Crypto Ransomware and Major Open-Source Algorithms Used

Marco Giacoppo
Dept. of Computer Science
Swinburne University of Technology
Melbourne, Australia
104071453@student.swin.edu.au

Abstract— **Crypto ransomware has emerged as one of the most significant cyber threats in recent years, with its ability to encrypt victims' data and demand payment for decryption. The success of crypto ransomware attacks largely depends on the strength of the cryptographic algorithms used to secure data. This paper explores the open-source encryption algorithms most frequently used by ransomware authors, including RSA, AES, and Elliptic Curve Cryptography (ECC). The report further analyses the potential vulnerabilities posed by quantum computing and considers future shifts toward quantum-safe encryption methods. We conclude by examining the implications for cybersecurity defences and the evolving threat landscape.**

I. INTRODUCTION

In recent years, the frequency and sophistication of ransomware attacks have increased dramatically, making it one of the most prominent threats to businesses, governments, and individuals worldwide. According to the 2023 Global Threat Report by CrowdStrike, ransomware attacks have surged by over 50% compared to the previous year, with estimated global damages exceeding $20 billion [1]. The main driver behind this success is the effective use of cryptographic algorithms to encrypt victims' data, rendering it inaccessible unless a ransom is paid, typically in cryptocurrency.

Crypto ransomware, a particularly destructive form of ransomware, uses advanced encryption techniques to lock victims' files, ensuring that decryption is virtually impossible without the correct key. In this report, we analyse the most commonly used open-source cryptographic algorithms in ransomware, including RSA, AES, and ECC, exploring how they provide both security and efficiency to ransomware authors.

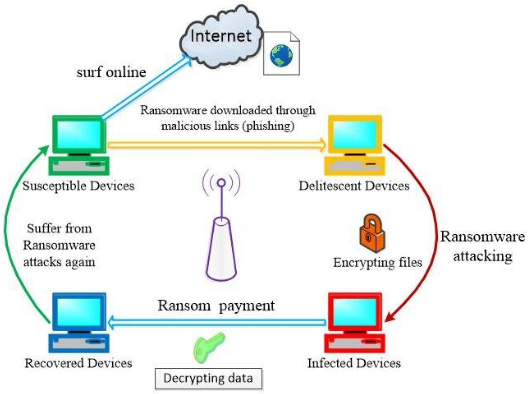


Figure 1: Ransomware attack flow diagram [10].

II. Crypto Ransomware Overview

Crypto ransomware attacks rely on encryption algorithms to deny victims access to their data. The ransomware encrypts files on the victim's system and demands payment, usually in cryptocurrency, for the decryption key. These encryption algorithms are designed to be computationally infeasible to break, giving the attacker full control over the victim's data. The evolution of crypto ransomware began with early attacks such as CryptoLocker in 2013, which set the standard for the use of *asymmetric encryption*. Over time, more sophisticated ransomware like WannaCry and Ryuk emerged, using a combination of *symmetric* and *asymmetric encryption* methods to maximize both efficiency and security [2].

In symmetric encryption, a single key is used for both encryption and decryption, whereas in asymmetric encryption, two keys (a public and private key) are used. The combination of these methods allows ransomware authors to securely encrypt large volumes of data while ensuring that the decryption key remains accessible only to them [3].

III. Major Open-Source Algorithms Used in Crypto Ransomware

A. RSA (Rivest-Shamir-Adleman)

The RSA algorithm is one of the oldest and most widely used encryption techniques in ransomware. Developed in 1977, RSA is an asymmetric encryption algorithm that uses two keys—a public key for encryption and a private key for decryption. The strength of RSA lies in the difficulty of factoring large prime numbers, a problem that is infeasible to solve with classical computers.

Ransomware like WannaCry and Ryuk have used RSA to secure decryption keys, making it impossible for victims to recover their files without access to the private key. However, RSA's reliance on the computational difficulty of factoring large integers has been challenged by the development of quantum computing. Shor's algorithm, a quantum algorithm, could potentially break RSA encryption by efficiently solving the integer factorization problem [4], [5].

