Pre-shared key

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Pre-shared_key#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Pre-shared_key#searchInput)

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a **pre-shared key** (**PSK**) is a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) which was previously shared between the two parties using some [secure channel](https://en.wikipedia.org/wiki/Secure_channel) before it needs to be used.[[1]](https://en.wikipedia.org/wiki/Pre-shared_key#cite_note-1)

Key[[edit](https://en.wikipedia.org/w/index.php?title=Pre-shared_key&action=edit&section=1)]

To build a key from shared secret, the [key derivation function](https://en.wikipedia.org/wiki/Key_derivation_function) is typically used. Such systems almost always use [symmetric key](https://en.wikipedia.org/wiki/Symmetric_key) cryptographic algorithms. The term PSK is used in [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) encryption such as [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP), [Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA), where the method is called WPA-PSK or WPA2-PSK, and also in the [Extensible Authentication Protocol](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) (EAP), where it is known as [EAP-PSK](https://en.wikipedia.org/wiki/EAP-PSK). In all these cases, both the [wireless access points](https://en.wikipedia.org/wiki/Wireless_access_point) (AP) and all clients *share* the same key.[[2]](https://en.wikipedia.org/wiki/Pre-shared_key#cite_note-2)

The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a [password](https://en.wikipedia.org/wiki/Password), a [passphrase](https://en.wikipedia.org/wiki/Passphrase), or a [hexadecimal](https://en.wikipedia.org/wiki/Hexadecimal) string. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.

[Crypto systems](https://en.wikipedia.org/wiki/Crypto_system) rely on one or more keys for confidentiality. One particular attack is always possible against keys, the [brute force key space search attack](https://en.wikipedia.org/wiki/Brute_force_attack). A sufficiently long, randomly chosen, key can [resist](https://en.wikipedia.org/wiki/Key_size) any practical brute force attack, though not in principle if an attacker has sufficient computational power (see [password strength](https://en.wikipedia.org/wiki/Password_strength) and [password cracking](https://en.wikipedia.org/wiki/Password_cracking) for more discussion). Unavoidably, however, pre-shared keys are held by both parties to the communication, and so can be compromised at one end, without the knowledge of anyone at the other. There are several tools available to help one choose strong passwords, though doing so over any [network](https://en.wikipedia.org/wiki/Computer_network) connection is inherently unsafe as one cannot in general know who, if anyone, may be eavesdropping on the interaction. Choosing keys used by cryptographic algorithms is somewhat different in that any pattern whatsoever should be avoided, as any such pattern may provide an attacker with a lower effort attack than brute force search. This implies [random](https://en.wikipedia.org/wiki/Random) key choice to force attackers to spend as much effort as possible; this is very difficult in principle and in practice as well. As a general rule, any software except a [cryptographically secure pseudorandom number generator](https://en.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator) (CSPRNG) should be avoided.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Pre-shared_key&action=edit&section=2)]

* [Transport Layer Security pre-shared key ciphersuites](https://en.wikipedia.org/wiki/TLS-PSK) (TLS-PSK)