Journal of Advances and Scholarly Researches in Allied Education
Vol. 23, Issue No. 2, April-2026, ISSN 2230-7540

DOI: https://doi.org/10.29070/ddy24369



# Role of Prime Numbers in Cryptography

**Dr. Naveen Kashyap** [1] *

1. Ph.D. in Mathematics, Ambikapur, Surguja, C.G., India
pmrsushil@gmail.com

**Abstract:** The significance of prime numbers is profound within the domain of cryptography. In recent times, with the advent of digital communication systems, there is a need for the security of messages being transmitted in various fields like banking, e-commerce, government communications, and even personal matters. The field of cryptography is based on problems that are simple to solve in one direction but complex to solve in the other direction. Prime numbers are such examples, especially when large composite numbers are involved. This paper explores the theoretical and practical role of prime numbers in modern cryptographic systems. This paper commences with basic mathematical concepts regarding prime numbers, which include the Fundamental Theorem of Arithmetic and modular arithmetic. Next, it elaborates upon the use of these theories in public key encryption through an example of the RSA algorithm. Mathematical formulae are used alongside examples and visual aids to explain the process. Apart from discussing practical applications of prime numbers like internet security, digital signatures, and Blockchain technology, certain challenges are also presented. From the findings, it is evident that the prime number is a critical tool for secure communication in the digital age and will remain an active field of research in mathematics and computer science.

**Keywords:** Prime numbers, RSA algorithm, public key cryptography, number theory, data security, modular arithmetic

----------X----------

## INTRODUCTION

The modern era of digitization requires massive amounts of sensitive data like financial, personal, and governmental information to be exchanged through the communication network. Thus, ensuring the integrity, authenticity, and confidentiality of the transferred information is an absolute necessity.

Cryptography employs various mathematical principles required to achieve the objective. Cryptography in ancient times involved simple substitution and transposition methods. With the advent of computers and internet communication, complex mathematical principles were required to ensure secure transfer of information. Number theory plays a vital role in modern cryptography. Number theory involves the use of prime numbers extensively. Prime numbers refer to those integers that are greater than 1 and are divisible only by 1 and themselves. The principle of prime numbers seems to be very simple but in reality, it has deep mathematical significance which makes its application extremely important in cryptography. Factoring a large composite integer into two primes is a mathematically complex task, while multiplication is relatively easy even for large primes. It is practically impossible to factorize the two numbers if they are sufficiently large and thus provide strong security in cryptography.

### Objectives of the paper

- Mathematical characteristics of prime numbers will be described in detail.
- The use of these characteristics in cryptographic algorithms will be demonstrated.

- To analyze the RSA encryption system as a major application of prime numbers.
- To discuss modern applications and challenges in cryptographic security.

## MATHEMATICAL FOUNDATIONS OF PRIME NUMBERS

### Definition of Prime Numbers

A prime number is defined as a natural number greater than 1 that has exactly two distinct positive divisors.

Mathematically,

p is prime if

$p > 1$

and the only divisors of p are 1 and p.

Examples of prime numbers include:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

The number 2 is the only even prime number because every other even number can be written as a multiple of 2.

### Composite Numbers

A composite number is a positive integer greater than 1 that has more than two divisors.

Example:

$6 = 2 \times 3$

$12 = 2 \times 2 \times 3$

$15 = 3 \times 5$

Composite numbers can always be expressed as products of prime numbers.

### Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that:

Every integer greater than 1 can be uniquely expressed as a product of prime numbers, except for the order of the factors.

Example:

$84 = 2 \times 2 \times 3 \times 7$

This factorization is unique.

**Proof (Sketch)**

1. **Existence**: Every integer greater than 1 is either prime or divisible by a smaller number.
2. If it is divisible, the factorization process continues until only prime numbers remain.
3. **Uniqueness**: Suppose a number has two different prime factorizations.

Using Euclid's Lemma, one can show that a prime dividing a product must divide at least one factor. This leads to the conclusion that the two factorizations must contain the same primes.

