Journal of Electronic Research and Application, 2025, Volume 9, Issue 2
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

A Brief Discussion on Data Encryption and Decryption Technology and Its Applications

Zhihong Jin*

The 22nd Research Institute of China Electronics Technology Group Corporation,Xinxiang 453000, Henan Province, China

***Corresponding author:** Zhihong Jin, 81984088@163.com

Abstract: With the rapid development of information technology, data security issues have received increasing attention. Data encryption and decryption technology, as a key means of ensuring data security, plays an important role in multiple fields such as communication security, data storage, and data recovery. This article explores the fundamental principles and interrelationships of data encryption and decryption, examines the strengths, weaknesses, and applicability of symmetric, asymmetric, and hybrid encryption algorithms, and introduces key application scenarios for data encryption and decryption technology. It examines the challenges and corresponding countermeasures related to encryption algorithm security, key management, and encryption-decryption performance. Finally, it analyzes the development trends and future prospects of data encryption and decryption technology. This article provides a systematic understanding of data encryption and decryption techniques, which has good reference value for software designers.

Keywords: Data encryption; Data decryption; Communication security; Data storage encryption; Key management

Online publication: March 28, 2025

1. Introduction

In today's digital age, strengthening the security management of computer data information and enhancing data encryption technology have profound significance for ensuring the security of data information in the entire society [1]. Data encryption and decryption technology has received widespread attention and research worldwide. In developed countries such as the United States, data encryption technology started early and has become relatively mature, widely used in multiple fields. On the basis of researching existing database encryption technologies, some scholars have designed and implemented an encryption system for specific information systems using the Java platform. These studies have made important contributions to the development of data encryption technology. This article explores the principles, applications, and challenges of data encryption and decryption technology in depth and proposes effective response strategies. It is expected to make beneficial contributions to the development of data security, with theoretical guidance and international application value.

2. Overview of data encryption and decryption technologies

2.1. Principles of data encryption technology

The basic principle of data encryption technology is to convert raw plaintext data into difficult to understand ciphertext data through specific algorithms and keys. The purpose of data encryption is to prevent unauthorized data access and data leakage. Data encryption technology can be divided into two categories based on whether the encryption and decryption keys used are the same: symmetric encryption algorithms and asymmetric encryption algorithms. The encryption process involves complex mathematical operations and key extension to ensure the confidentiality and integrity of data [2]. Chaos encryption, as an emerging encryption method, utilizes the characteristics of chaotic systems to generate complex chaotic sequences for encrypting and scrambling data. This method has good security performance and brings new ideas and methods to the field of data encryption.

2.2. Principles of data decryption technology

Data decryption technology is the inverse operation of data encryption, which is the process of restoring ciphertext data to original plaintext data through specific algorithms and the same or associated keys. The encryption process is a process of restoring data through complex mathematical calculations and the core of decryption technology lies in the management of keys and the selection of algorithms. In practical applications, data decryption technology is often combined with various security protocols and mechanisms to ensure the integrity and authenticity of data. In digital signature technology, decryption techniques are used to verify the validity of signatures, thereby confirming the source and unaltered state of data.

2.3. The relationship between data encryption and decryption

Data encryption and decryption are two core components of data security protection. Without the decryption process, encrypted data will become unusable and lose its original value. Similarly, without encryption, the security of data cannot be guaranteed, and there is a risk of theft or tampering. Therefore, data encryption and decryption are two interdependent and mutually reinforcing links, playing an indispensable role in the field of data security [3].

In practical applications, data encryption and decryption techniques need to be selected according to specific scenarios. With the continuous development of technology, data encryption and decryption methods are also constantly innovating and optimizing. Currently, the data encryption and decryption methods of collaborative cognitive models combine the basic principles of data encryption and decryption with those of collaborative cognitive models, providing a simple, secure, and reliable method for data encryption and decryption.

3. Classification of data encryption and decryption technologies

3.1. Symmetric encryption algorithm

Symmetric encryption algorithm uses the same key in the encryption and decryption process, with fast encryption and decryption calculation speed, which can meet the requirements of large-scale data processing or high real-time applications.

The Advanced Encryption Standard (AES) algorithm is the most typical symmetric encryption algorithm. The AES algorithm offers multiple key length options, including 128-bit, 192-bit, and 256-bit, to meet the needs of different security levels. As the key length increases, the security of the algorithm also improves accordingly, enabling AES to provide strong protection in various security-sensitive applications. The AES algorithm is

lightweight and highly flexible, making it easy to deploy and implement on different platforms and environments.

The most prominent problem faced by symmetric encryption algorithms is key management. Due to the use of the same key for encryption and decryption, once the key is leaked, the security of the entire encryption system will be seriously threatened. Therefore, in practical applications, how to securely and effectively manage and distribute keys has become a major challenge in the implementation of symmetric encryption algorithms. At the same time, secure key exchange protocols and regular key replacement can be used to increase the security of system data exchange.

