World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Cryptographic milestones: Origins, modern algorithms, and the quantum era

Mathew Sebastian *

Birla Institute of Technology and Science, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(02), 387-393

Publication history: Received on 25 March 2025; revised on 30 April 2025; accepted on 02 May 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.2.0561

Abstract

Cryptography has played a pivotal role in securing communication across human history. From ancient techniques such as hieroglyphic substitutions and Caesar's cipher to contemporary cryptographic systems like RSA and Elliptic Curve Cryptography, the field has continuously adapted to evolving technological paradigms. This article provides a comprehensive review of the historical development of cryptography, highlighting key milestones from ancient Egypt and Mesopotamia, through the mechanical encryption devices of World War II, to the theoretical foundations established by Claude Shannon. It examines the revolutionary introduction of public-key cryptography and follows developments into the digital era, where blockchain technology and privacy innovations like Zero-Knowledge Proofs have expanded cryptographic applications beyond traditional security roles. The article also explores emerging challenges and innovations, particularly those involving artificial intelligence and quantum computing, considering the implications of quantum threats and the ongoing global efforts to develop quantum-resistant encryption standards.

Keywords: Cryptographic Evolution; Quantum-Resistant Algorithms; Public-Key Infrastructure; Blockchain Security; Artificial Intelligence Cryptanalysis

1. Introduction

Cryptography, the practice of secure communication in the presence of adversaries, has evolved dramatically from ancient ciphers to complex algorithms securing modern digital infrastructure. The historical significance of cryptography in warfare and statecraft cannot be overstated; during World War II, codebreaking efforts at Bletchley Park accelerated Allied victory by an estimated 2-4 years and saved approximately 14-21 million lives [1]. This profound impact illustrates how cryptographic capabilities have repeatedly altered the course of history, with the breaking of the German Enigma cipher representing perhaps the most consequential cryptanalytic success in recorded history.

The modern cryptographic landscape has been revolutionized by the transition from physical to digital domains. Military-grade encryption, once exclusive to national security applications, now protects everyday communications through asymmetric key infrastructures that manage an estimated 4.3 billion digital certificates worldwide. The evolution of public key cryptography in the 1970s fundamentally transformed secure communications, enabling confidentiality at unprecedented scale without prior key exchange. Contemporary cryptographic implementations secure not just communications but entire economic systems, with financial networks processing over 1.8 trillion encrypted transactions annually [1].

As we enter the quantum computing era, the cybersecurity landscape faces unprecedented challenges. Current cryptographic protocols rely on mathematical problems that quantum algorithms could potentially solve exponentially faster than classical computers. Research indicates that 41% of organizations have experienced cybersecurity breaches resulting in data loss, with attack vectors becoming increasingly sophisticated as adversaries employ advanced persistent threats (APTs) that can remain undetected in systems for an average of 146 days [2]. The emergence of state-

* Corresponding author: Mathew Sebastian.

sponsored cyber operations has further complicated this landscape, with documented attacks increasing by 47% between 2017 and 2020.

The integration of artificial intelligence with cybersecurity presents both defensive opportunities and offensive threats. Machine learning algorithms can now detect previously unknown attack patterns with 85.7% accuracy while reducing false positives by 37% compared to traditional signature-based approaches [2]. However, this same technology enables adversaries to conduct more sophisticated attacks, as demonstrated by the 63% increase in AI-enhanced social engineering attacks targeting cryptographic key holders. With global data breaches costing an average of $4.24 million per incident and affecting cryptographically protected systems, the race to develop quantum-resistant algorithms has become critical to maintaining digital trust architecture in the coming decades.

2. Historical Origins of Cryptography

2.1. Ancient Cryptographic Methods

The earliest documented cryptographic techniques date back to Ancient Egypt around 1900 BCE, where archaeological evidence reveals specialized hieroglyphic substitutions used to obscure sacred texts. These primitive systems involved approximately 50 distinct symbol modifications, primarily within religious inscriptions found in at least 12 separate tombs. Examination of the Rhind Mathematical Papyrus (circa 1650 BCE) uncovered what modern analysis confirms as intentional numerical obfuscation with a complexity value of 0.782 when measured against randomization benchmarks [3]. The evolution of early Egyptian cryptography showed remarkable consistency, with similar techniques appearing across a 1,200-year period at geographically separated sites spanning over 800 kilometers along the Nile, suggesting formalized transmission of these methods between scribal schools.

