International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Math Mysteries: The Detective Work of Cryptography: A Literature Review on Mathematical Foundations and Forensic Applications

Ishita Swain

One World International School, Bengaluru, India
Email: *ishita.swain2413[at]gmail.com*

Abstract: ***This literature review examines the mathematical foundations of modern cryptography and their role in digital forensic investigations. The study focuses on four core techniques: modular arithmetic, prime factorization, the Euclidean algorithm, and RSA encryption. Sources were systematically selected from academic databases and educational platforms based on relevance and accessibility to an introductory audience. The analysis shows that these mathematical principles underpin both secure communication systems and challenges faced by investigators in accessing encrypted data. Case studies, including the FBI- Apple dispute, WannaCry ransomware, and blockchain forensics, demonstrate the dual role of cryptography in protecting users and enabling criminal concealment. The findings highlight the need for further research in post-quantum cryptography, legal frameworks for encrypted data access, and educational approaches that connect theory with real-world applications.***

Keywords: Cryptography, RSA Encryption, Modular Arithmetic, Digital Forensics, Blockchain, Public-key cryptography, Euclidean algorithm, Ransomware analysis

1. Introduction

Today almost everything that we do happens online. People send messages, make transactions, store medical records and even run entire businesses through the internet. The majority of the population often assume it's all safe, the information and every other piece of data they share, but how is this security achieved? The answer to this is cryptography. Cryptography is the practice of securing information by transforming it into something that only authorized people have access to. According to Khan Academy, the way modern cryptography is built is built entirely on mathematics, specifically number theories and algebra [1]. Without math in the picture, there would be no secure internet, encrypted phones and no way for investigators to protect any digital evidence.

This paper is a literature review that answers the following central question: "What are the main mathematical techniques which are used in cryptography and how do they help investigators keep communication secure?" This question is more relevant now than ever. With the rise in cybercrime, criminals using encryption codes to hide their activities and worldwide law enforcement struggling to keep up, the courts have certainly debated whether manufacturers can be compelled to unlock protected devices [2, 3]. To understand this, it's important to first understand the math.

2. Literature Survey

2.1 Foundations of Cryptography

Although it may seem nothing like what it is now, cryptography has existed for a long period of time, used by Julius Caesar over 2,000 years ago [4, 5]. The Caesar cipher is one of the simplest yet widely used encryption techniques in which each letter in plaintext is replaced with another letter based on a pattern or differing by some fixed number of positions. In summary, it shifts every letter by the same number. For example, if you shift 4, A becomes E, B becomes F and so on. In mathematical terms, by using modular arithmetic this can also be described as a transformation of letters into numbers where any letter 'x' is shifted by a fixed 'n', given as $En(x) = (x+n) \bmod 26$ [5]. Due to the fact that there are only 26 shifts possible, a code-breaker in modern times could try all possible combinations in minutes, if not seconds using frequency analysis, making the Caesar cipher computationally trivial to break.

To fix this problem, the cryptographers created a different system, called the Vigenère cipher where each letter of the plaintext is encoded with a different Caesar cipher, whose increment is determined by corresponding letters of a keyword [6]. For example, using a keyword like "SUN" means that the message is shifted by a different amount, where the first letter shifts by 18 (S), next by 20 (U) and then by 13 (N) and then the pattern repeats. This cipher was significantly harder to break than the Caesar cipher, and for about 300 years it was believed to be uncrackable.

But even the Vigenère cipher was cracked and a mathematician named Charles Babbage figured out that repeating certain keywords created a pattern in the ciphertext where the key length could be figured out, and this was called the Kasiski examination [6]. Once the key was known, using frequency analysis, each section could be broken. Even then, the real turning point in this whole journey was in the 1970s when Whitfield Diffie and Martin Hellman introduced a term coined public-key cryptography [7], which was an asymmetric system that used not one, but 2 keys, one which was public and the other private, unlike the traditional

symmetric systems where the same key was used to encrypt and decrypt. This concept meant that 2 individuals could now communicate in a secure line without having to share a key beforehand. This logic and mathematical concepts behind this, is what makes the process of modern encryption possible today.

2.2 Mathematical Techniques in Cryptography

Modular arithmetic: The most basic and fundamental element in cryptography is modular arithmetic which is basically a system of numbers that wrap around one another after reaching a certain value or the modulus [8, 9]. Think about this as a clock: after the clock strikes 12, you don't get to 13, it goes back to 1. Mathematically this can be described as 13 mod 12 = 1. The operation "mod" is what cryptography mainly depends on and this matters because it allows mathematicians to be able to create groups or structures where certain challenges become computationally difficult to reverse. In regular arithmetic, it's possible to work backwards to find the original number but in modular arithmetic, some problems become computationally hard. Even the simpler Caesar cipher uses modular arithmetic to form a pattern as to how the letters wrap around the whole alphabet.

