Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 5
AIDML 2024

# Employing Cryptographic Techniques for Data Security and Privacy Preservation

Honghao Liu

Beijing-Dublin International College at BJUT, Beijing University of Technology, Beijing, China

1707050218@stu.hrbust.edu.cn

**Abstract.** This scholarly discourse delineates the foundational principles and prevalent algorithms underpinning information encryption technology, illuminating its critical role in fortifying information security through the lenses of data protection and privacy safeguarding. Encryption technology serves as a stalwart guardian of data confidentiality, integrity, and availability, undergirding the secure and robust functioning of digital networks and systems. As the landscape of cyber threats undergoes relentless transformation, the mandate for the advancement of encryption methodologies becomes ever more pressing. The perpetual refinement and evolution of cryptographic practices are imperative to surmount the increasingly intricate challenges posed by sophisticated cyber adversaries. In an era where data breaches and privacy incursions are rampant, encryption acts as the sine qua non of digital security strategies. It not only obfuscates sensitive information from unauthorized viewers but also ensures that even if data is intercepted, it remains an indecipherable enigma to the interloper. Furthermore, encryption technologies underpin trust in the burgeoning realms of e-commerce and online communication, where they authenticate transactional exchanges and preserve the sanctity of digital interactions.

**Keywords:** information security; information encryption; data protection; privacy protection.

## 1. Introduction

The trajectory of information security technology is fraught with inherent risks, encompassing data loss or alteration, unauthorized intrusions, the proliferation of malware, hacker assaults, unsecured network connections, and vulnerabilities to physical breaches. A user's laxity in security practices and inattentiveness to cybersecurity measures can lead to an exposure of critical information loopholes, rendering them susceptible to hacker exploitation. Such breaches pose significant threats to information security, precipitating not only economic damages but also the compromise of sensitive personal data [1].

In the corporate realm, the implications of information security transgressions are profound, potentially culminating in the divulgence of pivotal corporate data. This not only hampers the trajectory of business growth but also inflicts substantial financial repercussions. On a national scale, breaches in information security can strike a devastating blow to the political, economic, and defense sectors. As such, the paper contends that a comprehensive and vigilant approach to information security is indispensable. This encompasses fostering robust security protocols, ensuring vigilant monitoring systems, and advocating for heightened user awareness and education. It is only through a concerted effort that encompasses these multifaceted strategies that the bulwark against the ever-evolving threats to information security can be reinforced, safeguarding the interests of individuals, enterprises, and nations alike.

## 2. The basic principles of information encryption technology

### 2.1. Symmetric encryption algorithm

Symmetric cryptography, also termed secret-key cryptography, is a well-established encryption technique characterized by its use of a singular key for both encryption and decryption processes. This method of cryptography processes plaintext alongside a key through a specialized algorithm,

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

culminating in the generation of ciphertext that possesses enhanced security and robustness. The sender of the data utilizes this method to transmit encrypted information to the receiver securely. Among the pantheon of symmetric encryption algorithms, DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm) have gained widespread adoption. However, AES (Advanced Encryption Standard), endorsed by the National Institute of Standards and Technology (NIST), is poised to supplant DES as the new encryption benchmark. A notable instance of a symmetric encryption protocol is the DES algorithm, which undergoes 16 rounds of complex transformations. The resultant outputs after these iterations are denoted as L16 and R16, which subsequently serve as inputs for the final stages of the encryption process. The mechanism of the DES data encryption algorithm is visually depicted in Figure 1, as indicated.

