Subject: Cripto with Botan
Posted by Ruimg on Thu, 02 Jul 2009 10:10:34 GMT
View Forum Message <> Reply to Message

Hi All

Can anyone help me compile the Botan Cryptographic library using ultimate++ with gcc because it has some nice algorithms missing in the Crypto package.

Here's were I'm now, I created a new Package, and used the Import Directory Source function in the Package Organizer, but with no success, it generates the file list but they all point to the first level of the folder structure. Is this expected?
I manually added some files later to the upp file.

Compile fails because it cannot find the include file <botan\whatever.h>

I could change the lines to "whatever.h" because all the <botan\...> include files are in utils sub directory, but I don't want to make changes to the code.

Can someone shed some light?

Thanks

Subject: Re: Cripto with Botan
Posted by koldo on Thu, 02 Jul 2009 21:50:37 GMT
View Forum Message <> Reply to Message

Hello Ruimg

Thank you for your post.

I was looking without success for some easy to use library to code files or data in a database (Cryptography is enough complex by itself) to be used from Upp. With your post you have given me the key

It seems Botan is the best option, over Crypto++.

So I will help you to compile Botan in Upp. Your compiling problems sound familiar to me.

One problem I have is that I will stay on holidays for one week.

If you have not done it before, we will have a Hello World ready pretty soon.

Best regards
Koldo

Subject: Re: Cripto with Botan
Posted by Ruimg on Fri, 03 Jul 2009 16:59:32 GMT
View Forum Message <> Reply to Message

Hi koldo

Glad to be of use, and thanks for the help.

Managed to compile Botan from command line with cl (VS 2009) compiler, although with the gcc (MinGW)(3.4.5) gives me the following message

.../3.4.5/cwchar:161: error: `::swprintf' has not been declared

I googled this error and it seams that this is an MinGW bug, I'm trying to work around it... maybe tomorrow I'll try again

Command Line used to compile :

perl configure.pl --msvc
nmake

here is some output so you can help me put the any necessary compiler parameter onto theIde
...
cl.exe /Ibuild\include /O2 /EHsc /GR /D_CONSOLE /nologo /c src\asn1\asn1_att.cpp /Fobuild\lib\asn1_att.obj
...

My question is this, how can I add the src files to theIde and perform the compilation from there?

Many thanks, have nice vacations

Subject: Re: Cripto with Botan
Posted by koldo on Fri, 03 Jul 2009 19:33:54 GMT
View Forum Message <> Reply to Message

Hello Rui

Just my last post before vacation.

It has happen the same to me: Good compiling with Msc9 but problems with MinGW (gcc 4.4.0).

We have a problem: Botan compiling infrastructure make some ad hoc .h files and choose the right .cpp set of files depending on for example OS and compiler . I do not know how to do that in Upp.

I have tried to compile in Upp the Msc version, taking the right set of .cpp files (after checking the configure output...) and using the command line options as you have indicated in your post. But I have found compiling problems in some files.

I am trying a solution:
- For the .cpp ... use the libbotan.lib compiled with the command line configure
- For the .h, I have checked that both msc and mingw have many common .h files but only 3 different, so I have created 3 dummy .h files with this:

build.h

```
#if defined(__MINGW32__)
#include <mingw/build.h>
#elif defined(_MSC_VER)
#include <msc/build.h>
#endif
```

This way it is very simple to update the library. The drawback is that you cannot debug inside.

Best regards
Koldo

Subject: Re: Cripto with Botan
Posted by Ruimg on Thu, 09 Jul 2009 15:38:17 GMT
View Forum Message <> Reply to Message

Hello

I found out that for you to compile most of the complex libs you have to disable BLITZ because of duplicated declarations. I was unable to workaround this.

I just created a upp file with the required files and compiler options. Botan does compile (with some dll warnings) with the MSVC compiler.

Please put the Botan.upp file in the root of your Botan project
My project root directory is called Botan
This file also includes some necessary compiler options.

This should compile only in windows and with the MSVC compiler.

Some problems have arise

The Assist++ has gone mad, it does not auto complete some parts of Botan.

To compile my project with Botan theIDE had to have the include paths option by project. Without this I had to include the /I option in my projects compiler like this "/I..\botan\build\include"

I did not link yet, so I don't know if it works.