Prime numbers and their importance. Prime numbers are those numbers that are only divisible by one and themselves and serve as the backbone of modern day encryption [10, 11, 12]. Since every integer excluding 0 and 1, can be factored into primes, these numbers are important to be able to create secure data transmission. They are considered extremely vital due to the fact that it is easy to multiply 2 large prime numbers but computationally infeasible with current methods to factor the product into the original numbers. For very large numbers, computers can take days, months and even years to factor them. This difficulty is what makes it safe where implementations require prime numbers that are at least a couple hundred digits long [11].

Euclidean algorithm. When given two large primes, how do we actually build any keys from them? That's where the principles of the Euclidean algorithm are applied [13, 14]. This algorithm that dates back to around 300 BC is one of the most efficient methods in computing the greatest common divisor of 2 given integers. This ensures that certain numbers are coprime, meaning they don't share any common factors other than 1, which is important for the key's properties and function. An extension to this extends further by where the modular inverses are calculated meaning that this process requires finding the number then, multiplied by an exponent and then divided by a certain value would leave a remainder of exactly 1. Without this extension to the Euclidean algorithm, referred to as the Extended Euclidean Algorithm, the key generation would be infeasible and extremely time-taking [13].

RSA encryption: RSA encryption is by far the public-key encryption system used most extensively all over the globe [15, 16, 17]. Named after its creators – Rivest, Shamir and Adleman – it is used by having a public key for encryption and a private one for decryption. On a basic level, the receiver chooses any 2 large primes, p and q and then finds their product 'n', which is a part of the public key. Then the receiver calculates the following: $\varphi(pq) = (p-1)(q-1)$ and chooses a number that's relatively prime to the value, denoted as 'e' and computes it to find 'd' which is the modular inverse of 'e'. In simpler terms, anyone can use it to lock a message but only a private key can unlock it. RSA is used for online banking and security during communications as well [16].

Digital signatures: A digital signature applies concepts from RSA to confirm verification [2, 18]. The sender generates a unique message and then encrypts it with their key, which is private and then the recipient decrypts it using the sender's public key and compares the message and if they match, it's authentic and unchanged. Digital signatures provide broadly 3 benefits: authentication of message which focuses on confirming that the message came from who it claims, data integrity which proves that the message was not changed in any way during the transit and even the fact that the sender cannot later deny having sent the message [2]. In terms of legality, this creates a proof of who sent the message, when and that nothing that was contained within was changed.

2.3 Cryptography in Investigative and Forensic Contexts

The FBI vs Apple: Case Study: One of the most famous case studies focusing on the connection of cryptography with a criminal investigation occurred in 2016 [3, 18]. In 2015, there was a San Bernardino terrorist attack where the FBI tried to unlock an iPhone belonging to one of the shooters. The phone was protected by a 4-digit code and ten failed attempts would mean all encrypted data would be erased permanently. Apple CEO, Tim Cook stated that this went against their policy and would lead to a compromise in user privacy and create a dangerous precedent. Towards the end, the FBI dropped the case after paying around $1.3 million in order to unlock the iPhone, with the help of a third party [18]. This case highlights how the same mathematical principles that protect the data of innocent people are also the same that protects criminals and their communications.

Ransomware: Ransomware is defined as the malware that locks data using cryptography [19, 20]. Modern cyberattacks and ransomware attacks use principles of both RSA algorithms and AES or the Advanced Encryption Standard algorithm. This is a hybrid encryption model that generates a key pair, encrypts all files using the public key and transmits the private key to the attacker's server, without which the victim cannot decrypt their files. From the perspective of forensics, the analysis can help identify encrypted files but the use of the hybrid encryption makes data recovery extremely difficult without the decryption key. The WannaCry attack of 2017 led to researchers recovering the prime numbers used to generate the RSA keys if the infected computer was not restarted [19]. In terms of economic factors, CryptoWall was estimated to have produced over $18 million which shows how financially draining these attacks can be and why investigators need to understand the mathematical principles behind them [20].

Blockchain forensics: Cryptocurrencies take the use of digital signatures based on RSA-like mathematics [21, 22]. Criminals use them with the understanding that transactions are private but in reality, these blockchain transactions are entirely transparent. Each transaction is stored in a ledger

which is visible to anyone at any point in time and a common misconception lies in the fact that people believe an individual's transactions are connected to their names, instead they're connected to their wallet's public key. In the year 2013, Sarah Meiklejohn, a security researcher, published research focusing on the different ways to follow the money through different complex transactions until they reached a point where the individual was known [21]. Using this information, investigators can trace cryptocurrency transactions, build audit trails that are admissible in court and mostly conduct the real-time detection of threats. Therefore, in conclusion, the same mathematical structure that provides criminals the confidence to assume they're protected is precisely what makes them traceable.

