Research on the Basic Combination of Elementary Number Theory and Encryption Algorithm

Yejun Wu, Hongli Yang

Nanjing Institute of Technology, Nanjing, 211167, Jiangsu, China

wyj852507@sina.com, yanghongli1016@163.com

Keywords: Elementary Number Theory; Encryption Algorithm; Divisibility Theory; Congruence Theory; Number Theory Function

Abstract: With the development of information technology, information security has attracted much attention, and encryption algorithm is the key to ensure information security. This paper focuses on the basic integration of elementary number theory and encryption algorithm. This paper systematically analyzes the basic theories of divisibility, congruence and number theory functions in elementary number theory, and deeply interprets the basic principles of symmetric and asymmetric encryption algorithms and hash functions to study the application relationship between them. It is found that the theories of elementary number theory are widely used in many aspects such as key generation, encryption and decryption operation, data integrity verification and so on. For example, divisibility theory is used for key generation and data preprocessing, congruence theory is used to construct encryption operation logic, and number theory function is used to verify data integrity. Digging deeply into the application of elementary number theory in encryption algorithm can provide strong theoretical support for the optimization and innovation of encryption algorithm and promote the development of information security field.

1. Introduction

With the rapid development of information technology, information security has become the focus of attention, and encryption algorithm is the core technology to ensure information security [1]. Encryption algorithm ensures the confidentiality, integrity and availability of data in the process of transmission and storage through specific transformation of data [2]. As an ancient and basic subject in the field of mathematics, elementary number theory takes integer properties as the research object, and its rich theoretical achievements provide solid theoretical support for many disciplines [3]. Combining elementary number theory with encryption algorithm is of far-reaching significance to promote the development of encryption algorithm and enhance the ability of information security.

From the historical development, the early encryption technology was relatively simple. With the increasing demand for information security, the encryption algorithm became more and more complex, and people began to seek more solid mathematical theory to support the development of encryption technology [4]. Many theories in elementary number theory, such as divisibility theory, congruence theory and number theory function, provide rich mathematical tools for the design and analysis of encryption algorithms [5]. The core principle of the famous RSA encryption algorithm is based on the theory of large integer decomposition and congruence in elementary number theory. This fully demonstrates the important application value of elementary number theory in the field of encryption algorithm.

At present, with the wide application of emerging technologies such as cloud computing, big data and Internet of Things, information security is facing more severe challenges. Traditional encryption algorithms need to be constantly optimized and innovated to meet the new security requirements [6]. Under this background, it is particularly urgent to deeply study the basic integration of elementary number theory and encryption algorithm and tap the potential application of elementary number theory in encryption algorithm [7]. With the help of the theoretical

  DOI: 10.25236/icceme.2025.032

advantages of elementary number theory, the security and efficiency of encryption algorithm can be further improved. The development of encryption algorithm also provides a new application scene and research direction for the study of elementary number theory. The purpose of this study is to systematically analyze the basic theory of elementary number theory, deeply discuss its application in encryption algorithm, and contribute theoretical support to the development of information security field.

2. Theoretical analysis of elementary number theory

Elementary number theory mainly focuses on the properties of integers, and its basic theory is rich and diverse, which plays a key role in the construction of encryption algorithms [8]. Divisibility theory is one of the cornerstones of elementary number theory. There is a special relationship between integers. If the integer a is divided by the non-zero integer b, the quotient is an integer and the remainder is zero, then b is called divisible a, which is recorded as $b|a$. Divisibility has some basic properties, such as transitivity and additivity, which are helpful to construct a specific mathematical model for data processing and protection in the design of encryption algorithm. As an important extension of divisibility theory, division with remainder has unique integers q and r for any integer a and positive integer b, which makes:

$$a = bq + r \; 0 \le r < b \tag{1}$$

This representation provides an important basis for the grouping and processing of data in encryption algorithm.

