THE SODIUM DEMO

1. Introduction

This documentation describes the demo for Sodium crypto library. It includes two sessions: about the demo and about the Sodium library.

2. The demo

The objective of this demo is for proving that we can use the Secret key cryptography functions of Sodium library on Windows environment.

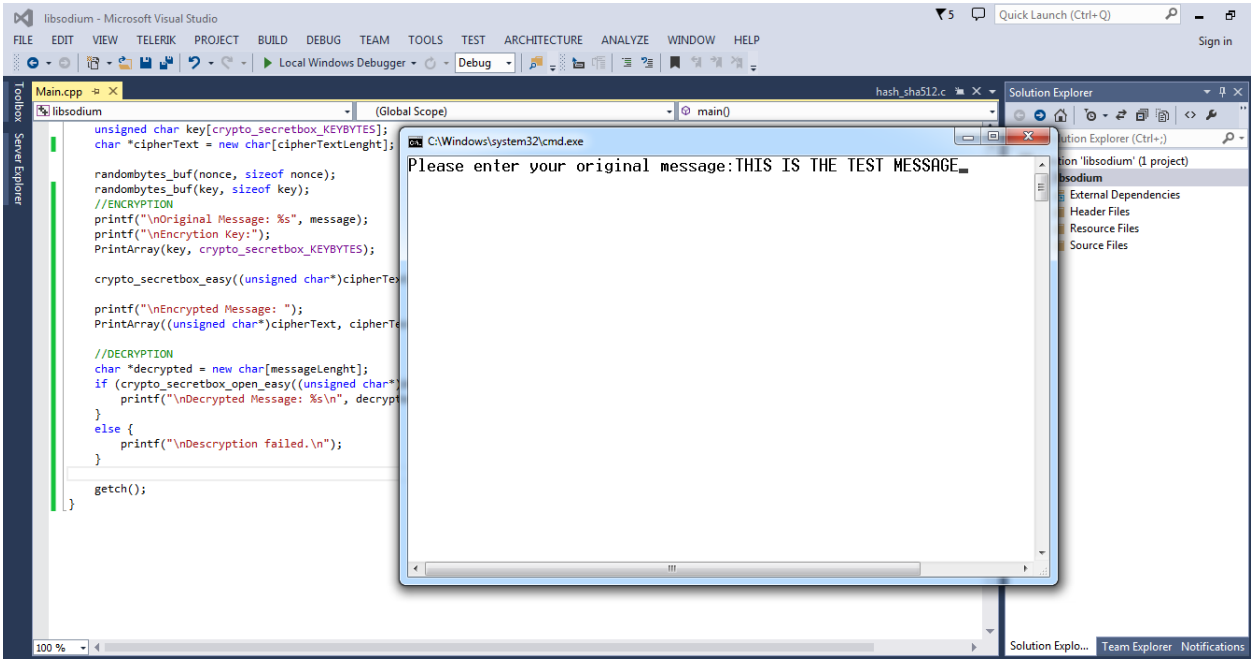
You can run the demo by two ways:

- build and run by Visual Studio .NET 2013 or
- run the libsodium.exe file (in the source code zip file)

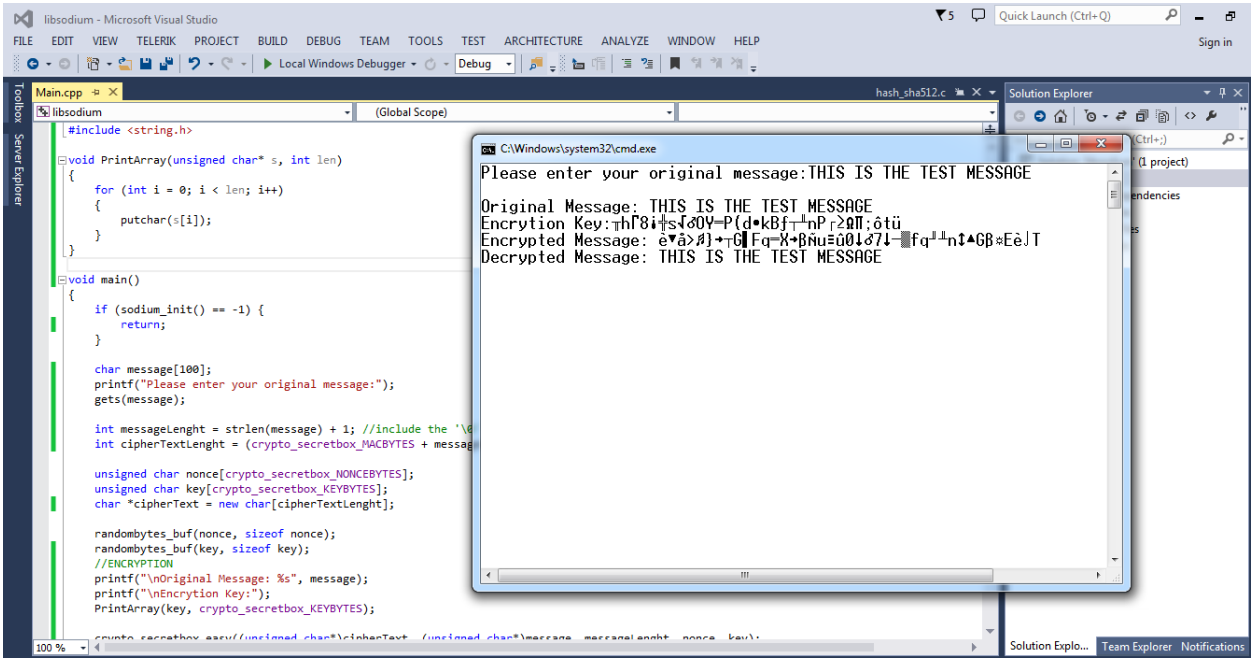
The demo will ask you to enter a message, and then it will encrypt this message by a random secret key. After that, it will decrypt the encrypted message by that key to get the original message.

Here are the screenshots:

Step 1:



Step 2:



What did I do to have this demo?

- Download the source code package of the Sodium library (http://download.dnscrypt.org/libsodium/releases/libsodium-1.0.1.tar.gz)
- Add a new code file Main.cpp at \libsodium-1.0.1\src
- Let the Visual Studio .NET 2013 build the exe file instead of the lib file.

3. The Sodium library

Sodium is a modern, easy-to-use software library for encryption, decryption, signatures, password hashing and more. **It is a portable, cross-compilable, installable, packageable fork of NaCl, with a compatible API, and an 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 supports a variety of compilers and operating systems, including Windows (with MinGW or Visual Studio, x86 and x64), iOS and Android**.

NaCl is a great library but it itself is not portable, only targeted for *nix systems. The Sodium library solves this by making it portable and making a few minor changes to better suite being distributed as a compiled binary.

Links:

http://labs.opendns.com/2013/03/06/announcing-sodium-a-new-cryptographic-library/

http://doc.libsodium.org/