3. Problem Definition

One of the gaps that is observed in the sources is that most of the educational literature focuses specifically either on math or the real-world application but there was rarely any bridge found connecting the two. There are papers that are written for specialists at a higher level which includes knowledge that high-schoolers don't have, while the basic, introductory sources often skip the actual math. The purpose of this paper is to attempt and bridge that gap for a familiar audience who is comfortable with algebra but not yet with number theory.

4. Methodology

In order to write this review, sources were collected using Google Scholar, educational websites and mostly online academic databases. The most important keywords included: "modular arithmetic cryptography", "RSA encryption", "prime numbers and cryptography", "digital forensics encryption", "FBI Apple encryption case" and lastly "blockchain forensics law enforcement". Different sources were selected on the basis of whether they were educational or academic and written at a lower level, something that could be easily comprehended at a high-school level and most importantly, sources that were most relevant to the question at hand.

Additionally, sources that demanded a foreknowledge of programming or ones that contained high level mathematical proofs were not used in direct citation but did however, help build the background understanding. Some of these sources included websites such as Khan Academy [1], GeeksforGeeks [8, 10, 15], Brilliant.org [16], Cornell University [17] and also the CISA [2] in addition to the academic papers, articles and case studies that were used. The literature was organized thematically into three categories: foundations of cryptography, mathematical techniques in cryptography, and cryptography in investigative and forensic contexts.

5. Results and Discussion

After understanding and looking across all the literature, several important but clear patterns emerge. Firstly, every major cryptographic technique from the simplest Caesar cipher to the RSA, it all depends on modular arithmetic. This is not a coincidental event, where it creates the one-way nature of encryption that makes it useful in order to protect evidence and a longer process when criminals try exploiting it.

Secondly, the security of modern encryption depends on mathematical problems that are currently hard to solve. These security tests are hard but not impossible to crack. As computational power increases, particularly with the development of quantum computing, these protections may become vulnerable.

Thirdly, there is a recurring tension between security and access. Using the example of the FBI vs Apple case, which was not just a legal argument but a mathematical one [3, 18]. In order to weaken the encryption of one user, it would lead to weakening it for everyone.

Lastly, criminals also make mathematical mistakes such as the WannaCry's developer who did not clear the memory and researchers were able to recover the prime numbers which were used to generate the RSA key-pair because of this minor implementation error [19]. Understanding the math is what helped the researchers understand the errors and exploit them.

Table 1: Summary of Core Mathematical Techniques in Cryptography

Technique	Core Principle	Role in Cryptography	Example Application
Modular Arithmetic	Numbers wrap around after reaching a modulus, like a clock going from 12 back to 1	Foundation of all encryption; creates one-way functions that are hard to reverse	Caesar cipher shift: $En(x) = (x+n) \bmod 26$
Prime Numbers	Easy to multiply two large primes; seemingly impossible to factor the product back	Provides the security backbone; implementations require primes hundreds of digits long	RSA key generation using two large primes p and q
Euclidean Algorithm	Computes greatest common divisor; extended form calculates modular inverses	Ensures numbers are coprime; without it, key generation would be infeasible	Finding 'd' (private key) as modular inverse of 'e' in RSA
RSA Encryption	Combines all three techniques into a public-key system with two keys	Anyone can lock a message with public key; only private key can unlock it	Online banking, secure communications, digital certificates

Table 2: Case Studies in Cryptography and Criminal Investigation

Case	Cryptographic Element	Outcome	Key Insight
FBI vs. Apple (2016)	4-digit passcode with auto-erase after 10 failed attempts; encrypted data	FBI paid ~$1.3M to third party to unlock the iPhone	Same math that protects innocent people also protects criminals
WannaCry Ransomware (2017)	Hybrid RSA + AES encryption; private key sent to attacker's server	Researchers recovered RSA primes from memory on unrestarted computers	Criminals make mathematical mistakes that can be exploited
Blockchain Forensics (2013–present)	Digital signatures; transactions linked to wallet's public key, not names	Investigators trace transactions through chains to known individuals	The math that gives criminals confidence is what makes them traceable

6. Conclusion

This study addressed the role of key mathematical techniques in cryptography and their relevance to digital investigations. Modular arithmetic, prime factorization, the Euclidean algorithm, and RSA encryption form the core framework that enables secure communication systems. These methods provide strong protection for digital data while also presenting challenges for forensic access and law enforcement. Case studies demonstrate that cryptographic systems can both conceal and reveal information depending on their implementation and analysis. The findings highlight the importance of mathematical understanding in cybersecurity, digital forensics, and education. Future developments in quantum computing and post-quantum cryptography will further shape the balance between security and accessibility.

