
Subject: Re: Protect package - A starting copy protection system

Posted by [mdelfede](#) on Sat, 02 Oct 2010 16:08:41 GMT

[View Forum Message](#) <> [Reply to Message](#)

281264 wrote on Sat, 02 October 2010 16:00Hi Massimo,

I am finding some unexpected outcome. The problem seems to be related with the key. The encryption key I am using is AABBCCDDEEFF00112233445566778899 (as shown, without quotes); the GetKey function is as the example:

```
String GetKey(void)
```

```
{  
    // WARNING -- TO PUT A NULL BYTE (0X00) INSIDE KEYSTRING  
    // REQUIRES SOME ADDITIONAL WORK !  
    String k = "\xAA\xBB\xCC\xDD\xEE\xFF";  
    k.Cat("\x00");  
    k += "\x11\x22\x33\x44\x55\x66\x77\x88\x99";  
    return k;  
}
```

The application compiles well and it runs fine, but it does not recognize the kye!

Where is the bug?

The bug is that your encryption key is AABBCCDDEEFF00112233445566778899 but in your source you use AABBCCDDEEFF.... Keys in optional build step command line and inside your code must match.

Quote:

Remarks:

well, you can use whatever you like, it's enough that keys are 16 or 32 byte long.

Of course, for sake of simplicity, the key in custom build step is entered as hex-ascii string, so AABBBB.... where each couple of chars form an hex byte, otherwise it would be hard to enter keys with control chars there.

If you enter for example 303132333435 in custom build step, the key in your code should be any of :

```
[code]
```

```
12345
```

```
\x30\x31\x32\x33\x34\x35
```

```
[/quote]
```

I'd suggest the second form as it's easy to compare with the custom build step one.....

2.- what is len in the PROTECT_DECRYPT function? The length of the key, perhaps (the it should be 16bytes or 32 bytes)?

[/quote]

PROTECT_DECRYPT is an helper function which takes following parameters :

Address of the block to be decoded

Length of the block

A String containing the key

In your case you should use :

```
bool Decrypt(byte *start, size_t len)
{
    return PROTECT_DECRYPT ( start, len, GetKey());
}
```

Where the GetKey() function is your above one.

Anyways, I guess I've to change the help a bit.....

Ciao

Max
