

[Home](#) > [Session key](#)

Session key

Session key definition

A session key is a one-use-only key for both encryption and decryption. A session key is randomly generated so that unauthorized users can't access or guess it. It is used to encrypt and protect the communication between two users, a user and a computer, or two computers. One session key can only be used once, which is excellent for protection as attackers won't be able to find it after the fact and use it to crack future communications. A session key is automatically generated when communication between two users or computers starts. After the communication is finished, the session key becomes unusable. Every time two users or computers start a new communication, a new session key will be created to encrypt it. For example, apps like WhatsApp and Telegram use session keys to provide end-to-end encryption to all users, ensuring that users can text each other safely.

See also: [session hijacking](#), [cryptographic key](#)

Session key encryption algorithms

Advanced encryption standard. Advanced encryption standard (AES) is the encryption specification that the U.S. government deems the standard for encrypting devices. It can be used in both hardware and software, and it's one of the best encryptions on the market.

Data Encryption Standard. You can use the Data Encryption Standard (DES) algorithm to encrypt digital data. However, it's not the best choice for most modern apps.

International Data Encryption Algorithm. The International Data Encryption Algorithm (IDEA) is an encryption algorithm that can encrypt text and convert it into unreadable formats, making the text unavailable for people who don't have the session key to decrypt it.

Further reading

🔗 [The best encryption software to use in 2024](#)

🔗 [What is session hijacking?](#)

Download the NordVPN mobile app for iOS or Android.



VPN APPS

Windows

macOS

Linux

Android

iOS: iPhone/iPad

Chrome

Firefox

Edge

HELP

Support Center

Tutorials

FAQ

Privacy Policy

Cookie Preferences

Terms of Service

Contact Us

DISCOVER

Nord Security

NordLayer

NordPass

NordLocker