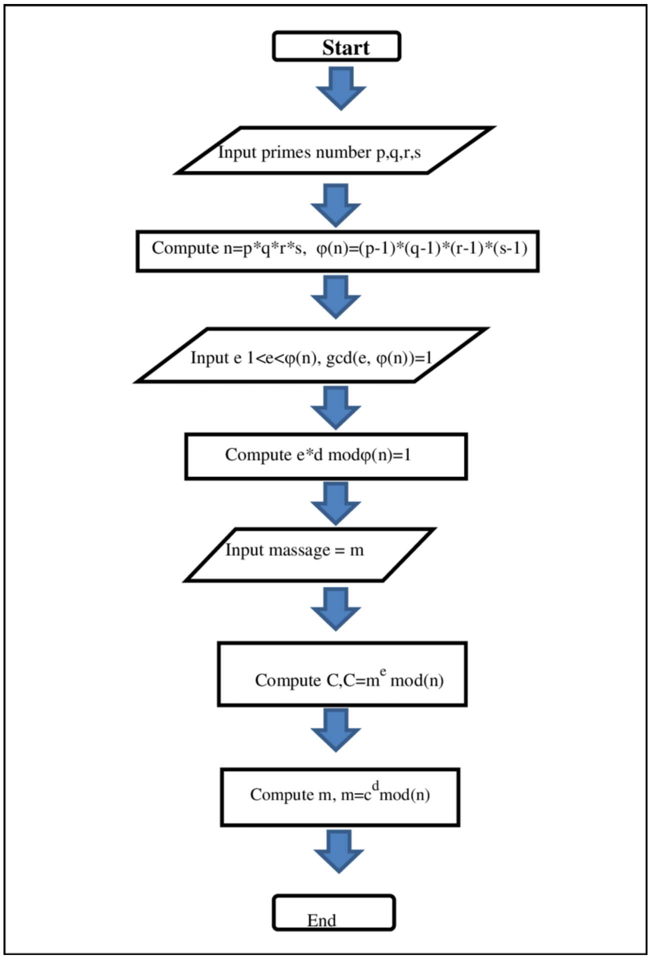

Start
Input primes number p,q,r,s
Compute n=p*q*r*s, φ(n)=(p-1)*(q-1)*(r-1)*(s-1)
Input e 1<e<φ(n), gcd(e, φ(n))=1
Compute e*d modφ(n)=1
Input massage = m
Compute C,C=m^e mod(n)
Compute m, m=c^dmod(n)
End

Figure 2: Diagram showing the RSA Encryption process in ransomware [11].

B. AES (Advanced Encryption Standard)

AES is a symmetric encryption algorithm and has been widely adopted due to its speed and security. AES operates on blocks of data and uses key sizes of 128, 192, or 256 bits. The algorithm is fast, making it suitable for encrypting large amounts of data in ransomware attacks. Many ransomware variants, including WannaCry, use AES for encrypting files, while relying on RSA for key management [6].

AES is resilient against most classical attacks, but like RSA, it is not immune to quantum attacks. Grover's algorithm, another quantum algorithm, can reduce the complexity of brute-force attacks on AES keys, effectively halving the key size. As quantum computing progresses, AES may need to adopt longer key sizes to remain secure against quantum threats [5].

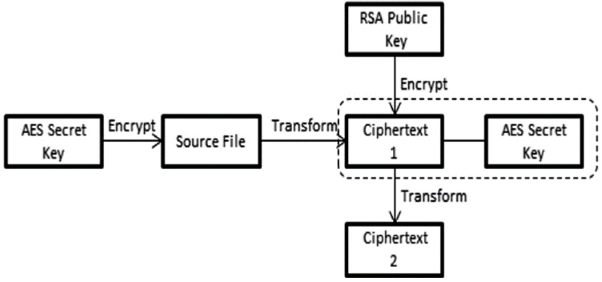


Figure 3: Workflow of AES encryption in ransomware [12].

C. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) offers similar security to RSA but with smaller key sizes, making it more efficient. ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem, which, like RSA, is computationally infeasible for classical computers. **CryptoLocker** was one of the first ransomware variants to use ECC, setting a precedent for modern ransomware encryption techniques [7], [5].

