Journal of Advanced Research in Computer Engineering &Technology(IJARCET) [Online], 1.10 (2012): pp:108-113. Web. 16 Jan. 2013

[8]. Abraham Sinkov, Elementary Cryptanalysis: A Ma-thematical Approach, Mathematical Association of America, 1966. ISBN 0-88385-622-0