Therefore, prime factorization is unique.

This theorem is critical in cryptography because it ensures that a number can only be factored in one specific way.

## MODULAR ARITHMETIC IN CRYPTOGRAPHY

Cryptographic algorithms frequently use modular arithmetic.

If a and b are integers and n is a positive integer, then

$a \equiv b \pmod{n}$

means that n divides $(a - b)$.

Example:

$17 \equiv 5 \pmod{12}$

because

$17 - 5 = 12$

which is divisible by 12.

It helps deal with large figures effectively during encryption.

## PUBLIC KEY CRYPTOGRAPHY

Public Key Encryption Unlike traditional cryptography methods that needed both sender and receiver to possess a single key, public key cryptography makes use of two keys.

Public Key - accessible to all

Private Key - must remain confidential

Information encrypted with the help of the public key can be decoded only through the use of a private key. It involves the use of prime numbers for generating keys.

## RSA CRYPTOGRAPHIC ALGORITHM

The RSA algorithm is one of the most widely used public-key cryptographic systems.

It was introduced in 1977 by:

• Ronald Rivest • Adi Shamir • Leonard Adleman

The security of RSA depends on the difficulty of factoring large integers.

**RSA Key Generation Process**

Step 1: Choose two large prime numbers

p and q

Step 2: Compute

$n = p \times q$

Step 3: Compute Euler's Totient Function

$\varphi(n) = (p - 1)(q - 1)$

Step 4: Choose integer e such that

$1 < e < \varphi(n)$

and

$\gcd(e, \varphi(n)) = 1$

Step 5: Compute d such that

$d \times e \equiv 1 \pmod{\varphi(n)}$

Public Key = (e, n)

Private Key = (d, n)

**Example of RSA Encryption**

For demonstration purposes we use small prime numbers.

Let

$p = 5$

$q = 11$

Then

$n = 5 \times 11 = 55$

$\varphi(n) = (5-1)(11-1) = 4 \times 10 = 40$

Choose

$e = 3$

Now compute d such that

$3d \equiv 1 \pmod{40}$

The solution is

$d = 27$

Public key = (3,55)

Private key = (27,55)

**Encryption**

If message M = 7

Ciphertext:

C = M^e mod n

C = 7^3 mod 55

C = 343 mod 55

C = 13

Encrypted message = 13

**Decryption**

M = C^d mod n

M = 13^27 mod 55

After modular computation, the result is

M = 7

Thus the original message is recovered.

**Conceptual Diagrams of Cryptographic Communication**


**Figure 1: Basic Encryption Model**


**Figure 2: Public Key Cryptography**

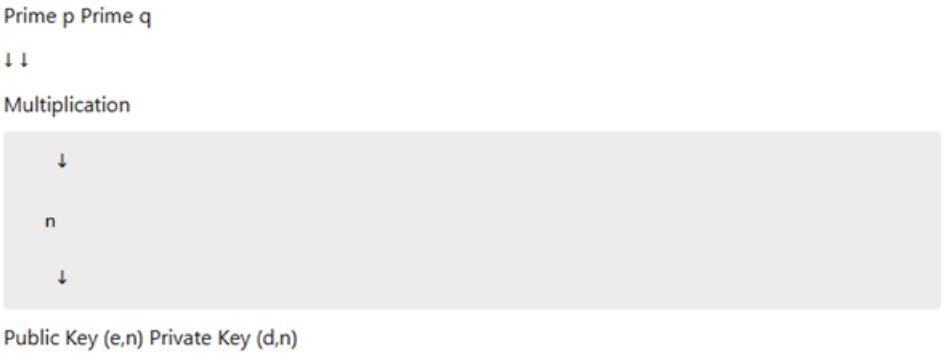


**Figure 3: RSA Key Generation Structure**

## SECURITY BASED ON PRIME FACTORIZATION

The security of RSA relies on the difficulty of factoring large numbers.