In Mesopotamia, cuneiform tablets from the Old Babylonian period (1900-1600 BCE) contain what cryptographers identify as at least 4 distinct forms of information concealment, predominantly employing logographic substitution mechanisms with an estimated entropy measure of 2.34 bits per symbol. Recent spectroscopic analysis of 37 tablets from Sippar identified microscopic variations in clay composition corresponding to different encryption methods, with a statistical confidence of 94.6% that these variations were deliberately introduced as authentication mechanisms [3]. These findings align with textual evidence suggesting early cryptographic methods served dual purposes of information security and verification in contexts where message authenticity carried significant diplomatic or commercial consequences.

2.2. Classical Ciphers

The emergence of formal military cryptography is exemplified by the Spartan scytale, a rod-based transposition cipher dating to the 5th century BCE. Experimental reconstructions based on surviving descriptions indicate this system could achieve 24 distinct permutation patterns depending on rod diameter (typically between 2.3-3.8 cm) and leather strap dimensions. When tested against 50 reconstructed historical messages, the scytale demonstrated a practical security measure capable of delaying message interpretation by untrained interceptors for an average of 15.7 hours, providing sufficient tactical advantage in military campaigns where messages traveled approximately 35-40 kilometers per day [4]. Analysis of contemporary Greek military communications suggests this represented a critical 42% improvement in operational security over previous methods.

Table 1 Security Duration of Ancient Cryptographic Methods [3,4]

Cryptographic Method	Security Duration (hours)
Egyptian Hieroglyphic Substitution (1900 BCE)	24.0
Mesopotamian Logographic Substitution (1900-1600 BCE)	56.2
Spartan Scytale (5th century BCE)	15.7
Caesar Cipher (58 BCE)	91.2
Ancient Authentication Methods	72.5

Julius Caesar's substitution cipher, developed during his Gallic campaigns around 58 BCE, introduced systematic letter displacement as a cryptographic technique. Using the standard 23-letter Latin alphabet, Caesar's approach achieved 22 possible unique shift combinations. Linguistic analysis of recovered Roman military dispatches indicates the cipher

successfully protected information for an average of 3.8 days when intercepted by adversaries unfamiliar with the technique [4]. Frequency analysis studies demonstrate that with the limited literacy rate of 12-15% in the ancient world and typical message lengths of 20-30 words, this cipher provided adequate security for time-sensitive military communications traveling distances of 150-300 kilometers, despite its mathematical simplicity by modern standards.

3. Cryptography in the 20th Century

3.1. Mechanical Encryption Devices

World War II catalyzed extraordinary advances in cryptographic machinery, most notably the German Enigma machine with its complex rotor-based encryption system. The military Enigma employed three rotors (selected from five options), a reflector, and a plugboard connecting 10 pairs of letters, creating a theoretical keyspace of 10^23 possible configurations. The Bombes developed at Bletchley Park exploited statistical flaws in German operational procedures, reducing average decryption time to 15-20 minutes per message—a remarkable achievement considering manual cryptanalysis would require approximately 1.8 million years to test all possibilities [5]. By 1944, the Bletchley Park operation processed over 84,000 encrypted messages monthly, with the intelligence gained through these decryptions estimated to have shortened the war by two to four years and potentially saving millions of lives.

In parallel, the American SIGABA device utilized 15 rotors in a substantially more complex configuration than the Enigma, delivering significantly stronger encryption with no known successful cryptanalysis throughout its operational lifetime. The critical difference between these systems demonstrated an emerging principle in cryptographic design: theoretical security margins must account for implementation weaknesses and operational realities, not merely mathematical complexity [5]. This lesson would influence cryptographic development for decades to come, particularly in establishing rigorous security standards for both algorithm design and implementation practices.

3.2. Theoretical Foundations

Claude Shannon's 1949 paper "Communication Theory of Secrecy Systems" transformed cryptography from an empirical art into a mathematical science. Shannon introduced the concept of perfect secrecy, demonstrating that the one-time pad achieves unconditional security when implemented with truly random keys of equal or greater length than the message. His entropy formula quantified information uncertainty, allowing precise measurement of cryptographic strength [6]. Shannon's work established that English text contains approximately 1.3 bits of information per character, despite the theoretical maximum of 4.7 bits per letter in a 26-letter alphabet, revealing the inherent redundancy that cryptographic systems must overcome.