Congruence theory also occupies an important position in elementary number theory. Given a positive integer m, if two integers a and b satisfy $m|(a-b)$, then a and b are said to be congruent with modular m, and recorded as:

$$a = b(\mathrm{mod}\, m) \tag{2}$$

Congruence class is a set of all integers that are modular m congruences, which provides a classification and mapping method for encryption algorithms. Congruence equation studies the solution of the equation that satisfies the specific congruence relation under the given modulus m, which has important application value for the key generation and decryption process in encryption algorithm.

Number theory function is also an important part of elementary number theory, which takes integers as independent variables and integers or real numbers as dependent variables. Common number theory functions, such as Euler function $\varphi(n)$, represent the number of positive integers less than or equal to n and coprime with n. The number theory function can be used to transform and verify data in encryption algorithm, and enhance the security and reliability of encryption algorithm.

3. Interpretation of the principle of encryption algorithm

3.1 Principle of symmetric encryption algorithm

Encryption algorithms are designed to protect the confidentiality, integrity and availability of information, and can be divided into symmetric encryption algorithms, asymmetric encryption algorithms and hash functions according to their characteristics and application scenarios. The principles of these algorithms are based on different mathematical concepts and calculation methods, and jointly build a defense line for information security.

Symmetric encryption algorithm uses the same key for encryption and decryption. Taking block cipher as an example, it divides plaintext into fixed-length blocks, and encrypts each block with the same encryption function and key. Common working modes of block cipher include electronic

codebook mode (ECB), cipher block linking mode (CBC), cipher feedback mode (CFB) and output feedback mode (OFB), as shown in Table 1:

Table 1: Comparison of Characteristics of Common Block Cipher Operating Modes

Operating Mode	Characteristics	Advantages	Disadvantages	Application Scenarios
ECB	Each plaintext block is encrypted independently, generating identical ciphertext blocks	Simple and efficient, easy for parallel processing	Identical plaintext results in identical ciphertext, vulnerable to attacks	Suitable for scenarios with short data and not extremely high security requirements
CBC	The previous ciphertext block participates in the encryption of the next plaintext block	Ciphertext blocks are interrelated, enhancing security	Cannot be processed in parallel; the initial vector needs to be kept confidential	Commonly used in general data encryption scenarios
CFB	The previous ciphertext block is encrypted and then XORed with the current plaintext block	Can handle data of any length and encrypt by bytes	Error propagation; security depends on the initial vector	Suitable for real-time data transmission encryption
OFB	A keystream is generated by continuously encrypting the initial vector and XORed with the plaintext	No error propagation; can be processed in parallel	Keystream generation depends on the initial vector	Suitable for encrypting data sensitive to errors.

The advantage of symmetric encryption algorithm lies in its fast encryption and decryption speed, which is suitable for processing a large number of data. However, it is difficult to manage the key, and both parties need to share the key in advance, and the number of keys increases exponentially with the number of communication parties.

3.2 Principle of asymmetric encryption algorithm

Asymmetric encryption algorithm uses a pair of keys, namely public key and private key. The public key is used for encryption and the private key is used for decryption. Taking RSA algorithm as an example, its principle is based on the problem of large integer decomposition. First, choose two big prime numbers p and q, and calculate:

$$n = pq, \varphi(n) = (p-1)(q-1) \quad (3)$$

Then, an integer e that is coprime with $\varphi(n)$ is selected as the public key, and then the private key d is calculated by the extended Euclidean algorithm, which satisfies the following requirements:

$$ed = 1(\mathrm{mod}\ \varphi(n)) \quad (4)$$

When encrypting, plaintext m is converted into ciphertext e through $e = m^e \bmod n$; When decrypting, the plaintext m is restored through $m = e^d \bmod n$. Asymmetric encryption algorithm solves the key distribution problem without sharing the key in advance. However, because it involves large integer operation, its encryption and decryption speed is relatively slow, and it is usually used in key exchange, digital signature and other scenarios.

