In hidden realms where data flows,
Where silence guards what no one knows,
Prime numbers stand as a secret wall,
The quiet sentinels of all.

— By Author

Prologue

In the quiet before numbers took on meaning, before commerce and code intertwined, there existed only purity — simple, indivisible truths written into the very fabric of mathematics. Prime numbers, timeless and untouched, stood like sentinels in the infinite expanse of numerical space. From the ancient musings of philosophers to the algorithms that now protect digital lives, primes have traversed history, not as mere digits, but as the hidden skeletons of logic and order. This is the story of how their silent strength became the foundation of modern security.

Whispers from the Infinite

LONG ago, in the boundless kingdom of Numbers, there lived special beings - rare, indivisible, and pure. These were the *Primes*, the elemental spirits of arithmetic, standing alone and unbroken. No one could divide them into smaller parts; they simply were whole and sovereign. These are the numbers that cannot be expressed as the product of two smaller whole numbers.

For instance, 11 and 13 are primes, standing alone in their uniqueness, while 12 is not - it breaks down into 3 multiplied by 4. Primes are like rare gems scattered through the boundless cosmos of numbers, glinting with a kind of mathematical purity. For centuries, mathematicians have wandered through this infinite numerical landscape, finding in primes a source of endless fascination.

Numbers like 2, 3, 5, 7, 11, 13, 17, 19, and 23 aren't just numbers on a page—they evoke a timeless beauty, as if they belong to a realm beyond the reach of the physical world. To mathematicians, they are more than just numbers; they are nature's elegant, eternal offering. Prime numbers serve as the fundamental components from which all other numbers are formed. Any number that isn't prime can be broken down into a product of these essential building blocks. Just as every molecule in the physical world is composed of atoms from the periodic table, every whole number is constructed from primes. In this way, a list of prime numbers becomes the mathematician's equivalent of the periodic table — a blueprint of numerical creation. In recent decades, prime numbers have stepped out of the quiet halls of academia and into the bustling world of commerce. Once the exclusive fascination of mathematicians, primes have now become key players in the global economy.

The turning point came in the 1970s, when three researchers *Ron Rivest, Adi Shamir, and Leonard Adleman* transformed the study of prime numbers from a theoretical pastime into a powerful tool for real-world security [1]. Building on a centuries-old insight by *Pierre de Fermat*, they developed a method to harness the unique properties of primes to safeguard sensitive data.

Creators of RSA

Ronald Rivest, Adi Shamir, and Leonard Adleman are a celebrated trio of computer scientists who, in 1977, developed the RSA algorithm, a cornerstone of modern public-key cryptography.

Ronald Rivest (May 6, 1947) is an American cryptographer

Figure 1: The Trio that secured the Digital World [2]

and computer scientist. He obtained a B.A. in Mathematics from Yale University in 1969 and a Ph.D. in Computer Science from Stanford University in 1974. He is an institute professor at the Massachusetts Institute of Technology (MIT) and a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL).

Adi Shamir (July 6, 1952) is an Israeli cryptographer and inventor. He received a Bachelor of Science degree in Mathematics from Tel-Aviv University in 1973 and obtained an MSc. and Ph.D. Computer Science from the Weizmann Institute in 1975 and 1977, respectively. He spent a year as a postdoctoral researcher at the University of Warwick and did research at MIT from 1977 to 1980.

Leonard Adlemann (December 31, 1945) is an American computer scientist. He received a B.S. in Mathematics in 1968 and a Ph.D. in Electrical Engineering and Computer Science (EECS) in 1976 from the University of California, Berkeley. He was a faculty member of the Mathematics Department at MIT from 1976 to 1980.