Since Botan is too architecture dependent I decided to compile Crypto++ with success, if you want I can pack it and send it to you.

Best regards

File Attachments

1) Botan.upp, downloaded 816 times

Subject: Re: Cripto with Botan
Posted by Ruimg on Thu, 09 Jul 2009 15:44:19 GMT
View Forum Message <> Reply to Message

Ok ok here's the Crypto++ lib

I should make some changes and make a wapper for the lib, in the mean time here's some simple functions

```
#include "CryptoPP/hex.h"
#include "CryptoPP/dll.h"
#include "CryptoPP/default.h"
#include "CryptoPP/md5.h"
#include "CryptoPP/hex.h"

.....

 String EncryptString(String &instr, String &passPhrase)
 {
  std::string outstr;

  CryptoPP::DefaultEncryptorWithMAC encryptor(passPhrase, new CryptoPP::HexEncoder(new
CryptoPP::StringSink(outstr)));
  encryptor.Put((byte *)instr.Begin(), instr.GetLength());
  encryptor.MessageEnd();

  return outstr;
 }

 String DecryptString(String &instr, String &passPhrase)
 {
  std::string outstr;

  CryptoPP::HexDecoder decryptor(new CryptoPP::DefaultDecryptorWithMAC(passPhrase, new
```

```
CryptoPP::StringSink(outstr)));
  decryptor.Put((byte *)instr.Begin(), instr.GetLength());
  decryptor.MessageEnd();

  return outstr;
 }
```

File Attachments

1) CryptoPP.7z, downloaded 787 times

Subject: Re: Cripto with Botan
Posted by Ruimg on Fri, 10 Jul 2009 13:37:32 GMT
View Forum Message <> Reply to Message

New post for new botan upp project.

Now Compiles with VC9 and MingW.

Before changing compiler you must run the configure.pl script, I tried to automate this or make some adjustments to the project with no success.

So, for Microsoft Visual Studio compiler run

perl configure.pl -cc msvc

For Mingw GCC (in my case I have to disable TR1 so)

perl configure.pl -cc gcc --with-tr1=none

Either MSVC and Mingw compilation gives me a lot of warnings

I'm using Ultimate++ build 1393 witch adds some interesting options like internal includes.
So I changed my project file, no more /I compiler options.

Some test code

```
#include <botan/botan.h>
#include <botan/pbkdf2.h>
#include <botan/hmac.h>
#include <botan/sha160.h>

...

 void DoBotan()
 {
```

```
using namespace Botan;
try{
 LibraryInitializer init;

      AutoSeeded_RNG rng;

      std::auto_ptr<S2K> s2k(get_s2k("PBKDF2(SHA-1)"));
      s2k->set_iterations(8192);
      s2k->new_random_salt(rng, 8);

      SymmetricKey key = s2k->derive_key(16, "TEST");

 std::string alg = "AES/CBC/PKCS7";
 Pipe enc(get_cipher(alg, key, ENCRYPTION), new Hex_Encoder);
 Pipe dec(new Hex_Decoder, get_cipher(alg, key, DECRYPTION));
 String secret = ToUtf8(txtIn.GetText());
 enc.process_msg(secret);
 String cipher = enc.read_all_as_string();
 dec.process_msg(cipher);
 String bubu = dec.read_all_as_string();

 PromptOK(bubu);
}
catch (std::exception se)
{
 String err;
 err << "Error \n" << se.what();
 PromptOK(err);
}
}
```

Assist++ is still a bit broken try to list the enc variable methods for example, many are missing.

Created a poll to spice discussion.

Next is to create a simple Botan Wrapper

File Attachments

1) Botan.upp, downloaded 792 times

Botan VS Crypto++(total votes: 3)

Botan of course 1/(33%)
Crypto++ Rules 2/(67%)

Subject: Re: Cripto with Botan
Posted by koldo on Mon, 13 Jul 2009 13:55:11 GMT
View Forum Message <> Reply to Message

Hello Ruimg

After some effort I have compiled a console sample with Botan

About the poll, could you advise me?

I just want a library to encrypt:
- Database fields (strings)
- Files

so that with the right password you can decrypt it.

Coding system?. I just want one so that nobody in the world (without running millions of computers to brute force attack it) can read the string or file without the password.

If you have that fitted into Upp, I will vote yes.

