2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

ORIGINAL RESEARCH Open Access

Advancing Post-Cryptographic Schemes Using Number Theoretic Structures: Algorithms, Security, and Real-World Implementation

Jency J[1]and Usha A[2]

Received: 20 May 2026/ Accepted: 08 June 2026 / Published online: 29 June 2026

Abstract

Cryptography, a term rooted in Greek that translates to 'secure writing,' encompasses the intricate study of methods employed to encrypt and decrypt information, ensuring secure communication between parties. This fundamental discipline plays a critical role in safeguarding sensitive data from unauthorized access and malicious entities. The process begins with encryption, where plain text, or the original readable information, is transformed into ciphertext through specific algorithms and protocols. This transformation obscures the content, making it unintelligible to anyone who does not possess the appropriate keys or credentials to decode it. Decryption is the complementary process that reverses this transformation, restoring the ciphertext to its original plain text format. This allows authorized users to access the information securely while preventing would-be intruders from deciphering its contents. In addition to these basic principles, modern cryptography incorporates various techniques, such as symmetric and asymmetric encryption, digital signatures, and hash functions, each serving specific purposes in the realm of data protection and secure communication. Overall, cryptography is essential in today's digital landscape, underpinning everything from online banking transactions to secure messaging systems and helping to ensure the integrity and privacy of information exchanged over insecure networks.

[1] Research Scholar, Department of Mathematics, Ponnaiyah Ramajayam Institute of Science and Technology (PRIST) Deemed to be University, Thanjavur – 613403, Tamil Nadu, South India. Email:nehajulit@gmail.com
[2] Associate professor , Department of Mathematics, Ponnaiyah Ramajayam Institute of Science and Technology (PRIST) Deemed to be University, Thanjavur – 613403, Tamil Nadu, South India.
Email: Ushamaths89@gmail.com

2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

Key Words: Cryptography, Algorithms, Encryption, Decryption, Cipher-text

1 Introduction

We use cryptography in our work to protect secrets. Cryptography uses full mathematical theory. We use mathematical formulas so that no one can read the data. The correct mathematical algorithm ensures our data is very secure. Using algorithms like this, we protect all the data on our mobile devices. The WhatsApp application has 256-bit encryption. Creating the What's up.The application involves going through major encryption. You cannot open all the application data keys, 99% of the data is saved by using the key. Advanced post-cryptography allows us to navigate the complexities of the digital world more securely. With increasing concerns about hacking, particularly with applications like WhatsApp and telecommunications on laptops, it's crucial to ensure that our messages remain safe. By using a unique code and implementing mathematical encryption and decryption methods, we can safeguard our communications. This way, all our messages on WhatsApp and laptops can be coded securely, providing us with peace of mind regarding our privacy. In the novel I came, I was able to understand encryption and decryption easily, using alphabets and numbers and shortcuts, from table 1 to table 5. I was able to clearly understand encryption and decryption, and I have briefly noted in which research.According to in my article real life application of a number theory in mathematical modelling Real life application in number theory, first, who is found in Zero, Aryabhata, 5 to century used Zero as a placeholder in his place value system. Next, Brahmagupta, 7 to century, in a find defined Zero as a number. Then, how it works in the number system in society, how it works in numbers, in my article on the foundation of digital security and technology, is integrated into applications, like cryptography, which safeguards online transactions through algorithms that utilize prime numbers.

RELATED WORK:CEASEAR CIPER PROBLEM:

In essence, this describes a substitution cipher, a method of encryption where the letters of the original message, known as the plaintext, are systematically replaced. This replacement follows a specific rule: each letter in the plaintext is exchanged for another letter located a certain, predetermined number of positions further along in the sequence of the alphabet. This fixed shift in the alphabet is the defining characteristic of this particular type of substitution cipher, ensuring that the same letter in the plaintext is always encrypted to the same ciphertext letter.

