Resources

A key derivation function (KDF) is a cryptographic algorithm used to obtain one or more cryptographic keys from a single secret value, such as a password or passphrase. The purpose of a KDF is to securely generate keys that can be used for encryption, authentication, or other cryptographic purposes.

Common KDF

Scrypt is a memory-hard key derivation function designed to resist brute-force attacks using specialized hardware (e.g., ASICs). It introduces a memory-hardness parameter to increase the memory requirements for key derivation, making it more expensive to parallelize and scale.

Argon2 is a versatile KDF that offers configurable parameters for time cost, memory cost, and parallelism degree. It aims to provide strong security against various attacks, including brute-force and side-channel attacks.

Links

What is a key derivation function (KDF) and how do they work? (comparitech.com)

What is Argon2 Hash? An In-depth Guide with Examples (debugpointer.com)

How to use them

Argon2 | Practical Cryptography for Developers (nakov.com)

Scrypt | Practical Cryptography for Developers (nakov.com)