A Sleepless Night Sparked the RSA Revolution

Rivest, Shamir, and Adleman formed a remarkably effective team. Rivest, a computer scientist, had an exceptional talent for absorbing new ideas and applying them in unexpected ways. He consistently kept up with the latest research, which inspired a stream of imaginative but ultimately flawed candidates for the one-way function at the core of an asymmetric cipher. Shamir, also a computer scientist, possessed a lightning-fast intellect and a knack for cutting through complexity to find the essence of a problem. Like Rivest, he proposed many ideas for constructing an asymmetric cipher, but these too proved flawed. Adleman, a mathematician known for his stamina, rigor, and patience, played a crucial role in identifying the weaknesses in the proposals of Rivest and Shamir. His critical eye helped prevent them from spending time on unworkable approaches. For a year, Rivest and Shamir generated ideas, while Adleman systematically dismantled them. Although they began to lose hope, they did not realize that this cycle of failure was steering them away from fruitless directions and guiding them toward more promising ground. Eventually, their persistence paid off. In April 1977, Rivest, Shamir, and Adleman spent passover at a student's home, returning to their places around midnight. Rivest, unable to sleep, lay on his couch reading a mathematics textbook. His mind kept circling back to a question that had consumed him for weeks:

- Is it possible to build an asymmetric cipher?
- Could there be a one-way function that only the intended recipient could reverse, using some special information?

Suddenly, the pieces began to fall into place. In a moment of clarity, Rivest had a breakthrough. He stayed up the rest of the night formalizing the idea, effectively drafting an entire scientific paper before dawn. Although the insight was his, it was the result of a yearlong collaboration with Shamir and Adleman—and it wouldn't have been possible without their joint effort. When he completed the paper, Rivest listed the authors alphabetically: Adleman, Rivest, Shamir.

The next morning, Rivest handed the paper to Adleman, who, true to form, tried to find flaws. This time, he couldn't. His only objection was the authorship.

> I told Ron to take my name off the paper," Adleman later recalled. "I told him it was his invention, not mine. But Ron refused, and we debated it. Eventually, we agreed that I'd sleep on it and decide.

The following day, Adleman returned with a compromise that he would be listed third.

> I remember thinking this would be the least interesting paper I'd ever co-author, Adleman said.

He couldn't have been more mistaken. The system—named RSA, for Rivest, Shamir, and Adleman (rather than ARS)—would go on to become the most influential cipher in modern cryptography.

Thanks to their work, prime numbers now help shield credit card information as it moves through the digital corridors of online shopping, proving that even the purest mathematics can find purpose in the chaos of modern life. Whenever you make an online purchase, your computer relies on the security provided by prime numbers with up to a hundred digits. To date, over a million primes have been employed to safeguard the world of e-commerce.

Leveraging the unique mathematical properties of prime numbers, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA public-key encryption system in 1977. It has become one of the most commonly used encryption techniques worldwide, relying on the challenge of factoring large numbers to secure data.

A Historical Overview

The creation of RSA marked a groundbreaking moment in cryptography. Before its invention, encryption relied on symmetric key methods, where the same key was used for both encryption and decryption. RSA introduced a revolutionary concept: the use of two distinct keys — a public key for encryption and a private key for decryption.

This breakthrough solved a long-standing issue in cryptography, *the key distribution problem*. With RSA, secure communication became possible without the need for both parties to exchange a secret key in advance, making it especially valuable for securing communication over untrusted networks, such as the Internet.

Over the years, RSA has evolved, with constant refinements enhancing its security and performance. Cryptographers have strengthened the algorithm by increasing key sizes and optimizing the underlying mathematics. Today, RSA is an integral part of modern cryptographic systems, continuing to protect sensitive data across the digital landscape.

Large Prime numbers: Building Blocks of RSA

RSA relies on three fundamental elements: the public key, the private key, and the modulus. The public key is used to encrypt messages, while the private key is used to decrypt them. The modulus is a large number created by multiplying two prime numbers, and it plays a central role in both the encryption and decryption processes.