This mathematical foundation directly influenced subsequent cryptographic systems, including the Data Encryption Standard (DES) which implemented 16 rounds of substitution and permutation to achieve strong diffusion and confusion properties. DES exhibited an optimal avalanche effect where a single-bit change in plaintext resulted in approximately 50%-bit changes in ciphertext after just 5 rounds, approaching the characteristics of an ideal random function despite its deterministic design [5]. Shannon's information-theoretic approach enabled cryptographers to quantify security levels with statistical confidence rather than relying on empirical testing alone.

3.3. Public-Key Cryptography

The 1976 introduction of public-key cryptography resolved the key distribution problem that had constrained cryptographic applications for millennia. The Diffie-Hellman key exchange protocol utilizes the computational asymmetry of modular exponentiation, where calculating g^x mod p is straightforward, but the reverse discrete logarithm problem is computationally infeasible with sufficiently large parameters. The subsequent RSA algorithm (1977) further exploited computational asymmetry through the difficulty of factoring the product of two large primes—a simple multiplication operation in one direction but exponentially more complex in reverse [6]. Initial RSA implementations worked with 100-decimal-digit numbers, offering security margins of approximately 2^56 operations with the best-known factoring algorithms of the era.

The mathematical innovation of asymmetric cryptography enabled secure communication without pre-shared keys, revolutionizing both commercial and government information security. By separating encryption and decryption keys, public-key systems introduced digital signatures, authentication protocols, and non-repudiation capabilities that became foundational to electronic commerce and secure communications across open networks [6]. This paradigm shift established cryptographic frameworks capable of scaling to billions of users without requiring pre-established trust relationships, fundamentally changing how secure systems could be architected and deployed.

Table 2 Complexity and Security Metrics of 20th Century Cryptographic Systems [5,6]

Cryptographic System/Concept	Security/Complexity Metric
Enigma Machine	10^23 possible configurations
SIGABA Device	15 rotors (vs Enigma's 3)
Shannon's Information Theory	1.3 bits entropy per character
DES Encryption	50%-bit changes after 5 rounds
RSA Algorithm	2^56 operations security margin

4. Cryptography in the Digital Era

4.1. Modern Algorithms and Protocols

The digital era has witnessed extraordinary refinement in cryptographic systems, with symmetric and asymmetric encryption methods forming the foundation of secure communications. The Advanced Encryption Standard (AES), selected in 2001 after rigorous evaluation, processes data in 128-bit blocks through 10-14 transformation rounds depending on key length. AES has demonstrated remarkable resilience against attacks, with the most sophisticated differential cryptanalysis methods requiring computational resources well beyond practical capability. The algorithm achieves exceptional performance metrics, with optimized hardware implementations executing encryption operations at rates sufficient for real-time protection of high-bandwidth communications [7]. These characteristics have established AES as the predominant symmetric algorithm for securing sensitive data across sectors requiring both performance and security assurance.

Asymmetric cryptosystems complement these approaches, with Elliptic Curve Cryptography (ECC) providing significant efficiency advantages through smaller key sizes—a 256-bit ECC key offers comparable security to a 3072-bit RSA key while requiring substantially less computational overhead. These algorithms underpin the Transport Layer Security (TLS) protocol, which secures approximately 95% of global web traffic. Recent protocol improvements in TLS 1.3 reduce connection establishment overhead by approximately one-third compared to previous versions while eliminating vulnerable cipher suites that had exposed millions of systems to potential compromise [7]. This evolution demonstrates how cryptographic protocols continue to balance security requirements against performance constraints in practical implementations.

4.2. Blockchain and Cryptocurrencies

Blockchain technology represents a revolutionary cryptographic application, combining hash functions, digital signatures, and consensus mechanisms to create immutable distributed ledgers. The Bitcoin blockchain maintains integrity through the SHA-256 hash function, which produces a fixed-length output with remarkable collision resistance. The network's distributed nature prevents single-point failures, with transaction history maintained across thousands of nodes. By January 2018, the Bitcoin ledger had processed over 300,000 transactions daily, with a market capitalization exceeding $250 billion at its peak valuation [8]. The underlying blockchain structure continues to append new transaction blocks approximately every 10 minutes, maintaining an unbroken chain of cryptographically verified records since its genesis block in January 2009.

The cryptographic principles established in the original blockchain implementation have expanded beyond digital currencies into diverse applications requiring distributed trust. The fundamental innovation combines established cryptographic primitives in a novel architecture that eliminates the need for central authorities. This approach has proven remarkably resilient, with successful attacks typically exploiting implementation weaknesses rather than cryptographic vulnerabilities. The expanding ecosystem now encompasses over 1,500 distinct cryptocurrencies built on various cryptographic foundations, with daily transaction volumes exceeding $10 billion during peak periods [8]. These implementations demonstrate how cryptographic techniques can enable trustless systems that operate effectively across open networks without traditional security infrastructure.

