

# Forum:[Hack Forums](#)

Thread: [C++ AES GCM 256](#)

**neonbytes** - December 30, 2020, 9:32 am

Hello everyone,

Is there a way to decrypt AES GCM 256 without statically linking any library?  
A pure C++ implementation?  
Or using Loadlibrary with a DLL (OpenSSL or another crypto) ?

Thank you

**Tafelpoot** - December 30, 2020, 9:59 am

<https://github.com/kokke/tiny-AES-c>

**cghhhhasd** - December 30, 2020, 10:08 am

idk what OS ur using but Windows comes with WinCrypt which gives you access to lots of encryption algorithms, hash algorithms, etc.

**0x0SH3** - December 30, 2020, 1:56 pm

You can do it by using WinApi only (header: <Bcrypt.h>) without linking any library. Try to check this repo on github XShar/Fuck\_Chrome\_C it performs a chromium password decryption using pure C winapi

**neonbytes** - January 4, 2021, 8:46 am

(Dec 30, 2020 10:59 AM)Tafelpoot Wrote: [\[CITE\]](#) [github.com/kokke/tiny-AES-c](https://github.com/kokke/tiny-AES-c)  
Thanks, although it says "small and portable implementation of the AES ECB, CTR and CBC encryption algorithms" it does not cover GCM.

**guardian** - January 4, 2021, 8:50 am

Of course, those libraries would also be written in C++. Just have a look at their source code and learn how they implemented it. Then implement it in your project.

**HFDone** - January 4, 2021, 10:30 am

(Jan 4, 2021 09:46 AM)neonbytes Wrote: [\[CITE\]](#) Thanks, although it says "small and portable implementation of the AES ECB, CTR and CBC encryption algorithms" it does not cover GCM.  
for GCM you will need to use openssl  
<https://github.com/bawejakunal/AES-GCM-256>

**DarkVision** - January 4, 2021, 12:58 pm

embedtls (formerly PolarSSL)

embedtls has GCM support. (Used it in the RAT to create a cipher to recover passwords for Chrome +v80 browsers).

embedtls also allows you to build (DLL) only using the exports you want.

???

neonbytes - January 5, 2021, 4:55 pm

(Dec 30, 2020 02:56 PM)0x0SH3 Wrote: [\[CITE\]](#) You can do it by using WinApi only (header: <Bcrypt.h>) without linking any library. Try to check this repo on github XShar/Fuck\_Chrome\_C it performs a chromium password decryption using pure C winapi

Thanks for the info. I was not aware it could be done with winapi only.

It's actually working for Chrome and Edge, but for some reason I cant make it work with Opera.

(Jan 4, 2021 01:58 PM)DarkVision Wrote: [\[CITE\]](#) embedtls (formerly PolarSSL)

embedtls has GCM support. (Used it in the RAT to create a cipher to recover passwords for Chrome +v80 browsers).

embedtls also allows you to build (DLL) only using the exports you want.

???

Thank you will check it out.

aude - January 8, 2021, 12:32 pm

(Dec 30, 2020 10:32 AM)neonbytes Wrote: [\[CITE\]](#) Hello everyone,

Is there a way to decrypt AES GCM 256 without statically linking any library?

A pure C++ implementation?

Or using Loadlibrary with a DLL (OpenSSL or another crypto) ?

Thank you

LOL damn, i have the exact opposite question as yours.

Today i made a chrome >80 password recoverer, i used libsodium. BUT i failed at doing with static library, but it directly worked on my first dynamic library test

Help me solve this and i give you my code ;)

I know there is this trick, and i did it, but still it doesnt work..

<https://github.com/jedisct1/libsodium/issues/247>

All working fine with dynamic DLL, so header and .lib are correctly called i guess..

```
#define SODIUM_STATIC TRUE
```

```
extern "C" {  
    #include "sodium.h"  
}
```

```
#pragma comment(lib, "libsodium.lib")
```

fucking lost so much time on this...

Another point is.. with base64 decode part and libsum the exe is not that small.

(Jan 4, 2021 01:58 PM)DarkVision Wrote: [\[CITE\]](#) embedtls (formerly PolarSSL)

embedtls has GCM support. (Used it in the RAT to create a cipher to recover passwords for Chrome +v80 browsers).

embedtls also allows you to build (DLL) only using the exports you want.

???

sound pretty good too

**poker** - January 8, 2021, 3:09 pm

(Dec 30, 2020 10:32 AM)neonbytes Wrote: [\[CITE\]](#) Hello everyone,

Is there a way to decrypt AES GCM 256 without statically linking any library?

A pure C++ implementation?

Or using Loadlibrary with a DLL (OpenSSL or another crypto) ?

Thank you

Yes, you can implement your own code or instead use LoadLibray & GetProcAddress in order to call desired functions.