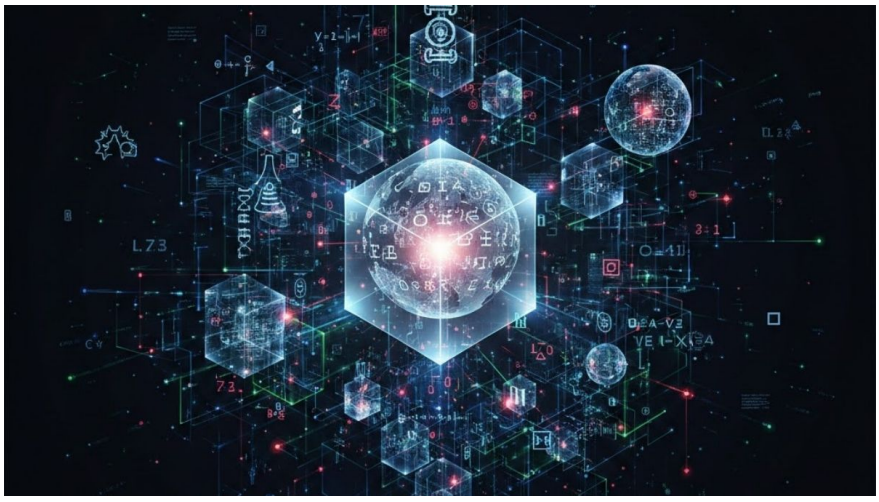
What is data encryption? Principles and practical applications.

This article explains what data encryption is in information technology. It explores the principles of encryption and their applications in banking and businesses.

What is data encryption? This is a question that many people are interested in. Understanding this concept is crucial in the face of increasing cybersecurity threats. Let's explore how this method works and its practical applications.

What is data encryption?

Encryption is the process of converting original information (plaintext) into other, unreadable data (ciphertext) using algorithms and a key. Only with the corresponding decryption key can you restore the information to its original form so that it can be read.



Explain the concept of data encryption.

Data in a computer is encoded as a sequence of bits because the device can only process binary signals, 0s and 1s. Thanks to this process, even if the information is stolen, the thief will only obtain a meaningless string of characters without the decryption key.

For example, a seller might need to encrypt a buyer's payment information, such as account number and name, into a meaningless string of characters. This would prevent a hacker from accessing the sales system and viewing the customer's payment information.

Nowadays, most modern computers have built-in hard drive encryption technology to protect user data. Upgrade to a new computer to store your information with peace of mind and without worrying about security risks.

How does data encryption work?

To understand what data encryption is, we need to know how it works. An encryption process will require the following core components:

1. **Input data (Plaintext)** : The original information that needs to be protected (text, images, files).
2. **Algorithm** : Using an algorithm (e.g., AES, RSA, etc.) to transform data.
3. **Key** : A special string of characters fed into an algorithm to scramble information.
4. **Ciphertext** : The result after applying the algorithm and key.
5. **Decryption** : When a legitimate party receives the data, they use the decryption key to reverse the process, returning the encrypted text to its original plaintext.

Depending on the system, encryption methods may vary, but the general principle remains the same: transforming information into a form that cannot be read without the key. This is the foundation of modern data security methods.

Why is data encryption necessary?

Now that you understand what data encryption is, you're probably wondering about its role in information security. Here are some reasons why this technology is essential for both individuals and businesses:

1. **Privacy protection** : Ensure that your messages, emails, and personal records are not intercepted by third parties.
2. **Compliance with regulations** : Many international standards require businesses to encrypt customer data in order to operate legally.
3. **Ensuring integrity** : Encryption combined with MAC addresses helps detect whether data has been tampered with during transmission.

Common types of data encryption currently in use

In fact, there are many different data encryption methods applied in specific fields. The following are the characteristics of four main types:

Symmetric data encryption

This method uses a single key shared by both the sender and the receiver. Its advantage lies in its high efficiency, making it suitable for encrypting large volumes of data. However, the biggest challenge is securely sharing the key between the two parties.

Asymmetric data encryption

Unlike symmetrical encryption, this method operates based on a pair of linked keys: one key for encryption and one key for decryption. This separation enhances security, allowing one key to be publicly disclosed while keeping the other confidential. As a result, this method is widely used in online transactions, digital signatures, and electronic authentication systems.

One-way data encryption

This is an irreversible conversion (hashing). After conversion, the original content cannot be recovered from the hash value. This method is often used to check file integrity or store passwords, as the system only needs to compare whether the two hash values ??match.