3.3 Hash function principle

Hash function maps input data of arbitrary length to output value of fixed length, that is, hash value or message digest. Hash function has the characteristics of unidirectional, anti-collision and data integrity verification. Taking SHA-256 algorithm as an example, it performs a series of operations such as filling, dividing and compressing the input data, and finally generates a 256-bit hash value. Hash function is often used to verify the integrity of data. The sender calculates the hash value of the data and sends it with the data. The receiver recalculates the hash value of the received data and compares it with the hash value of the sender. If they are consistent, it means that the data has not been tampered with. Hash function plays an important role in the field of information security. For example, in password storage, the hash value of user password is stored instead of plaintext password to improve password security.

4. Application of elementary number theory in encryption algorithm

4.1 Application of divisibility theory in encryption algorithm

Many theories of elementary number theory are widely and deeply applied in encryption algorithm, which provide a solid mathematical foundation for the design, optimization and security guarantee of encryption algorithm. Some properties of divisibility theory are skillfully applied in many aspects of encryption algorithm, especially in key generation and data processing. For example, in some symmetric encryption algorithms, the value range and structure of the key are determined by using the property of divisibility to enhance the confidentiality of the key. By analyzing the divisibility of a specific integer set, the integers that meet specific conditions are selected as the components of the key. The key generated in this way not only satisfies certain mathematical laws, but also increases the difficulty for attackers to crack the key. In the data processing stage, divisibility theory can be used to group and preprocess plaintext data. According to the divisible relationship, plaintext data is divided into different parts, which makes the subsequent encryption operation more regular and secure.

4.2 Application of congruence theory in encryption algorithm

Table 2: Application Characteristics of Congruence Theory in Common Encryption Algorithms

Encryption Algorithm Name	Application Scenarios of Congruence Theory	Role of Congruence Operations	Impact on Algorithm Security
RSA Algorithm	Encryption and decryption processes	Enable the mutual conversion between plaintext and ciphertext	Security is guaranteed based on the difficulty of solving large integer congruence operations
ElGamal Algorithm	Key generation and encryption operations	Generate key pairs and encrypt data	Relies on the difficulty of the discrete logarithm problem under congruence operations
Diffie-Hellman Key Exchange Algorithm	Key exchange process	Calculate the shared key	Utilizes congruence operations to construct a shared key and prevent man-in-the-middle attacks

Congruence theory plays a core role in encryption algorithm, especially in the process of encryption and decryption. The operation logic of many encryption algorithms is based on congruence relation. Taking RSA algorithm as an example, its encryption and decryption processes use a lot of congruence operations. In encryption, plaintext m is transformed into ciphertext c through $e = m^e \bmod n$; When decrypting, the plaintext m is restored by $m = e^d \bmod n$, and the $\bmod$ operation here is the embodiment of the congruence operation. Congruence theory can also be used to design some special encryption transformations. For example, in some stream cipher

algorithms, the key stream is generated by congruence operation. The congruence equation is used to determine the parameters in the key stream generation process, which makes the generated key stream have good randomness and unpredictability. At the same time, congruence theory is also applied in the authentication and integrity check of encryption algorithms. A specific check value is obtained by congruence transformation of data, which is used to verify whether the data has been tampered with during transmission. The application features of congruence theory in common encryption algorithms are shown in Table 2.

4.3 Application of number theory function in encryption algorithm

Number theory function is mainly used in data integrity verification and authentication mechanism in encryption algorithm. Taking Euler function $\varphi(n)$ as an example, in RSA algorithm, the calculation of $\varphi(n)$ plays a key role in determining the private key d. Due to:

$$\varphi(n)=(p-1)(q-1) \tag{5}$$

p and q are two big prime numbers in RSA algorithm, and the private key d can be correctly calculated by calculating $\varphi(n)$ and using its relationship with public key e:

$$ed=1(\mathrm{mod}\,\varphi(n)) \tag{6}$$

In addition, some number theory functions can be used to generate pseudo-random number sequences as key streams or initial vectors in encryption algorithms. These number theory functions generate seemingly random number sequences through specific calculation methods, which provide necessary random factors for the encryption algorithm and enhance the security of the algorithm. In the aspect of data integrity verification, the number theory function is used to transform the data to get a unique identification value, which is similar to the hash function and is used to verify the integrity and authenticity of the data.