In addition to AES, the Data Encryption Standard (DES) algorithm, as an earlier symmetric encryption algorithm, can still have certain application value in scenarios that require high performance but less strict security requirements. In addition, there are some symmetric encryption algorithms for specific application scenarios, such as stream encryption algorithms, block encryption algorithms, etc., which play important roles in their respective application fields.

3.2. Asymmetric encryption algorithm

Asymmetric encryption algorithms use a pair of public and private key mechanisms, with the public key used for data encryption and the private key used for data decryption, bringing revolutionary changes to the field of data security. This algorithm not only provides high-strength security but also solves the problem of key distribution in symmetric encryption algorithms. In asymmetric encryption algorithms, the public key is public and anyone can use it for data encryption, but decryption requires the use of the corresponding private key, which greatly enhances the security of the data.

The RSA algorithm, as a representative of asymmetric encryption algorithms, has attracted much attention since its inception. It is based on the mathematical problem of large number decomposition, and generates a public key and a private key by multiplying two large prime numbers, ensuring its security. In the RSA algorithm, the encryption process uses a public key, while the decryption process uses a private key. By using this method, even if the data is illegally intercepted during transmission, the interceptor cannot easily decrypt it, thus protecting the security of the data.

In addition to RSA algorithm, elliptic curve cryptography (ECC) algorithm is also a highly regarded asymmetric encryption algorithm in recent years. Compared to RSA, ECC requires shorter key lengths while providing the same level of security, which means faster and more efficient encryption and decryption. The ECC algorithm is based on the mathematical theory of elliptic curves and achieves secure encryption and decryption of data by selecting points on the elliptic curve as public and private keys.

The advantages of asymmetric encryption algorithms are high-strength security and flexible key management mechanisms, but the disadvantages are relatively slow encryption and decryption computation speed and complex private key storage. Therefore, in practical applications, asymmetric encryption algorithms are often combined with other encryption techniques to fully leverage their respective advantages and ensure data security.

3.3. Hybrid encryption algorithm

Hybrid encryption algorithm is a technology that combines the advantages of symmetric and asymmetric encryption algorithms, aiming to find the best balance between encryption efficiency and security. In this algorithm, asymmetric encryption algorithm is not directly used to encrypt large amounts of data but is used to encrypt the key of symmetric encryption algorithm.

The workflow of hybrid encryption algorithm is as follows: Firstly, the sender and receiver will each generate a pair of public and private keys for asymmetric encryption algorithm. The sender will use the receiver's public key to encrypt the key of the symmetric encryption algorithm, so even if the data is intercepted during transmission, the key of the symmetric encryption algorithm cannot be directly obtained. Then, the sender uses the key of this symmetric encryption algorithm to encrypt the actual data to be transmitted. Finally, after receiving the encrypted data and key, the recipient will use their own private key to decrypt the key and then use the borrowed key to decrypt the actual data to be transmitted.

The hybrid encryption algorithm combines the efficiency of symmetric encryption algorithms with the security of asymmetric encryption algorithms. Moreover, since the key of symmetric encryption algorithm is randomly generated and a new key is changed every time encryption is performed, even if a certain encryption is cracked, it will not affect the security of other data.

Common hybrid encryption algorithms include encryption algorithms in TLS/SSL protocols. These algorithms have been widely applied in network communication, providing strong guarantees for the secure transmission of data. In scenarios such as web browsing, email, and online shopping, hybrid encryption algorithms silently protect our data security.

4. Typical applications of data encryption and decryption technology

4.1. Application of data encryption in communication security

In terms of network communication, in addition to the application of HTTPS protocol and VPN technology, data encryption is also widely used in tools such as email and instant messaging to ensure that email content and chat records are not stolen or tampered with by third parties, thereby protecting users' privacy and information security. Data encryption is also commonly used to protect the security of network devices and servers such as firewalls, preventing hacker intrusion and data leakage.

In terms of mobile communication, data encryption is applied to sensitive information of mobile phone users such as bank transfers, shopping payments, etc., to prevent information from being easily stolen. In satellite communication, the use of data encryption technology can ensure that data in satellite communication is not stolen or tampered with, thereby ensuring the security and reliability of communication.

In short, the application of data encryption in communication security is comprehensive, involving various communication methods and scenarios. By using data encryption technology, users' privacy and information security can be effectively protected, preventing data leakage and theft.

4.2. Application of data encryption in data storage

In terms of database encryption, using symmetric encryption algorithms such as AES can encrypt sensitive data in the database, ensuring that even if the database files are illegally obtained, attackers will have difficulty directly reading the plaintext data.

Data encryption in cloud storage has also been a research hotspot in recent years. Through encryption technology, users can encrypt their data before uploading it and then store the encrypted data in the cloud. This can effectively protect cloud data from being accessed by illegal malicious users.

With the continuous development of technology, some emerging data encryption technologies are gradually being applied in the field of data storage. For example, attribute based encryption algorithms (ABE) can control

data access permissions based on the attributes of the data, thereby achieving finer grained data protection. Homomorphic encryption algorithms allow for computation and processing of data without decryption, providing a new solution for data privacy protection in scenarios such as cloud computing.