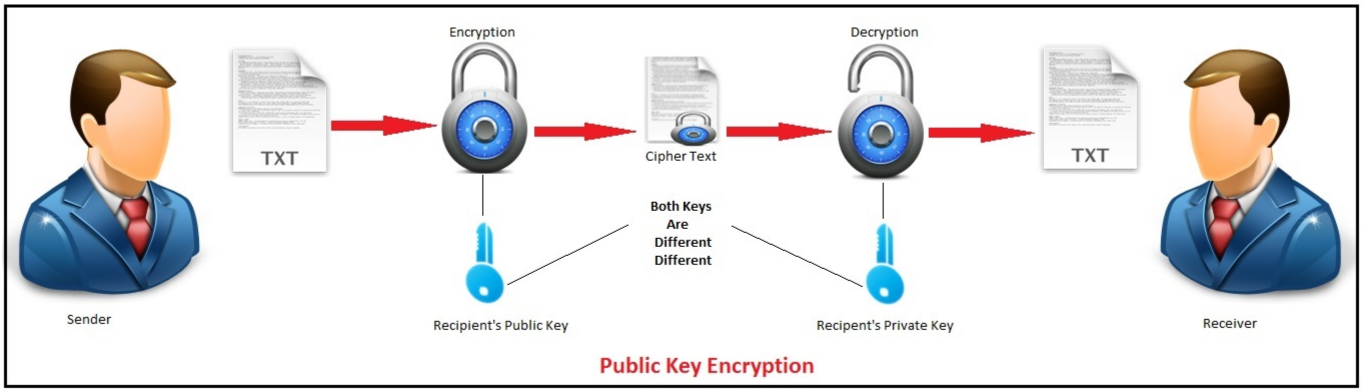

Figure 2: Public-Private Key Encryption-Decryption[3]

When a sender wishes to send a secure message, they encrypt it using the recipient's public key. Upon receiving the message, the recipient decrypts it using their private key, ensuring that only they can access the original content. This asymmetric encryption method guarantees that only the intended recipient can decode the message.

One of the standout features of RSA is its ability to generate digital signatures. By signing a message with their private key, the sender creates a unique signature that can be verified by anyone with access to the sender's public key. This mechanism ensures both the authenticity and integrity of the message, confirming it has not been altered in transit.

RSA's strength lies in the mathematical difficulty of factoring large prime numbers. The larger the key size, the more computationally intense it becomes to factor the modulus and compromise the encryption. This characteristic makes RSA a highly secure encryption method, effectively safeguarding sensitive data from unauthorized access.

The Mathematics Behind RSA: Prime Numbers and Their Role

Figure 3: Public Key Encryption[4]

RSA encryption relies heavily on the properties of prime numbers to ensure security. The core idea is based on the mathematical challenge of prime factorization.

Before delving into the intricacies of RSA encryption, it's crucial to grasp some fundamental concepts from number theory [5], [6]. These terminologies will provide a solid foundation for understanding the subsequent discussion on key generation.

Modulus:

At its core, the modulus n is the integer we are "dividing by" when we talk about remainders. The expression $a \equiv b(mod\, n)$, read as "a is congruent to b modulo n", means that the difference between a and b is an integer multiple of n. In other words, n divides $(a - b)$ without leaving a remainder.

Example: Consider the expression $17 \equiv 2(mod\; 5)$.

Here the modulus is 5. Because $17 - 2 = 15$ and 15 is a multiple of 5. Also both 17 and 2 leave the remainder 2 when divided by 15.

Real-World Case: A familiar use of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. Time-keeping on this clock uses arithmetic modulo-12.

Figure 4: Modular Arithmetic applied on 12 Hr. Clock[7]

- If the time is 7:00 now, then 8 hours later it will be 3:00.
- Simple addition would result in 7 + 8 = 15, but clocks “wrap around” every 12 hours.
- Because the hour number starts over after it reaches 12, this is arithmetic modulo 12.

Modular Multiplicative Inverse

THE modular multiplicative inverse of an integer a modulo n is an integer x such that their product is congruent to 1 modulo n. In mathematical notation,

$$a.x \equiv 1(mod\ n) \tag{1}$$

A modular multiplicative inverse of a modulo n exists if and only if a and n are *relatively prime*, i.e. $gcd(a, n) = 1$.

Example: Identify modular multiplicative inverse of 3 modulo $7!$.