2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

Related methodology: CRYPTGRAPHY QUANTAM TECHNOLOGY:

2 Quantum Communications

Among the various quantum information technologies, quantum communication stands out as one of the most advanced and intricate. Its primary objective is to establish quantum correlations between a sender (emitter) and a recipient (receiver). While this concept may seem straightforward, the underlying mechanics are extraordinarily complex, largely due to the distinctive properties of quantum signals. These unique characteristics enable quantum signals to accomplish tasks that are beyond the reach of classical signals. Afundamental challenge in quantum communication arises from the principle of uncertainty, particularly the impossibility of faithfully copying unknown quantum signals. This inherent limitation prevents the amplification of quantum signals, thereby constraining the effective range of quantum communications when attempting to transmit these signals through absorbing media. For instance, in optical fiber communications, the most favorable conditions occur in specific transparent windows, where optical losses typically hover around 0.2 dB/km. Under optimal circumstances, this means that after a distance of approximately 15 kilometers, the likelihood of a quantum signal successfully reaching its destination drops to about 50%. Current implementations of commercial Quantum Key Distribution (QKD) systems can handle optical losses in the range of 20–30 dB, allowing for effective communication over distances between 100 to 150 kilometers. However, the landscape of passive optical telecommunications networks is far more complicated than simple fiber optics; these networks also incorporate various additional components like splitters, filters, and multiplexers. Each of these elements contributes additional losses, compounding the challenges and typically restricting quantum communications to metropolitan areas, with some cases even limiting them to access segments within these zones. Another significant concern arises when quantum and classical signals are transmitted simultaneously over the same optical fiber. This scenario introduces complications due to phenomena such as four-wave mixing, scattering, and optical reflections, all of which further deteriorate the transmission quality of quantum signals. Traditional electro-optical conversion processes, commonly used in classical communications, cannot be applied to quantum signals as they lead to measurement and replication that compromise the quantum state. Classical signals also experience attenuation under these conditions, which is why optical amplifiers are commonly utilized in telecommunications networks to boost signal strength. However, it is

crucial to note that these amplifiers disrupt quantum signals as well, making their deployment incompatible with quantum communication. The co-propagation of classical and quantum signals introduces yet another challenge, as stray photons from classical pulses can interfere within the quantum channel, resulting in a significant increase in the error rate. This interference can quickly render the successful implementation of quantum communication protocols infeasible. Despite these numerous challenges, the field of quantum communication continues to make strides, refining methods and developing technologies to overcome the limitations posed by the unique nature of quantum signals. The ongoing research and innovation in this area promise to enhance the viability and reach of quantum communication systems in the future Simplify Technical Language: Consider simplifying some of the technical jargon or providing clearer definitions for terms like "Hilbert space," "wave function," and "Dirac notation." This would make the text more accessible to readers who may not have a strong background in quantum mechanics, enhancing overall comprehension.

Enhance Flow with Transitional Phrases: Incorporate more transitional phrases between ideas to improve the flow of the text. For instance, connecting the explanation of qubit states to the implications of the no-cloning theorem with phrases like "This leads to" or "As a result" could help readers follow the logical progression of concepts more easily.

Add Examples or Analogies: Including practical examples or analogies that relate qubits to familiar concepts might help demystify the subject. For example, drawing a parallel between qubits and everyday binary systems (like light switches being on or off) could assist in illustrating the concept of superposition in a more relatable way.

3.Technological Description and State of the Art

At the quantum level, the fundamental unit of information is the qubit. First conceptualized in 1994 by Schumacher and Wooters [19], a qubit is physically realized by a two-state quantum system. These two states represent the computational "0" and "1". As quantum-mechanical states, they are mathematically represented by state vectors within a two-dimensional Hilbert space. Physically, qubits can be embodied in various forms, such as the horizontal/vertical polarization states of a single photon, the spin up/down states of an electron, atom, or nucleus, or the charge or magnetic flux through a Josephson junction. Each of these implementations possesses a specific mathematical representation—a wave function—from which all physically relevant quantities of the system can be derived. However, from a purely