ECC's smaller key sizes make it attractive for ransomware authors who want to minimize computational overhead while maintaining high levels of security. However, like RSA, ECC is vulnerable to quantum attacks. Shor's algorithm could potentially break ECC, necessitating a shift toward quantum-safe alternatives [5].

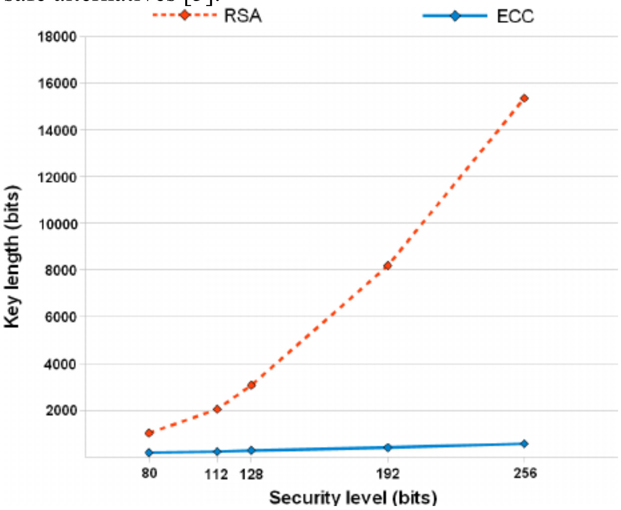


Figure 4: Comparison of key sizes between RSA and ECC in terms of performance and security.

D. ChaCha20

ChaCha20 is a stream cipher that has gained popularity due to its speed and resistance to certain types of cryptographic attacks, such as timing attacks. Ransomware authors may choose ChaCha20 for its efficiency in encrypting large volumes of data. It is particularly suitable for environments where AES might be too slow or vulnerable to side-channel attacks.

ChaCha20's design is based on a series of 20 rounds of mixing operations, making it a fast and secure alternative to AES. Although not as widely used in ransomware as RSA or AES, ChaCha20 represents a viable option for future ransomware variants looking for both speed and security.

IV. KEY CASE STUDIES

A. WannaCry

The WannaCry ransomware attack, which took place in May 2017, quickly spread worldwide by exploiting a vulnerability in the Windows SMB protocol. Affecting over 200,000 systems across 150 countries, WannaCry encrypted files on infected computers using AES-128 and then encrypted the AES key with RSA-2048. Victims were asked to pay in

Bitcoin to receive the decryption key for recovering their files [1].

The choice of AES and RSA in combination allowed WannaCry to encrypt large amounts of data efficiently while securely managing decryption keys. Despite the simplicity of its encryption scheme, WannaCry's self-propagating nature significantly increased its damage, affecting healthcare systems, businesses, and governments. However, due to a discovered "kill switch" domain, the spread of WannaCry was halted within days. Nevertheless, the attack caused over $4 billion in damages globally [2].

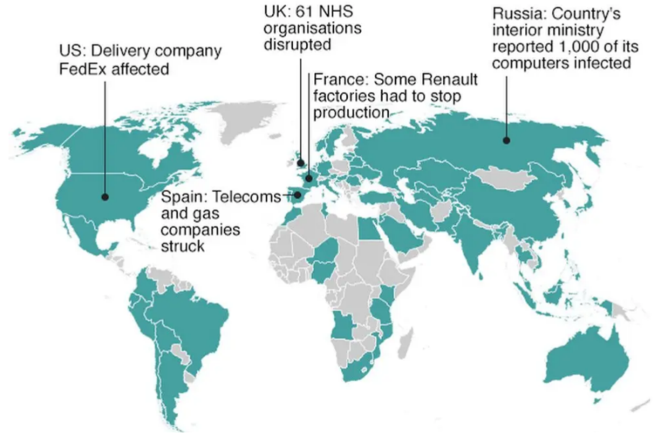

UK: 61 NHS organisations disrupted
Russia: Country's interior ministry reported 1,000 of its computers infected
US: Delivery company FedEx affected
France: Some Renault factories had to stop production
Spain: Telecoms and gas companies struck

Figure 5: Global distribution of WannaCry infections [13].