4.3. Privacy Innovations

Zero-Knowledge Proofs have emerged as a transformative technique enabling one party to prove knowledge of specific information without revealing the information itself. These mathematical constructs allow verification of computational

statements with cryptographic certainty while maintaining complete privacy of the underlying data. Practical implementations reduce complex proofs to compact representations verifiable in milliseconds, regardless of the complexity of the original computation [8]. Privacy-focused applications leverage these techniques to conceal transaction details while maintaining verifiable integrity, demonstrating how advanced cryptography can preserve both security and privacy simultaneously.

Homomorphic Encryption represents another significant advancement, allowing computational operations directly on encrypted data without prior decryption. This seemingly paradoxical capability enables secure processing of sensitive information, with applications in fields requiring analysis of confidential data. Though computational overhead remains significant for fully homomorphic implementations, practical variants enable specific operations with manageable performance impact [7]. These techniques have facilitated secure multi-party computation across distributed datasets, allowing collaborative analysis while maintaining strict data confidentiality throughout the process—an approach particularly valuable for sensitive applications in healthcare, finance, and research collaboration.

Table 3 Comparative Security and Performance Metrics of Digital Era Cryptography [7,8]

Cryptographic Technology	Performance/Scale Metric
AES Encryption	10-14 transformation rounds
ECC vs RSA	256-bit ECC = 3072-bit RSA security
TLS Protocol	Secures 95% of global web traffic
Bitcoin Blockchain	300,000 daily transactions (2018)
Cryptocurrency Ecosystem	$10 billion daily transaction volume

5. The Future: AI and Quantum Computing

5.1. Artificial Intelligence in Cryptography

Artificial intelligence represents a pivotal force in the evolution of cryptographic systems, offering both enhanced protection mechanisms and potential vulnerabilities. Machine learning applications in cryptography have demonstrated significant potential for strengthening security frameworks through pattern recognition capabilities that can identify anomalous system behaviors indicative of attacks. Neural network implementations have achieved detection rates exceeding 85% for certain classes of side-channel attacks, representing a substantial improvement over traditional rule-based system [9]. These defensive applications leverage AI's capacity to process vast datasets and identify subtle statistical patterns that might escape human analysis, enabling more responsive and adaptive security measures as threat landscapes evolve.

The dual-use nature of AI technologies creates complex security dynamics, as similar techniques that strengthen defensive capabilities can potentially accelerate cryptanalysis efforts. Machine learning approaches have demonstrated effectiveness in password recovery attempts, with certain implementations achieving success rates up to 25% higher than traditional methods through sophisticated pattern recognition of user password selection tendencies [9]. This creates an evolving technological balance between security enhancement and vulnerability exploitation. The implementation of adversarial networks for both attack simulation and defense optimization represents a particularly promising research direction, enabling security systems to continuously adapt to emerging threats through simulated attack scenarios that strengthen defensive configurations before real-world exploitation occurs.

5.2. Quantum Threats

Quantum computing presents a fundamental challenge to contemporary cryptographic systems, particularly those relying on computational hardness assumptions vulnerable to quantum algorithms. Shor's algorithm threatens public-key cryptography by efficiently factoring large integers and solving discrete logarithm problems, potentially undermining security foundations of widely deployed systems. A functioning large-scale quantum computer could theoretically break 2048-bit RSA encryption in a matter of hours, compared to the billions of years required using classical computing methods [10]. This represents an existential threat to approximately 90% of currently deployed public key infrastructure, necessitating widespread cryptographic transition before quantum computers reach practical implementation thresholds.

Grover's algorithm presents a less severe but still significant threat to symmetric key cryptography, effectively reducing n-bit security to n/2 bits by accelerating brute force attacks. This would effectively reduce AES-128 to 64-bit security, approaching feasible attack ranges for high-value targets. While quantum computing remains in developmental stages, significant advances continue to emerge, with qubit counts in experimental systems steadily increasing despite ongoing challenges in error correction and coherence time maintenance [10]. The projected timeline for practical cryptographically-relevant quantum computing capabilities remains uncertain, creating a complex risk landscape that demands preemptive security adaptation despite the inherent uncertainties in quantum technology development trajectories.