quantum information perspective, the specific mathematical form is inconsequential, and these base states are conventionally represented using Dirac notation as $|0\rangle$ and $|1\rangle$. Since these states are solutions to the Schrödinger equation, a complex linear differential equation, any linear combination thereof is also a solution. This is the superposition principle, which dictates that any state within the Hilbert space spanned by $\{|0\rangle, |1\rangle\}$ is valid, and the general form of a qubit is given by the superposition $\alpha|0\rangle + \beta|1\rangle$, where the normalization condition $\alpha^2 + \beta^2 = 1$ holds, and α, β are complex numbers. A direct consequence for information processing is the no-cloning theorem [2], as previously mentioned. While a qubit could theoretically store an infinite amount of information within the α and β values, this is not feasible due to another characteristic of quantum mechanics. When a state, such as the one described above, is measured, only two outcomes are possible: either $|0\rangle$ is obtained with a probability of α^2, or $|1\rangle$ is obtained with a probability of β^2. There is no direct access to α or β. Access would only be possible with multiple copies, allowing statistical determination of the α and β values. However, with a single quantum system, only $|0\rangle$ or $|1\rangle$ can be obtained. Following measurement, the state collapses to the state corresponding to the measurement result: $|0\rangle$ if "0" is obtained, or $|1\rangle$ if "1" is obtained. The probabilities of each outcome are given by α^2 and β^2, respectively. It is important to acknowledge the inherent randomness within the quantum realm, which enables the creation of random number generator devices.

In the realm of quantum mechanics, when we consider two qubits, the Hilbert space, which is the mathematical space describing all possible states of the system, encompasses intriguing states such as the one represented as $|\psi\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$. This particular state exemplifies a profound concept in quantum mechanics: entanglement. The most remarkable characteristic of these types of states is their inherent inseparability. Unlike classical systems, entangled states cannot be expressed as a simple tensor product of individual qubit states. In other words, we cannot find two single-qubit states, $|\phi\rangle$ and $|\varphi\rangle$, such that their tensor product, $|\phi\rangle \otimes |\varphi\rangle$, equals the entangled state $|\psi\rangle$, regardless of how we choose $|\phi\rangle$ or $|\varphi\rangle$. This fundamental non-separability is the defining feature that characterizes an entangled state, setting it apart from separable or classical states.

Now, let us delve into the consequences of performing a measurement on one of the qubits within an entangled pair. According to the measurement postulate of quantum mechanics, upon measuring one qubit, say the first one, we will invariably find that the second qubit is instantaneously projected into a specific state that is correlated with the outcome of the first

measurement. For instance, if we measure the first qubit and obtain the result "0", then, due to the entanglement, the second qubit is immediately known to be in the $|0\rangle$ state as well. Consequently, a subsequent measurement of this second qubit will produce a "0" with absolute certainty.

This peculiar behavior persists regardless of the physical distance separating the two qubits. Whether they are located adjacent to each other or separated by vast expanses of space, the correlation between their states remains intact. This seemingly instantaneous correlation is the underlying source of the "non-classical" correlations that empower quantum information processing. It is this non-locality that Einstein famously criticized, leading him to declare in 1935 that quantum mechanics was incomplete [20]. He proposed the existence of "hidden variables" that, if known, would fully explain these seemingly bizarre correlations and restore locality.

In 1965, John Bell [21] formulated a set of inequalities, now known as Bell's inequalities, that provided a means to experimentally test whether hidden variables could indeed account for the observed correlations in entangled systems. These inequalities set a limit on the correlations that can be explained by any local hidden variable theory. If experiments violate Bell's inequalities, it implies that quantum mechanics' predictions of non-local correlations are correct, and that no local hidden variable theory can fully explain the phenomena.

The initial experiments designed to test Bell's inequalities were conducted in the 1970s. However, these early experiments faced significant technical challenges, making it extremely difficult to definitively rule out the possibility of hidden variables. It wasn't until 2015 that a series of three independent and meticulously designed experiments, conducted in Austria, the Netherlands, and the United States, provided compelling evidence confirming the validity of quantum theory and definitively refuting local hidden variable theories. These experiments provided strong evidence against Einstein's objections and helped to further solidify the foundations of quantum mechanics. Quantum mechanics stands as one of the most rigorously tested and remarkably successful theories in the history of physics. It provides a framework for understanding the universe at its most fundamental level, and it unlocks information processing capabilities that are simply unattainable using classical physics alone.