For your info I have found a library comparison here:
http://cookingandcoding.wordpress.com/2008/09/20/c-crypto-li braries/

Best regards
Koldo

Subject: Re: Cripto with Botan
Posted by cbpporter on Mon, 13 Jul 2009 14:52:11 GMT
View Forum Message <> Reply to Message

IMO the poll is a little bit premature. Both libraries have a horrible interface from both what I think is the U++ way and a personal point of view. But with some nice wrappers, using both should be equally easy and then I think we should decide based on technical merit. Just my 2 cents, I don't want to discourage this effort, because I think it is well worth while.

But if I had to choose now, I would say Crypto++.

Subject: Re: Cripto with Botan
Posted by Ruimg on Mon, 13 Jul 2009 17:41:43 GMT
View Forum Message <> Reply to Message

Hello koldo

I must agree with cbpporter. Both of the libs have woeful interfaces. I will try to create a simple

wapper for Cripto++ the U++ way.

Botan is much harder to compile because it needs some scripts to enable the right files to be compiled. (Had a bad time with this one)
On the other hand Cripto++ compiled smoothly on both compilers.

This being said, for simple encryption with multi-platform ease Cripto++ is the way to go.

Subject: Re: Cripto with Botan
Posted by koldo on Mon, 13 Jul 2009 22:21:51 GMT
View Forum Message <> Reply to Message

Hello all

I think the same. Both seem to work but Botan is more difficult to match with Upp.

So for me it is better a wrapper to Crypto++ following your comments and if possible my suggestions.

Best regards
Koldo

Addition. Two links
- Integration with Msc in http://www.codeproject.com/KB/tips/CryptoPPIntegration.aspx
- Libraries comparison in http://idlebox.net/2008/0714-cryptography-speedtest-comparis on/

Other thing Rui. If you would not have time we are here to help

---

Subject: Re: Cripto with Botan
Posted by koldo on Thu, 30 Jul 2009 06:42:27 GMT
View Forum Message <> Reply to Message

Hello Rui

Could you post a project with a demo using Crypto ?. I cannot wait any more for the wrapper

Best regards
Koldo

Subject: Re: Cripto with Crypto++
Posted by Ruimg on Thu, 17 Sep 2009 18:41:05 GMT
View Forum Message <> Reply to Message

Hello all

Sorry for the delay...
Been very busy and have no time for my own projects.

But here is the current state of my small Crypto++ wrapper.

Features :
- MD5 and SHA Hash
- Symmetric String Encryption
- Asymmetric RSA String Encryption (this is cool)

See Test function for how to use it.

Please send comments, bugs and contributes. It is fairly easy to add code so do it!

Am trying to keeping it simple.

NOTES : It does not compile with MingW because the AES needs to be patched. Maybe on my second release.

File Attachments

1) CryptoPP.zip, downloaded 780 times

Subject: Re: Cripto with Crypto++
Posted by Ruimg on Mon, 21 Sep 2009 16:15:27 GMT
View Forum Message <> Reply to Message

Hi again

New version released

Changes include
MingW compiler support
Added allot more Hash Algorithms (CRC, SHA2, Tiger, Whirlpool, RIPEMD, ...)
Rijndael(AES) alloca bug solved.

File Attachments

1) CryptoPP.7z, downloaded 763 times

Subject: Re: Cripto with CryptoPP
Posted by Ruimg on Tue, 29 Sep 2009 14:40:34 GMT

View Forum Message <> Reply to Message

Hi again.

New release BUT with memory leak!

Added a password based template class that can use with any desired hash and encryption algorithm.

This is quite nice but suffers from a memory leak that I cant find.
passcrypt.h is not made by me so credits go to ???

Leak happens with MSVC compiler near PutMaybeModifiable in filters.h while executing Test method.

Can anyone please help?

File Attachments

1) CryptoPP.7z, downloaded 783 times

Subject: Re: Cripto with CryptoPP
Posted by koldo on Sat, 18 Feb 2012 20:06:30 GMT
View Forum Message <> Reply to Message

Hello Rui

Please check this version. It seems to work perfect for MinGW and MSC. It is now a pure console app (CryptoPP_demo).

It uses latest CryptoPP.

Best regards
Koldo

PD: Included a couple of fixes and now works perfectly with gcc 4.6 in Ubuntu 11.10.

File Attachments

1) CryptoPP_demo.7z, downloaded 563 times