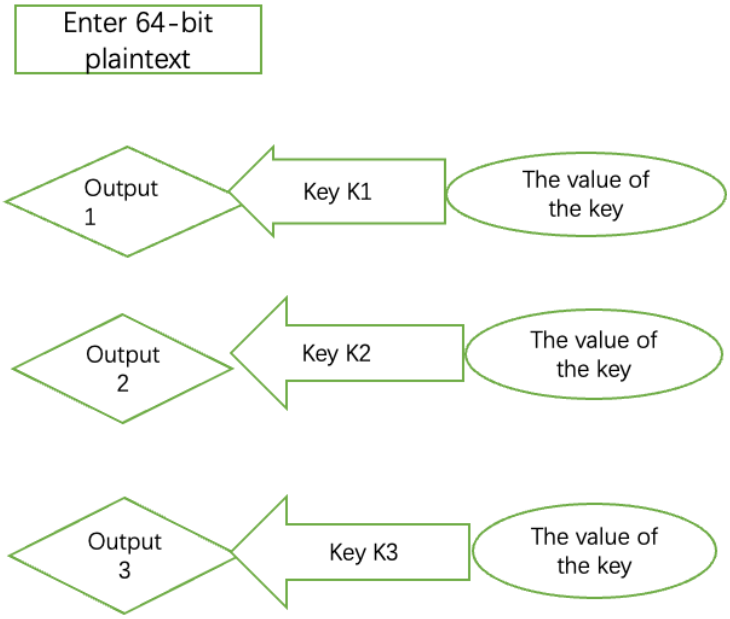


**Fig. 1** Schematic diagram of DES data encryption algorithm (Photo/Picture credit: Original).

The merits of symmetric encryption algorithms lie in their minimal computational demand, swift encryption speeds, and high efficiency in encrypting data. These algorithms become particularly robust against cryptographic attacks when deployed with extended key lengths. However, symmetric encryption also presents notable challenges. Since both parties involved in a transaction utilize the same keys, guaranteeing the security of the transaction can be problematic. Additionally, the management of these keys poses a significant challenge, often complicating the overall security protocol [2, 3].

### 2.2. Asymmetric encryption algorithms

In the realm of encryption, once a key is employed for encrypting data, only the corresponding decryption key held by the user can revert the data to its original form. This principle ensures that the exposure of one key pair does not compromise the confidentiality of another. In asymmetric encryption, the term "private key" denotes a key kept confidential, in contrast to the "public key" which is openly disseminated. Asymmetric encryption techniques, such as RSA (Rivest-Shamir-Adleman), ElGamal, and Elliptic Curve Cryptography (ECC), exemplify this methodology. A prominent algorithm within asymmetric cryptography is the RSA algorithm [5], which we shall now elucidate.

### 2.3. Hashing Algorithms

Hashing algorithms map data of any size to a hash of fixed length, typically expressed in hexadecimal format. These algorithms, essentially mathematical functions, transform input data (termed a "message") into a fixed-length string, known as a "hash" or "digest." This hash acts as a unique, irreversible identifier for the original message. Pervasive in realms like data security, compression,

and retrieval, hashing algorithms commence by dividing the input data into several blocks, either of equal or varying lengths, each referred to as a message block. Subsequently, each block undergoes a series of operations - including bitwise manipulation, shifts, modulo operations, and XOR processes - to generate an intermediate result termed a message digest [6]. The final hash output is then crafted by amalgamating or recalculating these individual message digests.

### 2.4. Digital Signatures

Digital signatures employ a series of unique numerical strings, akin to a robust evidence of a message's authenticity, much like a conventional handwritten signature on paper. Utilizing the principles of public key cryptography, digital signatures provide a mechanism for the identification of digital information. They typically encompass two complementary operations: signature creation and subsequent verification. At the heart of digital signatures lie asymmetric key cryptography and digital digest technology. When a message is authenticated using the sender's public key, it unequivocally establishes the sender as the original source. The process involves the sender encrypting the message with their private key, which is exclusively accessible to them, thereby rendering the signature unforgeable by others. This digital signature, essentially a sequence of numbers, can be seamlessly transmitted across networks to the recipient. It serves as a potent tool to ensure the integrity, authenticity, and non-repudiation of the message. In practical applications, digital signature technology is integral to various significant protocols and systems, playing a pivotal role in bolstering communication security [7].

## 3. Application of information encryption technology

### 3.1. The role of information encryption technology in data protection

The primary application of information encryption technology lies in data encryption. Digital signatures and checksums are two mechanisms through which encryption technology detects data alterations. In instances of data tampering, the discrepancy between the encrypted checksum and the original data serves as a timely indicator, ensuring data integrity [8]. Information encryption technology is instrumental in verifying that no data alteration or destruction has occurred, whether in storage or transit. Serving as the cornerstone of integrity protection, information encryption technology encompasses methods like Message Authentication Codes (MACs) and hash functions. To safeguard data against alterations during transmission, the sender may employ a digital signature on the outgoing information. Upon receipt, the recipient can use this digital signature to verify the data's integrity. Protocols such as RSA and SSL are prevalent in ensuring data confidentiality, affirming that the data remains unaltered in transit [9]. Additionally, encryption technology enhances the tamper-evident capabilities of data. Should tampering occur, it can be promptly detected, enabling the timely implementation of remedial measures.

Data sharing with third parties constitutes a critical phase in data protection. Varied profit models incentivize third-party participation, amplifying the frequency and scope of data circulation. This increased circulation, however, also presents opportunities for hackers to exploit vulnerabilities and launch attacks, leading to novel data security challenges [10]. Third parties often gain direct access to sensitive user information, such as location, browsing history, photo albums, and contact lists, via apps. A user's refusal to share this information can lead to a conflict between data sharing and data protection. Thus, a synergistic approach combining third-party data transparency with robust data protection technology is essential. Building user trust in third parties and reinforcing data protection technology will significantly enhance the effectiveness and resilience of data protection measures.