4.3. Application of data decryption in data recovery

In the process of data backup, encryption technology is usually used to process the backup data in order to ensure its security. After data backup, even if the backup data is illegally obtained, the data content cannot be directly read. At the same time, when data is lost or damaged due to hardware failures, software errors, human error, and other reasons, we need to rely on data decryption technology to recover the loss as much as possible.

The application of data decryption in data recovery is not limited to traditional local data recovery scenarios. In the era of cloud computing and big data, more and more data is being stored in the cloud or on remote servers. In this case, data backup and recovery often require crossing different physical locations and network environments. Therefore, data decryption technology also needs to adapt to this distributed and heterogeneous environment to ensure the security, integrity, and availability of data.

5. Challenges and countermeasures faced by data encryption and decryption technologies

5.1. Security issues of encryption algorithms

In recent years, with the rapid improvement of computing power and the deepening of cryptographic research, some classic encryption algorithms such as DES have been proven to have security risks and have even been successfully cracked, posing huge challenges to data encryption and decryption technology.

To address this challenge, cryptographers and computer scientists are constantly innovating and developing more secure and efficient encryption algorithms. For example, the AES algorithm, as an alternative to DES, provides higher security and encryption strength. Meanwhile, asymmetric encryption algorithms such as RSA and ECC also provide higher security for data encryption due to their unique public-private key mechanisms.

Relying solely on updating encryption algorithms is not enough to completely solve security issues. We need to establish a continuous encryption evaluation mechanism to conduct regular security assessments and vulnerability scans of encryption algorithms, promptly identify and address potential security risks, and ensure the security of encryption algorithms.

5.2. Key management issues

Key management is crucial in data encryption and decryption. Once the key is leaked or illegally obtained, the security of the entire encryption system will be seriously threatened.

The generation of keys must follow strict security standards, which typically involve using strong random number generators to generate sufficiently complex and unpredictable keys. The storage of keys also requires careful handling. Keys need to be stored in a secure device environment to prevent unauthorized access and ensure their physical security. The distribution of keys uses secure communication protocols such as SSL/TLS to encrypt the transmission keys. The key needs to be updated regularly, and leaked keys should be promptly revoked and replaced with new keys.

In addition to technical measures, strengthen the training and management of key management personnel, fully understand the importance of key management and related operating procedures, to ensure that management

personnel will not inadvertently leak keys or engage in improper operations.

5.3. Encryption and decryption performance issues

The performance issues of encryption and decryption are not only related to the efficiency of data processing and transmission, especially when dealing with large-scale data, which can seriously affect user experience and may also have a negative impact on the operational efficiency of enterprises. The following measures can be taken to optimize the performance of encryption and decryption calculations. Firstly, the efficiency of encryption and decryption operations can be improved by utilizing specialized hardware accelerators such as encryption cards or TPUs.

Secondly, optimizing encryption algorithms is also key to improving performance. On the one hand, algorithm-level optimization can be used to adopt more efficient mathematical operation methods, optimize lookup tables, etc., reducing the computational load during encryption and decryption processes. On the other hand, suitable encryption algorithms can be selected based on the application scenario to reduce unnecessary computation.

Finally, adopting a hierarchical encryption strategy to reduce computational overhead. High strength encryption is used for important data, while lower strength encryption is used for non-sensitive data. This can ensure data security while reducing the overall computational cost of encryption and decryption.

6. Development trends and prospects

Data encryption and decryption technology, as key technologies for information security, are systematically elaborated in this article. With the continuous advancement of information technology, data encryption and decryption techniques are also evolving, showing some new development trends:

(1) With the rise of quantum computing and the application of computational complexity theory, traditional encryption algorithms are facing unprecedented challenges and encryption algorithms will develop towards higher security and greater complexity.

(2) With the development of artificial intelligence and blockchain technology, key management will achieve higher levels of automation and intelligence.

(3) With the popularization of technologies such as cloud computing, big data, and the Internet of Things, the processing speed and data throughput of data encryption and decryption have become key performance indicators.

(4) Data encryption and decryption technology is expected to deeply integrate with cutting-edge technologies such as artificial intelligence, blockchain, and cloud computing.

(5) Governments and industry organizations around the world are increasingly concerned about data security issues, and data encryption and decryption technologies will inevitably move towards standardization and legalization.

Through continuous research and innovation, we look forward to developing more efficient, secure, and intelligent data encryption and decryption technology solutions, providing a more solid guarantee for information security.

Disclosure statement

The author declares no conflict of interest.

References

[1] Ping H, 2022, Network Information Security Data Protection Based on Data Encryption Technology. Wireless Personal Communications, 126(3): 2719–2729.

[2] Liu GX, 2022, The Application of Data Encryption Technology in Computer Network Communication Security. Mobile Information Systems, 2022(5): 1–10.

[3] Logofatu PC, Udrea C, Garoi F, 2024, Physical Encryption-Compression and Decryption-Decompression of Data Using the Fourier Transform. Romanian Reports in Physics, 76(1): 1–12.