B. Ryuk

Ryuk ransomware primarily targets high-profile organizations, especially within government, healthcare, and large enterprises. Unlike WannaCry, Ryuk does not propagate itself but is often delivered via phishing emails or other malware. Once installed, Ryuk utilizes AES-256 for file encryption and RSA-2048 for key management, adding a layer of complexity that requires the AES decryption key, which is itself encrypted with RSA.

Ryuk is particularly known for its ability to disable system recovery functions, thus preventing victims from recovering data via backups. The ransomware also performs extensive reconnaissance to identify high-value files and prioritize them for encryption. This selective targeting, coupled with its strong encryption, has led to high ransom demands, with some companies paying millions to restore access to their data [3].

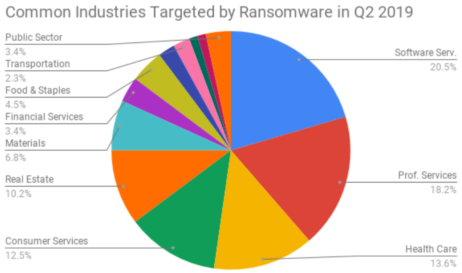


Figure 6: The impact of Ryuk across industries [14].

C. CryptoLocker

The 2013 CryptoLocker attack marked a pivotal moment in ransomware evolution as one of the first major attacks to employ Elliptic Curve Cryptography (ECC) for managing decryption keys. CryptoLocker encrypts files using AES and subsequently encrypts the AES key with ECC, ensuring that even if victims obtain the encrypted data, they cannot decrypt it without access to the private ECC key.

CryptoLocker's success inspired numerous other ransomware variants, and its use of ECC provided a balance between security and computational efficiency. By the time authorities disrupted the CryptoLocker network, the ransomware had extorted millions from victims worldwide, and its methodology remains influential in modern ransomware design [4].

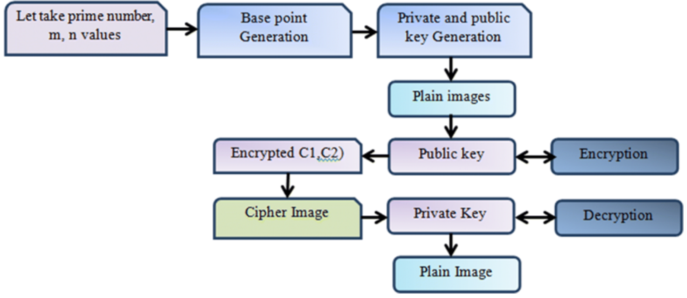


Figure 7: CryptoLocker's encryption flow [15].

V. The Impact of Quantum Computing on Ransomware Encryption

As quantum computing develops, its impact on cryptographic security is expected to be profound. Quantum computers leverage quantum-mechanical phenomena to solve complex problems exponentially faster than classical computers. This poses a significant threat to classical cryptographic algorithms, which rely on problems that are computationally infeasible for classical computers to solve. Quantum algorithms like Shor's algorithm and Grover's algorithm specifically threaten RSA, ECC, and AES, the very algorithms used in ransomware today [5].

A. Vulnerabilities of RSA and ECC

RSA and ECC rely on the difficulty of factoring large prime numbers and solving discrete logarithmic problems, respectively. Shor's algorithm enables a quantum computer to factorize large integers efficiently, effectively breaking RSA encryption. Similarly, ECC's reliance on elliptic curve discrete logarithm problems makes it vulnerable to quantum attacks. Given that RSA and ECC are foundational to many encryption protocols, including those in ransomware, their vulnerabilities pose a major risk to current cryptographic practices [6].

Quantum computing also threatens AES. While Grover's algorithm does not outright break AES, it effectively reduces the algorithm's key strength by half, meaning that an AES-256 key would offer equivalent security to an AES-128 key in a quantum context. As a result, even symmetric encryption techniques may need to adopt longer key sizes or alternative algorithms to remain secure against quantum computing threats.