In the realm of quantum communications, two of the most significant applications are Quantum Key Distribution (QKD) and quantum teleportation. Quantum Key Distribution

offers a revolutionary solution to the problem of symmetric key distribution, enabling the creation of a cryptographic key that is exclusively known to the parties executing the protocol at both ends of a quantum channel. The security of QKD is rooted solely in the fundamental laws of nature as described by quantum physics. Unlike classical cryptographic protocols that rely on computational assumptions, QKD requires no such assumptions. This means that the protocol is immune to any attacker, regardless of their computational power. This feature is known as Information Theoretic Security, ensuring that the security of the key is guaranteed by the laws of physics, not by the limitations of computational resources. QKD protocols are designed to limit the amount of information about the key that is leaked to the outside world to any desired level, providing an unparalleled level of security. Obviously, this is true in Quantum Key Distribution (QKD) is mathematically sound; however, its implementation in real devices is often subject to imperfections that may compromise security. Consequently, certifying QKD devices according to their intended security levels is an area of active research.

QKD can be performed using various protocols, which can be categorized based on whether they explicitly utilize entanglement or not. They can also be classified as prepare-and-measure protocols or based on the type of variables they use—discrete or continuous. From a security standpoint, all of these protocols can be proven to be secure. However, their implementations differ significantly and come with varying strengths and weaknesses.All QKD protocols require the ability to produce, manipulate, transmit, and measure quantum signals. In telecommunications, these quantum signals are typically photons, which are transported through either optical fiber or free space. The methods used to encode information are diverse and can include polarization, phase, and phase differences between adjacent pulses. In the case of entanglement-based protocols, photons are generated in entangled pairs. This process is more challenging and produces lower yields compared to generating single photons by attenuating a laser pulse.

Anylising>>

P = ATTACK

SHIFT KEY=3

2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

When I uncovered my true identity, an urgent code word for the attack arrived: 0, 19, 19, 0, 2, 10. By simply adding 3 to each number, I transformed it into 3, 22, 22, 35, 13. This sequence unveiled a critical message: "DWWDFN." Understanding this encryption was vital for our next steps.

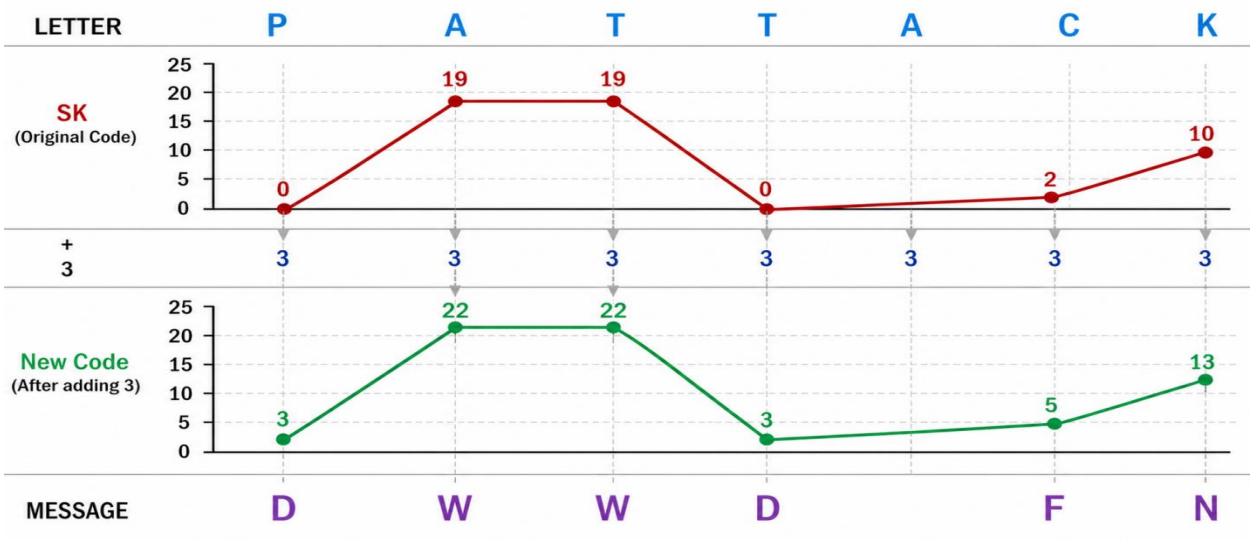
Encryption:

P=ATTACK

SHIFT KEY=3

Table:1 Encryption

A	T	T	C	K
0	19	19	2	10
3	3	3	3	3
3	22	22	5	13
D	W	D	F	N



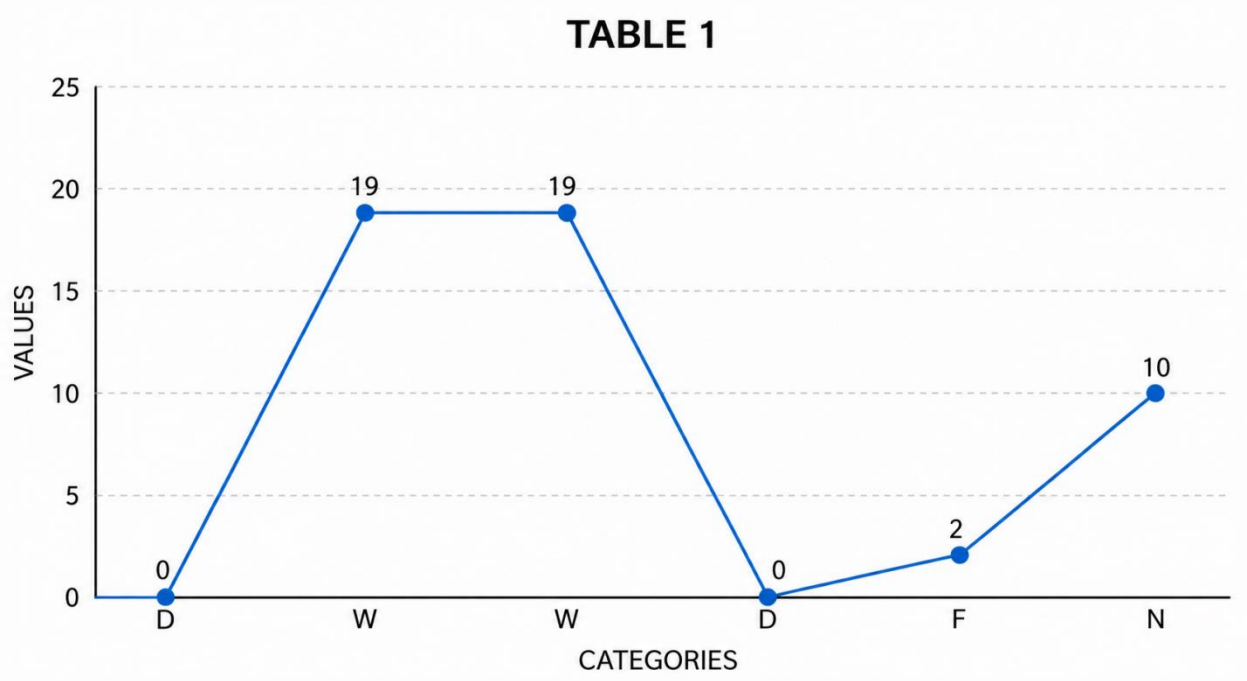
2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

Decryption: When I uncovered my true identity, an urgent code word for the attack arrived: "DWWDFN." By simply subtracting 3 from each letter's position in the alphabet, I transformed it into 3, 22, 22, 3, 5, 13. This sequence unveiled a critical message: 0, 19, 19, 0, 2, 10. Understanding this decryption was vital for our next steps: A T T A C K.

Solution is 30,19,0,2,10 is converted t decryption is Attack

Table 1.1Decreption

D	W	W	D	F	N
3	22	22	3	5	13
3	3	3	3	3	3
0	19	19	0	2	10



In advanced post-cryptography, I assign mathematical numbers to the English alphabet. For example, in the word 'hai,' the number 819 comes. If I add +2 to that, it becomes 10311. When we use that code word, we get the encrypted message 'jck'

2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

Table:2

Actual message = HAI	THIS is how it will be stored in memory	819

Table:3

Encryption = Add +2 to each character in the message.	encryption message	10311	Answer is	JCK

Table:4

KEY WORD	5131512523

W	E	L	C	O	M	E
23	5	12	3	15	13	5

TABLE 4: SENDER CODE | Letter | W | E | L | C | O | M | E | |--------|---|---|---|---|---|---|---| | Number | 23 | 5 | 12 | 3 | 15 | 13 | 5 |

Table:5

E	M	O	C	L	E	W
5	13	15	3	12	5	23

I have given the table at my place, Table 4TABLE: 4 SENDERW E L C O M E=23 5 12 3 15 13 5. How it is given is the sender message, but for the receiver.

