Subject: Encrypted storage with streaming (OpenSSL, AES)
Posted by Mindtraveller on Wed, 16 Sep 2009 20:17:54 GMT
View Forum Message <> Reply to Message

Sometimes we may have task to store some large file (4+ GB) or small string inside encrypted storage. I tried to make a pair classes which make it easy. This is the first version, so any ideas are welcome.

This package assumes you have OpenSSL library successfully installed and its paths are added to TheIDE.

OK, let me introduce a pair of classes called AESEncoderStream and AESDecoderStream. They support streamed adding and encryption/decryption of data. Encryption is made with AES (Rijndael) with 128, 192 or 256 bit keys.

Encrypted data 32 bytes larger than source length aligned to 16-byte boundary. I.e. if your source data is 170 bytes long, the resulting length is:
170 rounded by 16-byte pieces = 176
plus
32 (header data)
= 176 + 32 = 208 bytes.
Not so ugly for a number of applications especially if source data is large.

Here is a simple self-explanating demo:

```
#include <Core/Core.h>
#include <openssl/aes.h>
#include <AESStream/AESStream.h>

using namespace Upp;

CONSOLE_APP_MAIN
{
 AESInit();

 // Generate cryptographically stable key
 String key(AESRandomString(32));

 // Encryption
 String sIn,sOut;
 sIn =
"qwertyuiop[p\tasdfghjkl;zxcvbnm,./quwiueqiwueoiquweioquweioquweiqwueicuwinuqiweqiwue pqi
ueci eiqniuriryuweyruweyruewrycuwbrurbywuyrwquiercbbcrebrquwey";
 AESEncoderStream aesEncoder(sIn.GetLength(), key);
 aesEncoder << sIn.Left(10);
 aesEncoder << sIn.Mid(10,10);
 aesEncoder << sIn.Right(sIn.GetLength() - 20);

 sOut << aesEncoder; //do streamed encoding
```

```
// Decryption
//key.Set(0, 'a'); //uncomment to see what happens with wrong key
AESDecoderStream aesDecoder(key);

aesDecoder << sOut.Left(15); //you may add by parts
aesDecoder << sOut.Right(sOut.GetLength() - 15);

try
{
 String sDecoded;
 sDecoded << aesDecoder; //throw exception if key is wrong

 Cout() << (sDecoded == sIn) << "\n\n"; //check if all converted successfully
}
catch (const char *xp)
{
 Cout() << "\n!!Error: " << ToSystemCharset(xp);
}
}
```

File Attachments

1) AESStream.zip, downloaded 853 times