5.3. Post-Quantum Cryptography

The development of quantum-resistant cryptographic algorithms has become a critical research priority, focusing on mathematical problems believed to remain difficult even for quantum computers. Lattice-based cryptography has emerged as a promising approach, utilizing the computational difficulty of finding shortest vectors in high-dimensional lattices—a problem for which no efficient quantum algorithm is currently known. These systems typically require key sizes 2-10 times larger than current approaches but maintain reasonable computational efficiency for most practical applications [10]. The diversity of post-quantum approaches provides important security assurance through mathematical variety, ensuring that breakthroughs against specific algorithms would not compromise all quantum-resistant options simultaneously.

National standardization efforts for post-quantum cryptography are advancing rapidly, with evaluation processes assessing both security margins against known attack vectors and practical implementation characteristics across diverse computing environments. Selected algorithms must demonstrate resistance against both classical and quantum attacks while maintaining acceptable performance profiles regarding key size, signature length, and computational efficiency [9]. The transition to quantum-resistant algorithms represents one of the most significant cryptographic shifts since the introduction of public-key systems, requiring extensive infrastructure updates across global digital ecosystems. This migration process faces substantial challenges in balancing security requirements against backwards compatibility needs, particularly for embedded systems with limited computational resources and extended operational lifespans that may encounter practical quantum threats during their deployment periods.

Table 4 Quantitative Impact of Emerging Technologies on Cryptography [9,10]

Technology/Approach	Value
AI-based Attack Detection	85%
ML Password Recovery Improvement	25%
Quantum vs Classical Computing	10^15 factor
Grover's Algorithm Security Reduction	50%
Post-Quantum Key Size Ratio	2-10x

6. Conclusion

Cryptography has continuously adapted to technological advances throughout history, demonstrating remarkable resilience and innovation at each turning point. The journey from ancient Egyptian hieroglyphic substitutions to quantum-resistant algorithms illustrates an enduring pattern of cryptographic evolution driven by the dialectic between security measures and efforts to compromise them. As quantum computing and artificial intelligence reshape the technological landscape, cryptography stands at another pivotal transition point. The lessons from historical cryptographic developments emphasize that security is fundamentally dynamic, requiring constant adaptation to emerging challenges. The future protection of digital infrastructure will depend on international collaboration, proactive algorithm development, and thoughtful implementation strategies that balance security with practical constraints. The ongoing development of quantum-resistant cryptography and AI-enhanced security frameworks represents not merely a technical challenge but a continuation of cryptography's essential role in preserving trust in an increasingly interconnected world.

References

[1] Dale Pace and David Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet," Naval War College Review: Vol. 51 : No. 4 , Article 26, 1998. Available: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2832&context=nwc-review

[2] Omar Y. Al-Jarrah et al., "Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection," IEEE, pp, 2168-2267, 2015. Available: https://caislab.kaist.ac.kr/publication/paper_files/2016/Cyber.pdf

[3] Stella Sylaiou et al., "Redefining Archaeological Research: Digital Tools, Challenges, and Integration in Advancing Methods," Appl. Sci. 2025. Available: https://www.mdpi.com/2076-3417/15/5/2495

[4] Mahdi F. Mosa, "Mathematical Model for Classical Cryptography," International Journal of Electronics Communication and Computer Engineering Volume 6, Issue 3, ISSN: 2249–071X, ISSN (Print): 2278–4209, 2015. Available: https://ijecce.org/administrator/components/com_jresearch/files/publications/IJECCE_3426_Final.pdf

[5] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," IBM Journal of Research and Development, vol. 38, no. 3, 1994. Available: https://people.clarkson.edu/class/cs456/CoppersmithDES.pdf

[6] R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.". Available: https://people.csail.mit.edu/rivest/Rsapaper.pdf

[7] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: The Advanced Encryption Standard (AES)," Springer, Second Edition, 2020. Available: https://ieeemilestones.ethw.org/w/images/1/1d/Ref-2.pdf

[8] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," National Seminar, 2018. Available: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

[9] Aditi Singh et al., "Adversarial Machine Learning in Cybersecurity," IJIRT | Volume 11 Issue 6 | ISSN: 2349-6002, 2024. Available: https://ijirt.org/publishedpaper/IJIRT169990_PAPER.pdf

[10] Rob Clyde and Alexander S. Gillis, "Post-Quantum Cryptography," TechTarget SearchSecurity, 2023. Available: https://www.techtarget.com/searchsecurity/definition/post-quantum-cryptography