SECTUAL TEXT:

W	E	L	C	O	M	E
23	5	12	3	15	13	5

LECTURER REVIEW:

If I say, 'What is the first table?' it means we have given the numbering corresponding to the alphabet letters. (1)In Table 2, what should be said is that we have talked about an encryption, which is our coded words. TABLE:2 *Actual message = HAI**This is how it will be stored in memory is 819. (2)

(3)In Table 3, it says that in the encryption message, a coding number is obtained by adding 2 to each character. Table 3 shows the encryption message, where each character in the message is shifted by adding 2. The encryption message is 10311. The answer is JCK. This results in no readable meaning. Encryption message: 10311. Answer: JCK. No meaning (unreadable format).

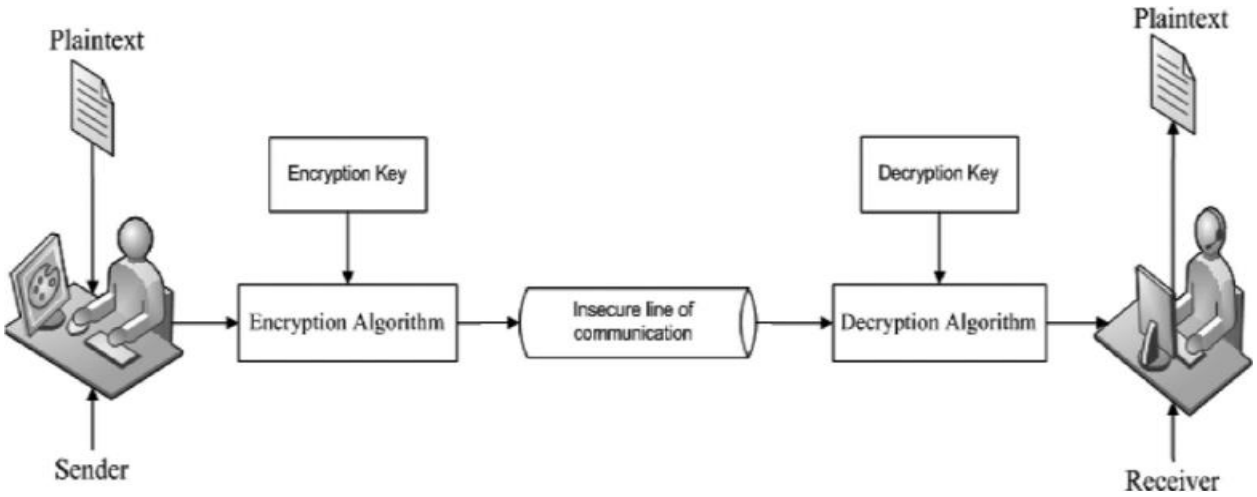
(4)Table 4 shows that if a solution is given, the alphabet's letter code word provides the answer in numbers. What is the sender code word?

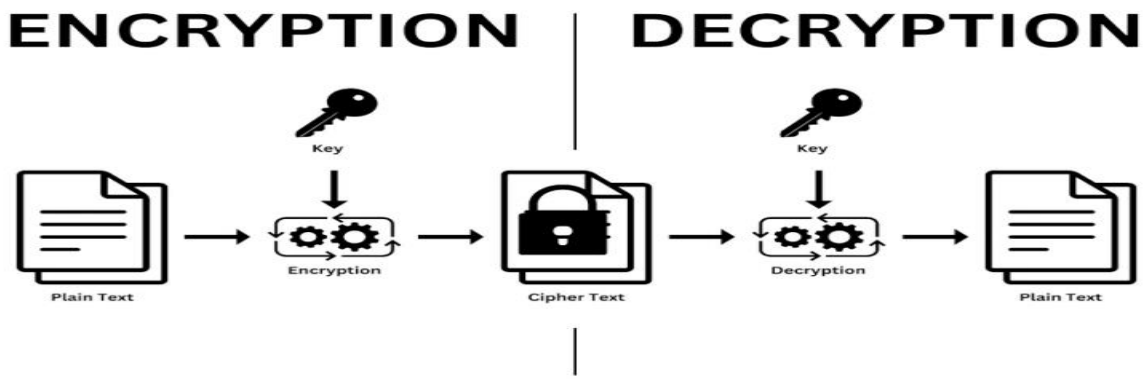
TABLE 4: SENDER CODE | Letter | W | E | L | C | O | M | E | |--------|---|---|---|---|---|---|---| | Number | 23 | 5 | 12 | 3 | 15 | 13 | 5 |