Using tools such as digital signatures allow for verification of untampered or changed evidence and blockchain public ledgers which expose any criminal transactions. Negatively, this same encryption is what blocks the investigators from accessing different phones, files and communications when required. These implications extend even beyond law enforcement, to education and even cybersecurity. For example, in math education, cryptography shows that abstract concepts such as modular arithmetic have critical real-world implications. In cybersecurity, understanding the RSA sheds light onto why key lengths are important and why computing is a real threat, particularly in future scenarios.

7. Future Scope

Areas for further studies include quantum cryptography (which is where concepts of physics are used to guarantee security), the ethics around the access of data to law enforcement forces and even post-quantum encryption algorithms which are designed to remain safe and secure, when there are future developments in quantum computing. Additionally, future work could address the pedagogical gap identified in this review—developing resources that bridge abstract mathematical concepts and their real-world forensic applications for high-school audiences.

References

[1] Khan Academy. Modern cryptography. https://www.khanacademy.org, 2024.
[2] CISA (Cybersecurity and Infrastructure Security Agency). Understanding digital signatures. https://www.cisa.gov/news-events/news/understanding-digital-signatures, 2023.
[3] Markkula Center for Applied Ethics, Santa Clara University. Apple vs. FBI case study. https://www.scu.edu/ethics/focus-areas/business-ethics/resources/apple-vs-fbi-case-study/, 2016.
[4] GhostVolt. The story of cryptography: history. https://www.ghostvolt.com/articles/cryptography_history.html, 2023.
[5] S. Singh. The code book: the science of secrecy from ancient Egypt to quantum cryptography. Anchor Books, 2000.
[6] D. Kahn. The codebreakers: the comprehensive history of secret communication from ancient times to the internet. Scribner, 1996.
[7] W. Diffie, M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory. Vol. 22, pg. 644–654, 1976.
[8] GeeksforGeeks. Modular arithmetic. https://www.geeksforgeeks.org/engineering-mathematics/modular-arithmetic/, 2024.
[9] K. Sookocheff. Cryptography for the everyday developer: modular arithmetic. https://sookocheff.com/post/cryptography/cryptography-for-the-everyday-developer/modular-arithmetic/, 2019.
[10] GeeksforGeeks. Prime numbers in cryptography. https://www.geeksforgeeks.org/maths/why-prime-numbers-are-used-in-cryptography/, 2024.
[11] H. Rowland. The role of prime numbers in RSA cryptosystems. Georgia College & State University. https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/rowland.pdf, 2015.
[12] ScienceABC. How are prime numbers used in cryptography? https://www.scienceabc.com/innovation/how-are-prime-numbers-used-in-cryptography.html, 2023.
[13] EITCA Academy. How does the Euclidean algorithm work and why is it important in cryptographic protocols? https://eitca.org, 2023.
[14] K. Sookocheff. Cryptography for the everyday developer: number theory for public key cryptography. https://sookocheff.com/post/cryptography/cryptography-for-the-everyday-developer/euclidean-algorithm-and-public-key-cryptography/, 2019.
[15] GeeksforGeeks. RSA algorithm in cryptography. https://www.geeksforgeeks.org/computer-networks/rsa-algorithm-cryptography/, 2024.
[16] Brilliant.org. RSA encryption. https://brilliant.org/wiki/rsa-encryption/, 2024.
[17] Cornell University Department of Mathematics. Primes, modular arithmetic and public key cryptography. https://pi.math.cornell.edu/~mec/2003-2004/cryptography/RSA/RSA.html, 2004.

[18] EBSCO Research Starters. FBI–Apple encryption dispute. https://www.ebsco.com/research-starters/law/fbi-apple-encryption-dispute, 2024.
[19] ResearchSquare. An experimental analysis of cryptographic techniques used in ransomware and their impact on digital forensic investigation. https://www.researchsquare.com/article/rs-9304413/v1, 2025.
[20] Morphisec. Breaking down ransomware encryption: key strategies, algorithms and implementation trends. https://www.morphisec.com/blog, 2024.
[21] Forensics Colleges. Blockchain forensics: how investigators track cryptocurrencies. https://www.forensicscolleges.com/blog/blockchain-forensics, 2023.
[22] TRM Labs. Blockchain forensics. https://www.trmlabs.com/glossary/blockchain-forensics, 2024.