Let x be the modular multiplicative inverse, then $3.x \equiv 1(mod\ 7)$

We will try values for x from 1 to 6,

- $3.1 = 3 \equiv 3(mod\ 7)$
- $3.2 = 6 \equiv 6(mod\ 7)$
- $3.3 = 9 \equiv 2(mod\ 7)$
- $3.4 = 12 \equiv 5(mod\ 7)$
- $3.5 = 15 \equiv 1(mod\ 7)$...got it!
- $3.6 = 18 \equiv 4(mod\ 7)$.

As $15(mod\ 7) = 1$, therefore modular multiplicative inverse of 3 modulo 7 is 5.

Euler's totient function

The Making of $\phi(n)$: A Brief History

The Euler totient function's journey from initial concept to established mathematical tool spanned over a century. It began in the 18th century with **Leonhard Euler's** pioneering work on counting coprime integers, initially without a specific symbol. By 1784, he used πD to denote this value [8]. The early 19th century brought standardization with Carl Friedrich Gauss's introduction of the $\phi(n)$ notation in his *Disquisitiones Arithmeticae* [9]. The final stage in its formalization came in 1879 when J.J. Sylvester provided the descriptive name *totient* [10]. This historical evolution showcases the gradual process of discovery, notation, and naming that often characterizes the development of mathematical ideas.

Mathematical definition: For a positive integer n, $\phi(n)$ is the number of integers k in the range $1 \leq k \leq n$ such that $gcd(n, k)$[1] $= 1$.

[1] gcd stands greatest common divisor, e.g. $gcd(2, 4) = 2$.

