

i What is Sodium?

Sodium is a modern, easy-to-use software library for encryption, decryption, signatures, password hashing, and more.

It is a portable, cross-compilable, installable, and packageable fork of NaCl, with a compatible but extended API to improve usability even further.

Its goal is to provide all of the core operations needed to build higher-level cryptographic tools.

Sodium is cross-platform and cross-language. It runs on many compilers and operating systems, including Windows (with MinGW or Visual Studio, x86 and x86_64), iOS, and Android. JavaScript and WebAssembly versions are also available and fully supported. Furthermore, bindings for all common programming languages are available and well-supported.

The design choices emphasize security and ease of use. But despite the emphasis on high security, primitives are faster across-the-board than most implementations.

Source: doc.libsodium.org

Encryption/Decryption

Secret Key Encryption (AES-like)

Encrypt `crypto_secretbox_easy()`

Decrypt `crypto_secretbox_open_easy()`

```
```cpp
```

```
unsigned char key[crypto_secretbox_KEYBYTES];
unsigned char nonce[crypto_secretbox_NONCEBYTES];
unsigned char ciphertext[crypto_secretbox_MACBYTES + message_len];
unsigned char decrypted[message_len];

crypto_secretbox_easy(ciphertext, message, message_len, nonce, key);
crypto_secretbox_open_easy(decrypted, ciphertext, sizeof(ciphertext), nonce, key);
`
```

## Installation

Linux Use package managers (e.g., apt-get install libsodium-dev).

Windows Download precompiled binaries or build from source.

macOS Use Homebrew (brew install libsodium).

## Random bytes

```
unsigned char buf[32];
random_bytes(buf,
sizeof(buf));
```