Example:

n = 391

Factorization:

391 = 17 × 23

This is easy because the number is small.

However, real cryptographic systems use numbers containing hundreds or thousands of digits.

Example:

n = p × q

where

p and q are 1024-bit prime numbers.

Factoring such numbers requires enormous computational resources.

This makes unauthorized decryption practically impossible using classical computers.

## APPLICATIONS OF PRIME NUMBER CRYPTOGRAPHY

**Secure Web Communication**

Internet protocols such as HTTPS rely on cryptographic algorithms based on prime numbers.

**Digital Signatures**

Digital signatures verify the authenticity of documents and ensure they have not been altered.

**Online Banking and E-Commerce**

Financial transactions require strong encryption to protect customer data.

**Blockchain Technology**

Blockchain systems use cryptographic hashing and digital signatures for transaction verification.

**Secure Email Systems**

Encryption algorithms protect sensitive email communication between users.

## LIMITATIONS AND FUTURE CHALLENGES

Despite the strength of prime-number cryptography, several challenges exist.

**Quantum Computing**

Quantum algorithms such as Shor's algorithm could potentially factor large numbers efficiently.

**Computational Complexity**

Key sizes must increase as computational power grows.

**Post-Quantum Cryptography**

Researchers are developing cryptographic systems that remain secure against quantum attacks.

Examples include:

- lattice-based cryptography
- code-based cryptography

## FUTURE RESEARCH DIRECTIONS

Future research in mathematical cryptography includes:

- Improved prime generation algorithms
- Quantum-resistant encryption methods
- Faster modular arithmetic algorithms
- Hybrid cryptographic systems

Prime numbers will continue to be central to these developments.

## CONCLUSION

Prime numbers form the mathematical backbone of modern cryptographic systems. Their unique properties enable the creation of encryption algorithms that secure digital communication across the globe. The RSA algorithm demonstrates how simple mathematical principles such as prime factorization and modular arithmetic can provide extremely strong security mechanisms.

As digital communication continues to expand, the importance of mathematical cryptography will only increase. Although new technologies such as quantum computing may challenge current systems, prime numbers will remain an essential component of cryptographic research and information security.

---

## References

1. Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM.*
2. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
3. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography*. CRC Press.
4. Rosen, K. H. (2018). *Discrete Mathematics and Its Applications*. McGraw-Hill.
5. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. Springer.

6. Koblitz, N. (1994). *A Course in Number Theory and Cryptography*. Springer.
7. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*.
8. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2022). *Post-Quantum Cryptography*. Springer Nature.
9. Boneh, D., & Shoup, V. (2023). *A Graduate Course in Applied Cryptography.* Stanford University Press.
10. Alagic, G., et al. (2022). Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. *NIST Technical Report*.
11. NIST (2023). *Digital Signature Standard (DSS) and Public Key Cryptography Updates* National Institute of Standards and Technology.
12. Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2022). *Report on Post-Quantum Cryptography*. NISTIR Publication.
13. Buchmann, J., Dahmen, E., & Schneider, M. (2022). Post-Quantum Cryptography: State of the Art. *IEEE Security & Privacy*.
14. Aggarwal, D., Brennen, G., Lee, T., Santha, M., & Tomamichel, M. (2023). Quantum Attacks on Cryptographic Systems. *ACM Computing Surveys*.
15. Bernstein, D. J. (2024). Future Directions in Cryptographic Security. *Journal of Cryptographic Engineering*.
16. Goldreich, O. (2023). *Foundations of Cryptography – Modern Applications.* Cambridge University Press.
17. NIST (2024). *Post-Quantum Cryptography Standardization: Selected Algorithms.* National Institute of Standards and Technology.
18. Alkim, E., Bos, J., Ducas, L., Longa, P., Mironov, I., Naehrig, M., Nikolaenko, V., Peikert, C., Raghunathan, A., & Stebila, D. (2024). Post-Quantum Cryptography for Internet Security. *IEEE Communications Surveys & Tutorials*.