5. Conclusions

This paper focuses on the basic combination of elementary number theory and encryption algorithm, and discusses the relationship between them comprehensively and deeply. In the theoretical analysis part, the divisibility theory, congruence theory and number theory function of elementary number theory, as well as the principles of symmetric encryption, asymmetric encryption and hash function of encryption algorithm are expounded in detail. In the exploration of application connection, the important role of elementary number theory in each link of encryption algorithm is clarified. In the key generation and data preprocessing, divisibility theory uses its properties to screen keys and divide plaintext, which improves the confidentiality and regularity of encryption. Congruence theory occupies a core position in encryption and decryption operations, such as RSA algorithm, which is based on it to construct operational logic, and also plays an important role in authentication and integrity verification. Number theory function is indispensable in data integrity verification and authentication mechanism, such as Euler function plays a key role in the process of determining the private key of RSA algorithm, and can also be used to generate pseudo-random number sequences.

To sum up, the combination of elementary number theory and encryption algorithm is of great significance. Elementary number theory provides a powerful mathematical tool for encryption algorithm, improves the security and efficiency of encryption algorithm, and promotes its continuous optimization and innovation. Encryption algorithm provides a new application scene for elementary number theory, which promotes the continuous expansion of number theory research. With the continuous development of information technology, information security will face more challenges in the future. We should further study the combination of the two, explore the application under the background of emerging technologies, tap more potential value of elementary number theory in encryption algorithms, and inject new impetus into the development of

information security.

Acknowledgements

The authors acknowledge the Cross-Curriculum Project of "Jiebang Guashuai" (Open Bidding for Key Projects) at Tianyinhu Institute of Science and Technology Innovation, Nanjing Institute of Technology:“The Topic of University Mathematics and Physics Comprehensive Course” (NO:2025TKJA01).

References

[1] Y. T. Yang, J. P. Cao, L. Y. Chen, et al. Efficient Implementation of BFV Fully Homomorphic Encryption Algorithm Based on Zynq Platform[J]. Journal of Communications, 2024, 45(9): 192-205.

[2] S. L. Hua, H. G. Zhang, S. C. Wang. Optimization and Implementation of Number Theoretic Transform Multiplication Butterfly Operation for Fully Homomorphic Encryption[J]. Journal of Electronics & Information Technology, 2021, 43(5): 1381-1388.

[3] B. L. Yang, F. Zhang, Y. L. Zhao, et al. Fault Attack Against AKCN-MLWE Algorithm[J]. Chinese Journal of Computers, 2023, 46(7): 1396-1408.

[4] Z. X. Tu, X. L. Wang, G. M. Du, et al. FPGA Design and Implementation of High-Speed Pipeline Structured Large Integer Multiplier[J]. Microelectronics, 2022, 52(1): 6-11.

[5] D. W. Lei, D. B. He, M. Luo, et al. High-Speed Parallel Implementation of Lattice-Based Cryptography Based on AVX512[J]. Computer Engineering, 2024, 50(2): 15-24.

[6] H. J. Li, Y. Q. He. Integer Formulas for the Sum of Reciprocals of Cubes of Odd and Even Terms in Fibonacci Sequence[J]. Acta Mathematica Sinica, 2024, 67(5): 926-938.

[7] Y. H. Sun, T. J. Yan, J. M. Zhang. Application of Euclidean Algorithm in Cryptanalysis[J]. Mathematics in Practice and Theory, 2020, 50(21): 286-290.

[8] M. L. Zhang, L. Gao. Solvability of a Ternary Variable Coefficient Euler Function Equation with Constant Term[J]. Henan Science, 2020, 38(3): 351-355.