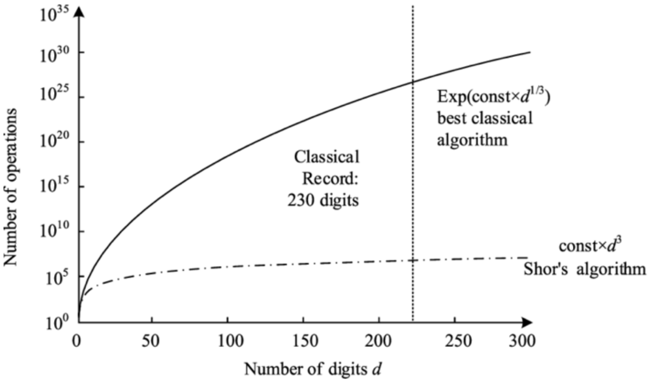


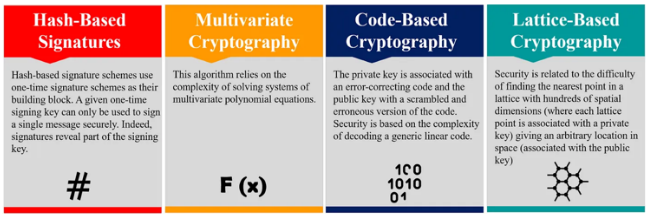
Figure 8: Shor's algorithm's impact on RSA and ECC [16].

B. Transition to Quantum-Safe Algorithms

In response to the potential impact of quantum computing, researchers are developing quantum-safe algorithms that are resistant to quantum attacks. Some of the most promising options include:

1. Lattice-based Cryptography: Lattice-based methods, such as the Learning With Errors (LWE) problem, offer security based on the difficulty of finding specific vectors within a lattice structure. These methods are highly resistant to both classical and quantum attacks and are currently leading candidates for post-quantum cryptography [7].
2. Hash-based Cryptography: Using Merkle trees, hash-based cryptography creates secure digital signatures that are resistant to quantum computing. Although limited in certain applications, hash-based methods are being explored for high-security environments like blockchain technology [8].
3. Code-based Cryptography: The McEliece cryptosystem is one of the oldest code-based systems and is known for its resilience against quantum attacks. Code-based cryptography relies on the complexity of decoding linear codes, making it a strong candidate for quantum-resistant encryption [9].

As quantum computing technology advances, ransomware authors may adopt these quantum-safe methods to future-proof their attacks. This would pose new challenges for cybersecurity, as quantum-safe algorithms generally require greater computational resources and larger key sizes.



Hash-Based Signatures

Hash-based signature schemes use one-time signature schemes as their building block. A given one-time signing key can only be used to sign a single message securely. Indeed, signatures reveal part of the signing key.

Multivariate Cryptography

This algorithm relies on the complexity of solving systems of multivariate polynomial equations.

Code-Based Cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the complexity of decoding a generic linear code.

Lattice-Based Cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where each lattice point is associated with a private key) giving an arbitrary location in space (associated with the public key)

Figure 9: Comparative security of quantum-safe algorithms [17].

VI. Analysis of Open-Source Algorithm Effectiveness

The cryptographic algorithms used in ransomware are effective in today’s cybersecurity landscape but face significant challenges with the advent of quantum computing. RSA and ECC provide robust protection, but they are increasingly vulnerable in a quantum-enabled future. Symmetric encryption algorithms like AES are somewhat more resistant, but they may still require adjustments, such as increased key sizes, to withstand quantum attacks effectively.

Quantum-safe algorithms represent promising alternatives, but their adoption in ransomware and other applications faces practical challenges. Many quantum-safe algorithms require larger key sizes, which can slow down encryption and decryption processes. In addition, implementing these algorithms in existing systems may require significant infrastructure changes.

The transition to quantum-safe algorithms in ransomware may depend on advances in hardware and software optimization, allowing for more efficient processing of these computationally intensive encryption methods. Thus, while quantum-safe cryptography offers future resilience, it will likely come with trade-offs that ransomware authors and defenders must navigate carefully.