2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237

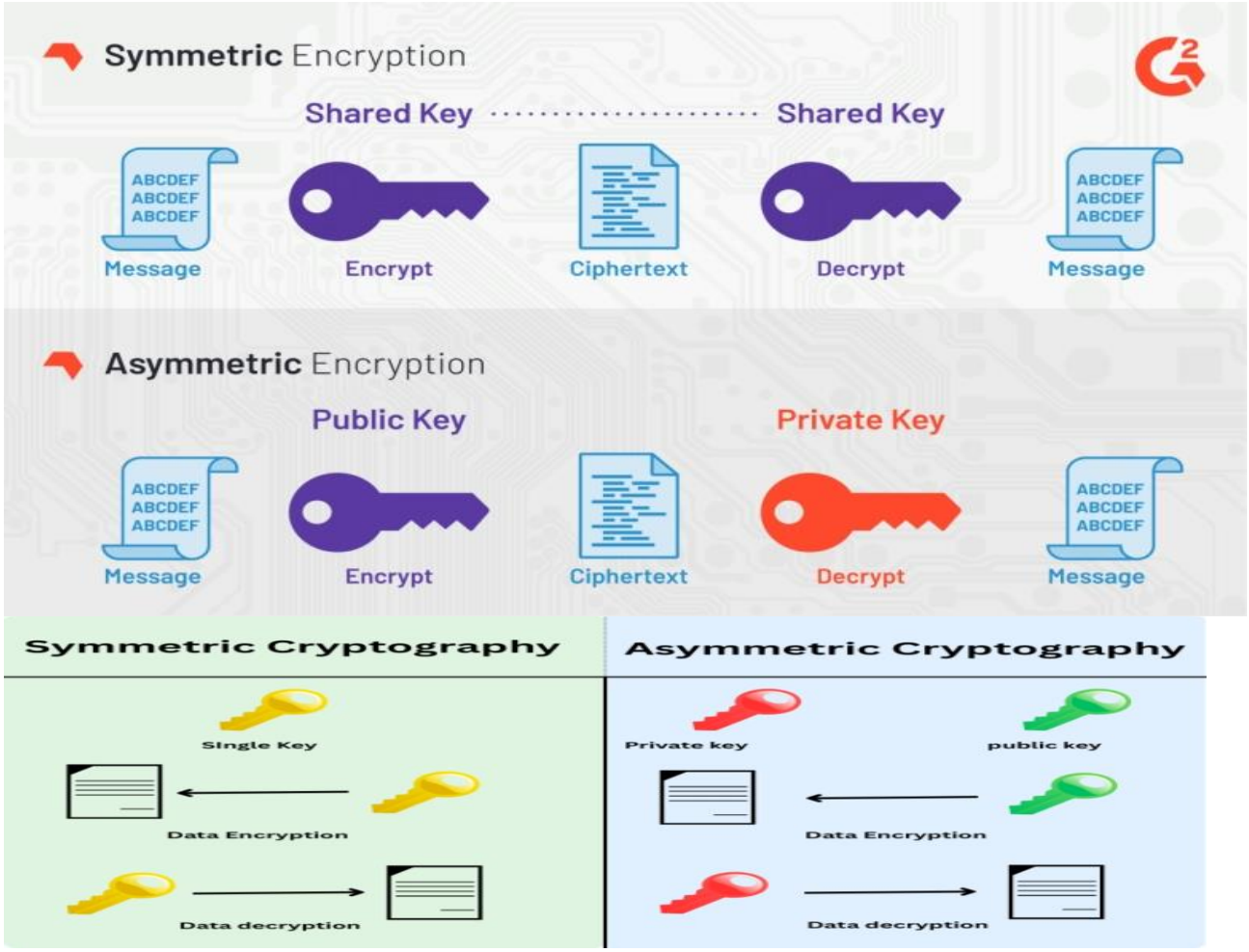
(5) Table (5) has come, and they say it is an encryption alphabet letter coding. TABLE:5 RECEIVER E M O C L E W 5 13 15 3 12 5 23

I have given the table at my place, Table 4. TABLE: 4 SENDERW E L C O M E=23 5 12 3 15 13 5. How it is given is the sender message, but for the receiver.