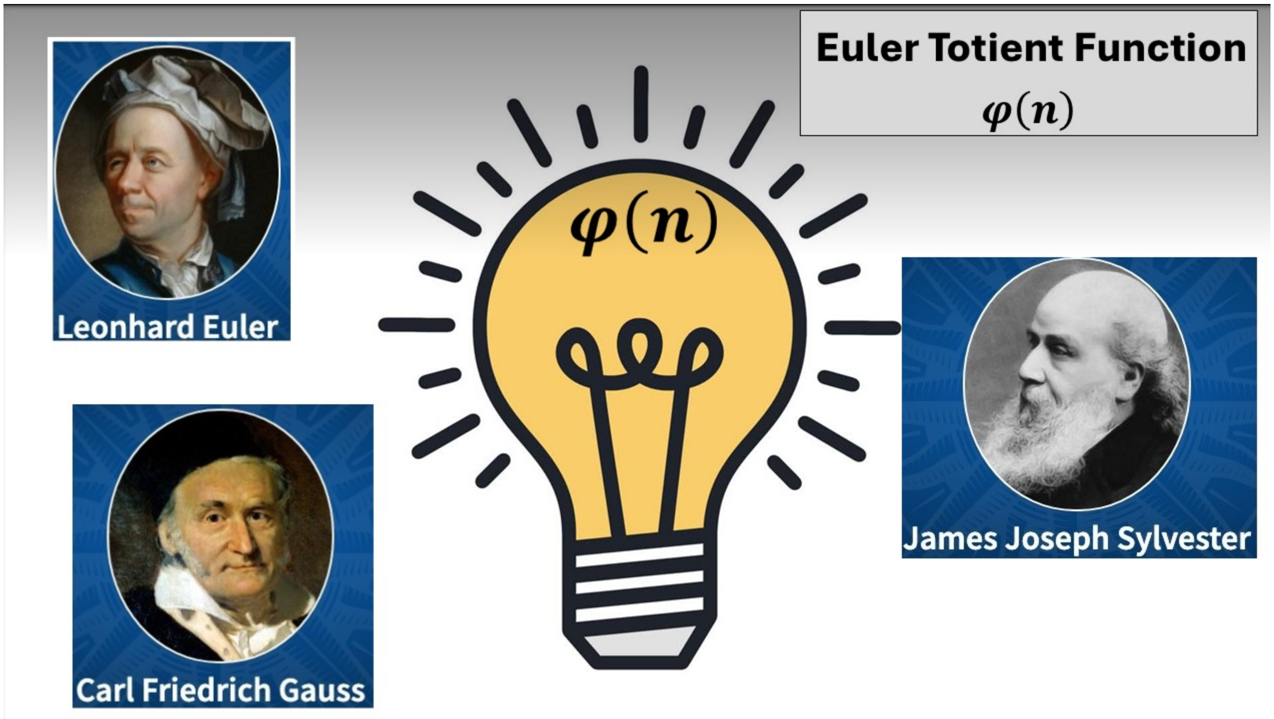

Figure 5: Generators of Totient.

Formula: If the prime factorization of n is $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where $p_1, p_2, \dots, p_r$ are distinct prime numbers and $k_1, k_2, \dots, k_r$ are positive integers, then Euler's totient function is calculated as:

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \tag{2}$$

i.e.

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \tag{3}$$

Example: Let us find $\phi(12)$: Prime factorization of 12 is $12 = 2^2 \times 3^1$. $\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$. We can also see that there are four numbers $1, 5, 7, 11$ relatively prime to 12.

Euler's totient function is crucial in the RSA public key cryptosystem for determining the size of the multiplicative group modulo n, which is essential for key generation in classical cryptography.

With these fundamental definitions in mind, we can now proceed to understand the process of Key Generation in RSA encryption.

In RSA, two large prime numbers, p and q, are chosen and multiplied to produce a large composite number, $n = p \times q$, which becomes part of the public key. While it's easy to compute n from p and q, the reverse—determining p and q from n—is computationally hard when p and q are large enough. This one-way nature (easy to compute, hard to reverse) forms the backbone of RSA's security.

These primes are used to generate both the modulus (n) and the totient

$$\phi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p-1)(q-1) \tag{4}$$

which are essential for computing the public and private keys. The security of RSA increases with the size of the prime numbers: larger primes mean greater difficulty in factoring n, making brute-force attacks infeasible with current computing power.

Key Generation: Step-by-Step

1. *Choose Two Large Prime Numbers:*
   Select two distinct large prime numbers, p and q. These primes are kept secret.
2. *Compute the Modulus:*
   Calculate $n = pq$.This modulus n is used in both the public and private keys.
3. *Calculate Euler's Totient Function:*
   Compute $\varphi(n) = (p-1)(q-1)$. This value is crucial for determining the public and private exponents.

4. *Choose the Public Exponent:*
   Select an integer e such that $0 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$
5. *Determine the Private Exponent:*
   Compute d as the modular multiplicative inverse of e modulo $\varphi(n)$ satisfying:

$$e * d \equiv 1(mod\varphi(n))$$

6. *Form the Public and Private Keys:*
   - Public Key:(e, n)
   - Private Key: (d, n)

Practical Application

Secure Web Browsing

RSA encryption plays a crucial role in securing sensitive data by preventing unauthorized access and interception. For instance, when you browse a website that uses *https*, RSA encryption helps secure the connection between your browser and the server. It ensures that data exchanged during your session remains private and protected from interception or tampering by malicious actors. Major companies like *Google*, *Facebook*, and *Amazon* rely on RSA to protect their users' information. RSA encryption is also widely used in secure email communication, *virtual private networks (VPNs)*, and other applications requiring secure data transmission.

Secure Email Communication

EMAIL remains a vital part of modern communication, making the security of email transmissions critically important.

RSA encryption is commonly used to protect email content by encoding messages in a way that only the intended recipient, using their private key, can decrypt and read. Using public- and private-key pairs, RSA provides a strong defense against unauthorized access and eavesdropping, helping to keep sensitive information secure during transmission.

