# What is data encryption? Things to know about data encryption

Data encryption is to transfer data to a new form that users cannot read and need to use the key to encrypt the data.

One of the safest and most commonly used data security methods in the digital age is data encryption. However, not everyone knows what data encryption is, how it functions, and how the encryption process takes place. In this article, TipsMake.com will be with you to learn the basics of data encryption offline.

1. Instructions for securing 2 layers of Facebook by phone number
2. How to activate Instagram security with 2 layers by phone

## 1. What is data encryption?

Data encryption is to transfer data from one form to another or into a code that only people with access to the decryption key or **password** can read it. Encrypted data is often called ciphertext, normal data, unencrypted is called a plaintext.

Currently, data encryption is one of the most popular and effective data security methods, trusted by many organizations and individuals. In fact, data encryption will not prevent data from being stolen, but it will prevent others from reading the contents of the file, because it has been turned into a character form. other, or other content.

How to use Bitlocker to encrypt data on Windows 10 (Part 1)

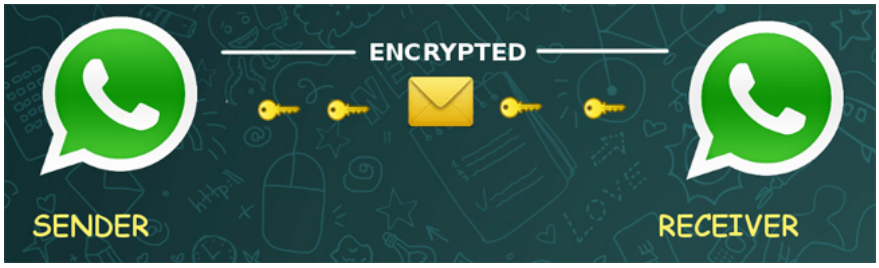
There are two main types of data encryption that exist: asymmetric chemistry, also known as public key encryption, and symmetric encryption.


## 2. The main function of data encryption

The purpose of data encryption is to protect digital data when it is stored on computer systems and transmitted over the Internet or other computer networks. Encryption algorithms often provide key security elements such as authentication, integrity and non-recovery. Authentication allows verification of the origin of data, integrity proves that the content of the data has not been changed since it was sent. No revocation ensures that people cannot cancel sending data.

The encryption process will turn the content into a new form, thus adding a layer of security to the data. So even if your data is stolen, decoding the data is extremely difficult, consuming a lot of computing resources and needing a lot of time. For companies and organizations, the use of data encryption is essential. This will avoid damage when confidential information is accidentally exposed, and it is difficult to decode immediately.

Currently there are many messaging applications that use encryption to secure messages for users. We can mention Facebook, WhatApps with the type of encryption used called End-to-End.




## 3. Data encryption process

The data or plaintext is encoded with an encryption algorithm and an encryption key, creating a ciphertext. Data after encryption can only be viewed in the original form if decoded with the correct key.

Symmetric encryption uses the same secret key to encrypt and decrypt data. Symmetric encryption is much faster than asymmetric encryption, since asymmetric encryption the sender must exchange the encryption key with the recipient before the recipient can decrypt the data. Since companies need to safely distribute and manage large numbers of keys, most data encryption services also realize this and use asymmetric encryption to exchange secret keys. Confidential after using a symmetric algorithm to encrypt data.

Asymmetric encryption algorithm is also called public key encryption, using 2 different keys, a public and a private. We will learn about these two keys in the next section.

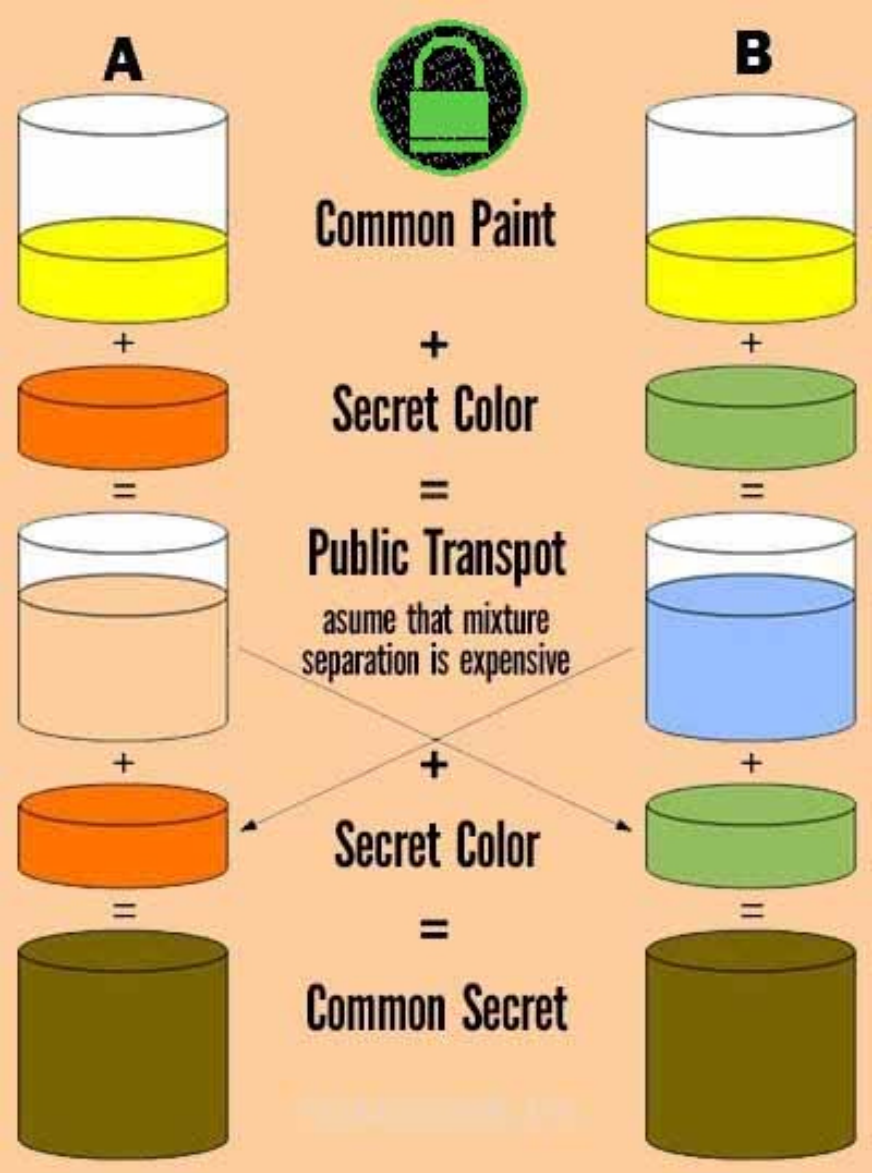
# 4. What is End-to-End data encryption?