VII. Conclusion

Crypto ransomware remains one of the most impactful forms of cybercrime, leveraging powerful cryptographic algorithms like RSA, AES, and ECC to deny victims access to their data. However, the rise of quantum computing poses an existential threat to these encryption techniques, with algorithms like Shor’s and Grover’s promising to break or weaken RSA, ECC, and AES in a quantum context. As a result, the future of ransomware encryption may lie in quantum-safe algorithms, such as lattice-based, hash-based, and code-based cryptography.

Understanding these algorithms and preparing for their adoption is essential for both cybersecurity professionals and ransomware authors. As quantum computing advances, organizations must proactively adopt quantum-safe defences to counter future ransomware attacks effectively. In this evolving landscape, staying ahead of cryptographic advancements will be crucial to ensuring the security and resilience of digital systems.

References

[1] CrowdStrike, "2023 Global Threat Report," CrowdStrike, 2023. [Online]. Available: https://www.crowdstrike.com/resources/reports/global-threat-report/.

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134, doi: https://doi.org/10.1109/sfcs.1994.365700.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219, doi: https://doi.org/10.1145/237814.237866.

[4] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sep. 2018, doi: https://doi.org/10.1109/msp.2018.3761723.

[5] M. Giacoppo, "The Threat of Quantum Computing to Cryptographic Security and the Development of Quantum-Safe Algorithms," Swinburne University of Technology, 2023.

[6] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: https://doi.org/10.1038/nature23461.

[7] C. Peikert, "A Decade of Lattice Cryptography," *Foundations and Trends® in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016, doi: https://doi.org/10.1561/0400000074.

[8] NIST, "Post-Quantum Cryptography Standardization Project," NIST, 2023. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[9] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Laboratory DSN Progress Report, vol. 42-44, pp. 114-116, 1978.

[10] W. Liu, "Modeling Ransomware Spreading by a Dynamic Node-Level Method," *IEEE Access*, vol. 7, pp. 142224–142232, 2019, doi: https://doi.org/10.1109/access.2019.2941021

[11] B. Musa, Mr Pankaj Chajera, and A. B. Garko, "ADVANCED SECURE METHOD FOR DATA TRANSMISSION IN MANET USING RSA ALGORITHM," vol. 3, no. 1, pp. 176–185, Sep. 2015, Available: https://www.researchgate.net/publication/306018436_ADVANCED_SECURE_METHOD_FOR_DATA_TRANSMISSION_IN_MANET_USING_RSA_ALGORITHM. [Accessed: Oct. 26, 2024]

[12] Sk. Al Mamun, Md. Ashiq Mahmood, and A. Amin, "Ensuring Security of Encrypted Information by Hybrid AES and RSA Algorithm with Third-Party Confirmation," May 2021, doi: https://doi.org/10.1109/iciccs51141.2021.9432174

[13] BBC News, "Ransomware cyber-attack: Who has been hardest hit?," *BBC News*, May 15, 2017. Available: https://www.bbc.com/news/world-39919249

[14] "Ransomware Amounts Rise Threefold," *Coveware: Ransomware Recovery First Responders*. Available: https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

[15] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Computing and Applications*, Oct. 2018, doi: https://doi.org/10.1007/s00521-018-3801-x. Available: https://link.springer.com/article/10.1007%2Fs00521-018-3801-x

[16] Y. Dong *et al.*, "Improving the Success Rate of Quantum Algorithm Attacking RSA Encryption System," *Research Square (Research Square)*, Mar. 2022, doi: https://doi.org/10.21203/rs.3.rs-1501203/v1. Available: https://www.researchgate.net/publication/359643607_Improving_the_Success_Rate_of_Quantum_Algorithm_Attacking_RSA_Encryption_System. [Accessed: Oct. 26, 2024]

[17] VIT, "Post-Quantum Cryptography: Securing Data in the Quantum Era," *Medium*, Jul. 27, 2024. Available: https://medium.com/@IEEE_Computer_Society_VIT/post-quantum-cryptography-securing-data-in-the-quantum-era-0c389a597183. [Accessed: Oct. 26, 2024]