Classical data encryption

These are early data encryption methods such as Caesar cipher (letter shift) or Vigenère cipher. Although classical data encryption is no longer secure enough today, they still serve as an important foundation for the development of more complex algorithms later on.

Common data encryption algorithms

Each encryption algorithm has its own characteristics in terms of speed, security, and scope of application. Here are the characteristics of some of the most common algorithms:

1. **AES (Advanced Encryption Standard)** : The current strong symmetric encryption standard, trusted by the US government.
2. **RSA (Rivest-Shamir-Adleman)** : A classic asymmetric encryption algorithm used in online transactions.
3. **DES (Data Encryption Standard)** : An older algorithm, now replaced by AES due to its low security.
4. **Triple DES (3DES)** : An upgraded variant of DES that applies the algorithm three times.
5. **Blowfish** : A fast, symmetric algorithm that replaces DES.
6. **Twofish** : The successor to Blowfish, supporting keys up to 256 bits.
7. **ECC (Elliptic Curve Cryptography)** : Elliptic curve-based encryption, highly efficient with short keys.

Which type of data encryption should be used in each case?

Choosing the right data encryption methods will optimize security and system performance. Below are suggestions for selecting the appropriate encryption type for different purposes:

1. **Symmetric encryption (AES)** : Used when processing large amounts of data at high speed (backup, internal storage).
2. **Use asymmetric encryption (RSA, ECC)** : When secure information exchange over the internet is required with partners, customers, or for digital signatures.
3. **One-way encryption (SHA-256)** : Used when storing passwords or checking data integrity.
4. **Using classical encryption** : This should only be applied for academic purposes, cryptographic history research, or entertainment; not for use with real-world data.
5. **Combining symmetric and asymmetric encryption** : In complex cases such as website security, VPNs, or high-security data transmission.

Current practical applications of data encryption.

In daily life, data encryption is no longer a distant theory but is present in every digital activity. The following are some practical applications of encryption technology:

1. **Secure browsing (HTTPS)** : When you see a padlock icon in your browser, the data between you and the website has been encrypted.
2. **Messaging apps (End-to-End Encryption)** : Zalo, Telegram, etc., use end-to-end encryption.

3. **Online payments** : Bank card information and OTPs are always encrypted extremely strictly using PCI DSS standards.
4. **Cloud storage:** Google Drive and iCloud encrypt your data before storing it on their servers.
5. **Digital signatures and electronic invoices** : Ensuring legal validity and preventing forgery of documents in administrative and business transactions.

Standards and regulations related to data encryption

To ensure consistency and information security, international organizations and governments have issued mandatory standards. A prime example is AES (Advanced Encryption Standard). This algorithm, approved by the National Institute of Standards and Technology (NIST) of the United States, is now a widely used encryption standard globally.

In addition, financial institutions are often required to meet FIPS 140-2/140-3 – regulations specifying security requirements for cryptographic modules. In Vietnam, civilian cryptographic devices also need to comply with national technical standards such as QCVN 15:2023/BQP to ensure national information security.

Challenges and limitations of data encryption

Although the benefits of data encryption are clear, the process still faces technical hurdles:

1. **Key Management** : If the decryption key is lost, the data will be permanently lost. If the key is compromised, the encryption becomes useless.
2. **System performance** : Encryption and decryption consume hardware resources (CPU, RAM), which can slow down the processing speed of older devices.
3. **Impact of quantum computer development** : In the future, quantum computers could break even the strongest encryption algorithms currently in use, such as RSA.
4. **Deployment complexity** : Requires a highly skilled technical team to set up a properly functioning system, avoiding vulnerabilities and leaks.

This article has helped you understand what data encryption is, how it works, common types, and some related information. Implementing the right security solution will be key to better protecting yourself in cyberspace. If you have any further questions, feel free to share them with us for clarification.

Frequently Asked Questions

Is data encryption completely secure?

No system can guarantee absolute data encryption security; risks always exist. However, with strong algorithms and good key management, the level of security can be very high.

Can encrypted data be decrypted?

The answer is yes for both symmetric and asymmetric encryption (if you have a valid key). However, for hashing, in most cases you cannot reverse the process to recover the original data.

Do average users need to encrypt their data?

Users should also enable encryption on their personal devices. This will help protect them from the risk of information theft or digital blackmail.

You finished reading the article "**What is data encryption? Principles and practical applications.**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com