2456-8686, x(ii), 2026:001-015
https://doi.org/10.26524/cm237



CONCLUSION

In this novel, I will discuss how mathematics, particularly number theory, plays a crucial role in cryptography, including encryption and decryption. We will explore how messages can be secured and shared using these techniques. This novel will explain the methods used in cryptography, including how we can encrypt and decrypt messages effectively. Additionally, I will delve into how apps like What Sapp and other messaging platforms utilize these cryptographic principles to ensure that our communications remain private and secure. Through this exploration, you'll gain insights into the technicalities of cryptography and how we can apply them in everyday communications.

Reference:

1. Bonaparte, Y. (2025). Quantum Blockchain: A Theoretical Framework and Applications in Cryptocurrency. International Journal of Financial Studies, 13(4), 220.

2. Fan, Y. Y., Chew, C. J., & Lee, J. S. (2025). Asynchronous quantum-resistant blockchain for secure intelligence sharing. Applied Sciences, 15(11), 5921.

3. Habib, U., Bano, M., Iqbal, J., Hajjej, F., & Ullah, (2025). Integrating blockchain with lattice-based cryptography for privacy-preserving and quantum-secure smart grid communications. Frontiers in Physics, 13, 1727394.

4. Hajar, D., Afifi, N., & Hilal, I. (2025). Dynamic sharding and Monte Carlo for post-Quantum blockchain resilience. Cryptography, 9(2), 22.

5. Karimani, S., & Eghlidos, T. (2025). Verifiable Multi-Authority Attribute-Based Encryption with Keyword Search Based on MLWE. Cryptography, 9(4), 76.

6. Liu, Y., Wang, L., & Zhou, Y. (2025). A novel CLWE-based attribute-based encryption scheme from lattices with privacy preserving. Cybersecurity, 8(1), 76.

7. Luo, J., Zuo, L., & Liu, H. (2025). Quantum-resistant lattice-based proxy signature. Symmetry, 017(2), 261.

8. Palma, D., & Montessoro, P. L. (2025). A Post-Quantum Cryptography Enabled Feature-Level Fusion Framework for Privacy-Preserving Multimodal Biometric Recognition. Cryptography, 9(4), 72.

9. Ravisankar, S., & Maheswar, R. (2025). SecureEdge-MedChain: A Post-Quantum Blockchain and Federated Learning Framework for Real-Time Predictive Diagnostics in IoMT. Sensors, 25(19), 5988.

10. Renisha, P. S., & Rudra, B. (2025). Quantum-Safe Threshold Cryptography for Decentralized Group Key Management via Dealerless DKG (CRYSTALS–Kyber). Mathematics, 13(21), 3429.

11. Raavi, M., Khan, Q., Wuthier, S., Chandramouli, P., Balytskyi, Y., & Chang, S. Y. (2025). Security and performance analyses of post-quantum digital signature algorithms and their TLS and PKI integrations. Cryptography, 9(2), 38.

12. Taherdoost, H. (2026). A Comprehensive Review of Quantum-Resistant Architectures for Blockchain Security. Sci, 8(2), 47.

13. Yan, H., Wu, L., Sun, Q., & He, P. (2026). Lattice-Based Cryptographic Accelerators for the Post-Quantum Era: Architectures, Optimizations, and Implementation Challenges. Electronics, 15(2), 475.

14. Zhang, Z., Cao, Z., & Wang, Y. (2025). Forensics System for Internet of Vehicles Based on Post-Quantum Blockchain. Sensors, 25(19), 6038.

15. Zhang, Y., Duan, P., Li, C., Ahmad, H., & Zhang, H. (2025). Secure and Efficient Lattice-Based Ring Signcryption Scheme for BCCL. Entropy, 27(10), 1060.