

Re: Hunt for rand and srand implementations ;)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1325.html>

From: Skybuck Flying (*nospam_at_hotmail.com*)

Date: 10/29/04

Date: Fri, 29 Oct 2004 01:41:10 +0200

Well,

It turns out the implementation found on the next was indeed from Visual C/CPP 6.0 ;)

(The code found on the internet did not initialize the holdrand variable to one... that probably put me off a bit ;) and also the code was probably "compressed" (read obfuscated :D))

Pretty interesting so far:

Also I tested knoppix's rand and srand.... and somebody else tested debian's rand and srand... and at least debian generates other random number values than the posix version...

```
#include <STDLIB.H>
```

```
/*
```

FROM MSDN WEBSITE:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore98/HTML/crt_srand.asp

srand

Sets a random starting point.

```
void srand( unsigned int seed );
```

Routine Required Header Compatibility

srand <stdlib.h> ANSI, Win 95, Win NT

For additional compatibility information, see Compatibility in the Introduction.

Libraries

LIBC.LIB Single thread static library, retail version
LIBCMT.LIB Multithread static library, retail version
MSVCRT.LIB Import library for MSVCRT.DLL, retail version

Return Value

None

Parameter

seed

Seed for random-number generation

Remarks

The srand function sets the starting point for generating a series of pseudorandom integers. To reinitialize the generator, use 1 as the seed argument. Any other value for seed sets the generator to a random starting point. rand retrieves the pseudorandom numbers that are generated. Calling rand before any call to srand generates the same sequence as calling srand with seed passed as 1.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore98/HTML/crt_rand.asp

rand

Generates a pseudorandom number.

```
int rand( void );
```

Routine Required Header Compatibility

rand <stdlib.h> ANSI, Win 95, Win NT

For additional compatibility information, see Compatibility in the Introduction.

Libraries

LIBC.LIB Single thread static library, retail version
LIBCMT.LIB Multithread static library, retail version
MSVCRT.LIB Import library for MSVCRT.DLL, retail version

Return Value

rand returns a pseudorandom number, as described above. There is no error return.

Remarks

sci.crypt: Re: Hunt for rand and srand implementations ;)

The rand function returns a pseudorandom