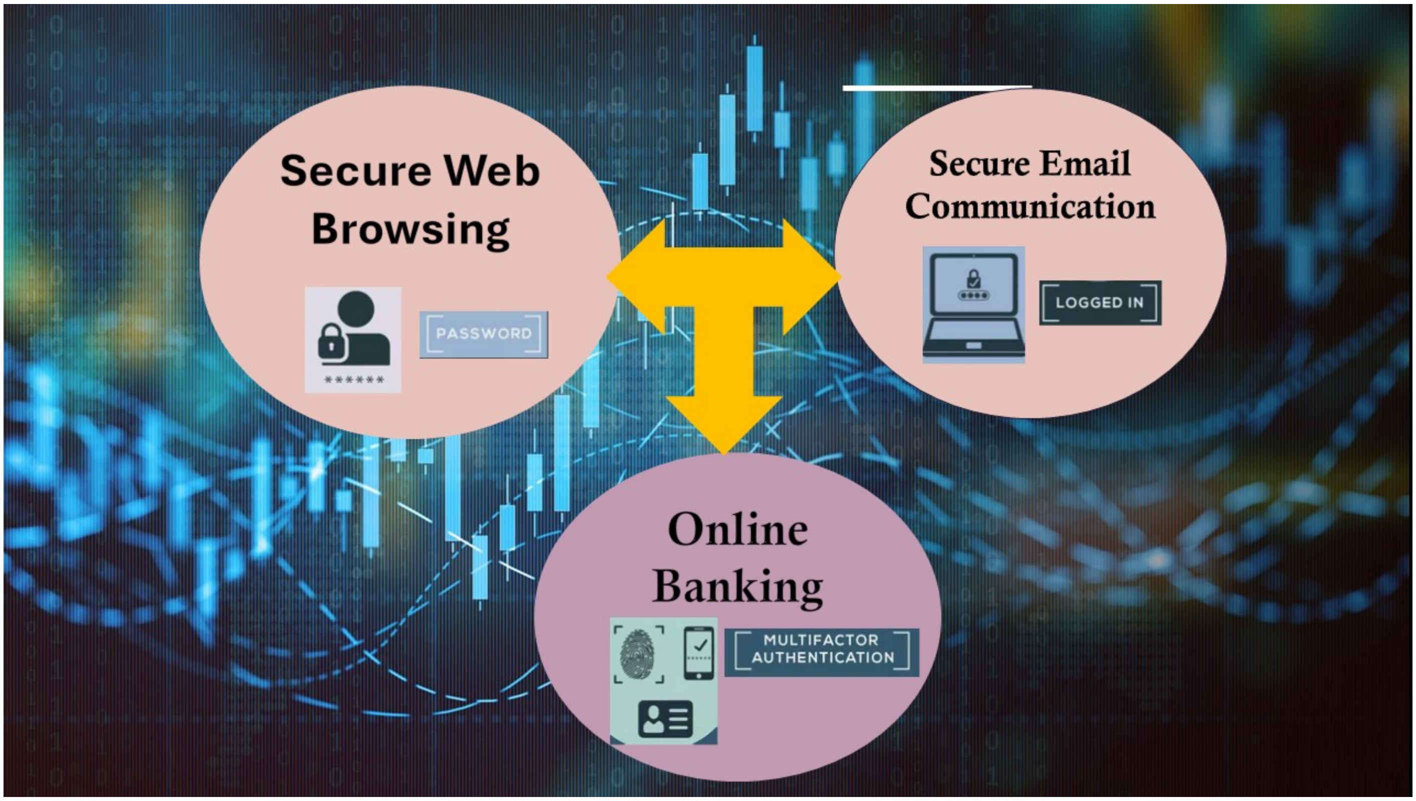

Figure 6: Secure communication systems.

Online Banking

Online banking has revolutionized the way we manage our finances, offering unmatched convenience and accessibility. Yet, securing online transactions is crucial. RSA encryption plays a vital role in protecting the confidentiality and integrity of these financial interactions. When you access your online banking account, RSA helps establish a secure link between your device and the bank's server, ensuring that sensitive data, like login details and account information, remains shielded from unauthorized access. Many banks also incorporate RSA into two-factor authentication systems, combining encrypted communication with extra layers of security such as *one-time passwords (OTPs)* or *biometric verification.* This multi-layered approach strengthens protection and builds trust in online banking services.