End-to-End Encryption (E2EE) is an encryption method that only recipients and senders can understand this encryption message. No one will know what content we're transmitting, including Internet service providers.

This encryption method uses a key between the recipient and the sender who is directly involved in the process of sending data. Unless a third party knows this key, it won't be possible to decrypt it.

Operation mechanism of End-to-End encryption type through Diffie-Hellman key exchange protocol. We can understand through the example of sending a message, two people will proceed to send a public key and a secret key. The message will then be encrypted using a secret key in combination with the public key. And then the recipient will use the secret key to be able to decrypt the message and the content of the message.

So what is the secret key and public key?

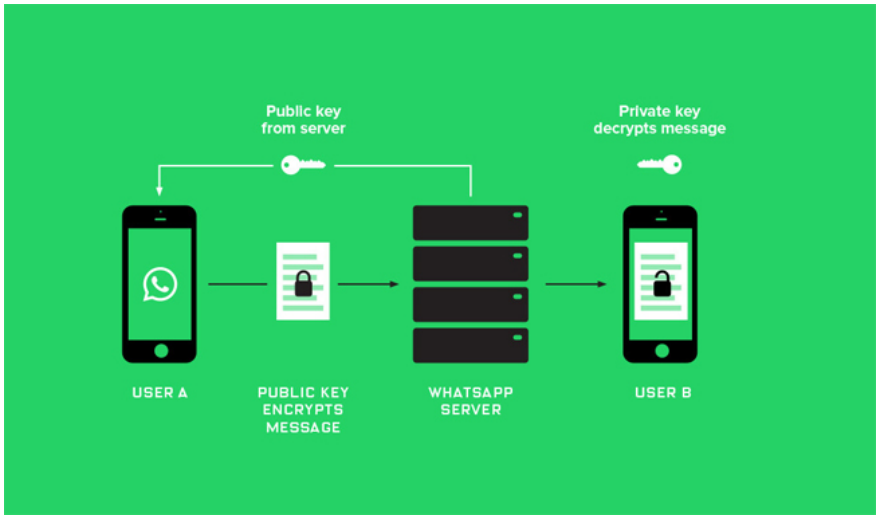



## 5. Secret and public key in End-to-End Encryption?

These two types of keys are all made up of random numbers. The public key will be shared with everyone, but the secret key must be protected, it will be completely in the person who has the right to decrypt it. These 2 codes work with completely different tasks. The public key will conduct data encryption, change the content of the document. The secret key will take over the task of decoding the content.

So when the sender of the message encrypts the data using the public key, the recipient will proceed to decrypt it using the secret key and vice versa.

The Rivest-Sharmir-Adleman (RSA) algorithm is a public key encryption system, widely used to protect sensitive data, especially when it is sent over an unsecured network like the Internet. The popularity of this algorithm is because both the public key and its secret key can encrypt data and ensure the confidentiality, integrity, authenticity and non-recovery of data and technical communications. numbers through the use of digital signatures.




# 6. Challenges to contemporary data encryption

Most basic attacks on encryption are currently Brute Force (continuous trial and error) and try random keys until the correct key is found. It is possible to minimize the probability of unlocking by increasing the length and complexity of the key. The stronger the encryption, the more resources needed to perform calculations will increase, requiring more time and resources to break the code.

How can Windows passwords be cracked - Part 1

Other cryptanalysis methods include sub-channel attacks and cryptographic analysis. Side channel attack occurs after encryption is completed instead of directly attacking the encryption. These attacks are likely to succeed if there are errors in system design or execution. Similarly, cryptographic analysis will find weaknesses in encryption and exploit it. This attack can be successful if there is a vulnerability in the code.

In general, data encryption is essential so that we can increase the security of documents, especially confidential documents and personal account information. Currently, data encryption can be done through a number of online tools such as Whisply, or Nofile.io.

Hope the above article is useful to you!

See also: Summary of popular network attacks today

You finished reading the article "**What is data encryption? Things to know about data encryption**" 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.