### 3.2. The role of information encryption technology in privacy protection

Information encryption technology plays an indispensable role in safeguarding privacy. By encrypting sensitive data, personal privacy, corporate secrets, and government information can be shielded from unauthorized access and theft. Individual privacy is particularly vulnerable, as personal

data can fall prey to hackers or identity thieves who may exploit it for fraud, identity theft, and other malicious purposes [11,12]. Encryption renders personal information inaccessible to attackers, thereby bolstering user privacy and security.

In the corporate sphere, encryption is crucial for protecting confidential information. Large corporations and organizations possess a plethora of sensitive data, including financial records, marketing strategies, and research and development outcomes. Exposure of such information to competitors or cybercriminals can inflict severe harm on a company's interests. Data encryption ensures that this critical information remains accessible only to authorized individuals, thus safeguarding corporate business interests [14].

Furthermore, encryption is vital for national security. In an era where cyber threats are increasingly sophisticated, encryption acts as a bulwark against hackers, terrorists, and other malevolent entities. By securing sensitive data, it prevents these adversaries from accessing information that could jeopardize national security, playing a crucial role in defending a nation's interests [15].

## 4. Conclusion

In an era where cyber threats morph with unnerving velocity, the imperative for continuous exploration and innovation in information security technologies cannot be overstated. To keep pace with these evolving challenges, future research must pivot towards optimizing extant methodologies and probing the potential of these technologies in novel domains. Concurrently, there is a compelling need to translate theoretical advancements into practical applications, thereby bolstering our defensive capabilities against information security breaches. The quintessence of information technology in safeguarding digital realms is irrefutable. It is incumbent upon us to delve deeper and leverage these technologies to their fullest extent to counteract the sophisticated and multifaceted nature of modern cyber threats. As we navigate through the complexities of this digital age, a concerted effort to refine and apply encryption algorithms, enhance data anonymization protocols, and develop cutting-edge cryptographic defenses is paramount. This will not only strengthen our information security infrastructure but also foster a safer cyberspace ecosystem.

## References


[1] Li, L. (2022). Application of Data Encryption Technology in Computer Network Information Security. Security and Communication Networks, 2022.

[2] Zhang, H. (2022). Application of Information Encryption Technology in Computer Network Communication Security. Wireless Communications and Mobile Computing, 2022.

[3] Weissbaum, F., & Lugrin, T. (2023). Symmetric Cryptography. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in Data Protection and Encryption Technologies. Cham: Springer.

[4] Stohrer, C., & Lugrin, T. (2023). Asymmetric Encryption. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in Data Protection and Encryption Technologies. Cham: Springer.

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

[6] Wagner, U., & Lugrin, T. (2023). Hash Functions. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in Data Protection and Encryption Technologies. Cham: Springer.

[7] Lin, W. (2023). Digital Signature. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in Data Protection and Encryption Technologies. Cham: Springer.

[8] Wang, Y. (2023). On the Application of Data Encryption Technology in Computer Network Security. Computer Programming Skills and Maintenance, 2023(10), 166-169.

[9] Renuka Devi, K., Nithyapriya, S., Pradeep, G., Menaha, R., & Suganyadevi, S. (2023). Securing Shared Data Based on Homomorphic Encryption Schemes. In V. Seethalakshmi, R.K. Dhanaraj, S. Suganyadevi, & M. Ouaissa (Eds.), Homomorphic Encryption for Financial Cryptography. Cham: Springer.

[10] Xu, J., & Luo, Y. (2023). Construction of personal data protection obligations of enterprises in third-party data sharing. Science & Technology and Law, 2023(04), 32-42.

[11] Gasser, L., & Hubaux, J. P. (2023). Blockchain. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in Data Protection and Encryption Technologies. Cham: Springer.

[12] Hannah, K. J., Ball, M. J., & Edwards, M. J. (2006). Data Protection. In Introduction to Nursing Informatics (Health Informatics). New York, NY: Springer.

[13] Huang, L., & Shen, Q. (2021). Application of Computer Network Security Data Encryption Technology. In J. W. Chang, N. Yen, & J. C. Hung (Eds.), Frontier Computing (FC 2020. Lecture Notes in Electrical Engineering, vol 747). Singapore: Springer.

[14] Wu, Y. (2023). Application of Data Encryption Technology in Computer Software Testing. In I. Ahmad, J. Ye, & W. Liu (Eds.), The 2021 International Conference on Smart Technologies and Systems for Internet of Things (STSIoT 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 122). Singapore: Springer.

[15] Jiang, L. (2021). The Application Analysis of Computer Network Security Data Encryption Technology. In J. Abawajy, K. K. Choo, Z. Xu, & M. Atiquzzaman (Eds.), 2020 International Conference on Applications and Techniques in Cyber Intelligence (ATCI 2020. Advances in Intelligent Systems and Computing, vol 1244). Cham: Springer.