Epilogue

What began as a quiet curiosity among ancient mathematicians has become a cornerstone of the digital age. From whispers in the libraries of Alexandria to algorithms securing the world's financial arteries, prime numbers have proven their enduring importance. RSA encryption, grounded in the elegant difficulty of prime factorization, is more than a feat of engineering; it is a testament to the power of pure thought. As we move deeper into an era shaped by data and connection, primes endure, not just as tools, but as enduring symbols of how beauty, simplicity, and rigor intersect to safeguard the most complex aspects of our modern lives. Despite the strength of RSA and other modern ciphers, cryptanalysts continue to play a vital role in intelligence gathering. Their ongoing success is evident in their high demand—the NSA remains a major employer of mathematicians. A relatively small fraction of global information flow is securely encrypted; the remainder is poorly encrypted or not encrypted at all. This is due to the rapid increase in Internet users, many of whom neglect adequate privacy precautions. Consequently, national security organizations, law enforcement, and others can access vast amounts of information. Even when users employ the RSA cipher properly, codebreakers can still glean information from intercepted messages. Techniques like traffic analysis remain valuable; even without deciphering message content, identifying senders and recipients can be highly revealing. Cryptanalysts recognize that their goal is to crack the RSA cipher, the cornerstone of modern encryption. RSA protects critical military, diplomatic, commercial, and criminal communications—precisely the messages that intelligence agencies seek to decipher. To challenge robust RSA encryption, cryptanalysts require a major theoretical or technological breakthrough. They have long sought a shortcut to factoring, a method that drastically reduces the steps required to find the prime factors p and q, but all attempts to develop a fast-factoring algorithm have failed. Mathematicians have studied factoring for centuries, and modern techniques are not significantly better than ancient ones. Indeed, the laws of mathematics may forbid the existence of a substantial shortcut for factoring.

With little hope of a theoretical breakthrough, cryptanalysts have focused on technological innovation. If there is no way to reduce the steps required for factoring, they need a technology that can perform these steps more quickly. While silicon chip speeds continue to increase, doubling roughly every eighteen months, this progress is insufficient to significantly impact factoring speeds. Cryptanalysts require a technology that is billions of times faster than current computers. Consequently, they are exploring a radically new form of computing: the Quantum Computer (QC). A functional QC could perform calculations with such enormous speed that it would make a modern supercomputer seem like a broken abacus. This necessitates the study of quantum cryptography.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983, ISSN:

0001-0782. DOI: 10.1145/357980.358017. [Online]. Available: https://doi.org/10.1145/357980.358017.

[2] D. Parovsky, *How to master advanced encryption algorithms: AES vs. RSA*, en, https://howset.com/how-to-master-advanced-encryption-algorithms-aes-vs-rsa/, Oct. 2023.

[3] S. Somani, *RSA algorithm with c#*, en, https://www.c-sharpcorner.com/UploadFile/75a48f/rsa-algorithm-with-C-Sharp2/, Dec. 2013.

[4] M. Abad, *EU sets new online rules for google, meta to curb illegal content*, en, https://www.rappler.com/technology/european-union-sets-new-online-rules-google-meta-curb-illegal-content/, Apr. 2022.

[5] D. Burton, *Ebook: Elementary number theory*. McGraw Hill, 2010.

[6] G. Hardy, "An introduction to the theory of numbers," 1929.

[7] S. Tobak, *The secret to prioritizing your time*, en, https://www.entrepreneur.com/living/the-secret-to-prioritizing-your-time/231520, Feb. 2014.

[8] L. Euler, A. Diener, and A. Aycock, "Theoremata arithmetica nova methodo demonstrata," *arXiv preprint arXiv:1203.1993*, 2012.

[9] O. Neumann, "The disquisitiones arithmeticae and the theory of equations," in *The Shaping of Arithmetic after CF Gauss's Disquisitiones Arithmeticae*, Springer, 2007, pp. 107–127.

[10] D. H. Lehmer, "On euler's totient function," 1932.