

Re: Hunt for rand and srand implementations ;)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1315.html>

From: Skybuck Flying (*nospam_at_hotmail.com*)

Date: 10/28/04

Date: Thu, 28 Oct 2004 23:33:51 +0200

Ah... I found a way to reply to my own message with the buggy outlook express ;)

(Go into the sent folder and then click reply all and remove yourself from the CC :) hehehe)

Ok there was a little bug in my initial version... srand was being called for the IBM version... but IBM_AIX_srand should ofcourse be called...

I have also added another platform... it's actually more an UNIX/POSIX api I think... yes POSIX hehe... and the funny thing is IBM_AIX results are the same for the POSIX results.... and unix,linux,solaris and some hp os-es probably have the same srand() and rand() routines... I wonder if redhat,debian, etc also have the same ones.. or different ones ?! ;)

Here is the code so far ;) (and I'll add to links for microsoft's doc for visual c... I pasted the whole text in the source.. but I dont wanna paste it here... so here goes :))

```
// Hunt for random number generators ;)
```

```
// Started by Skybuck Flying on 28 october 2004 :)
```

```
// visual c cpp 6 srand and rand
```

```
// implementation unknown...
```

```
//
```

```
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore98/HTML/crt\_srand.asp
```

```
//
```

```
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore98/HTML/crt\_rand.asp
```

```
void visual_c_cpp_6_srand( unsigned int seed )
```

```
{  
    srand( seed );  
}
```

```
int visual_c_cpp_6_rand(void)
```

```
{  
    return rand();  
}
```

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

```
// IBM AIX srand and rand implementation occurring to:
//
http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/libs/basetrf2/rand.htm
static unsigned int IBM_AIX_next = 1;

int IBM_AIX_rand(void)
{
    IBM_AIX_next = IBM_AIX_next * 1103515245 + 12345;
    return ((IBM_AIX_next >>16) & 32767);
}

void IBM_AIX_srand(unsigned int Seed)
{
    IBM_AIX_next = Seed;
}

// POSIX 1003.1–2003 gives the following example of an implementation of
// rand() and srand(), possibly useful when one needs the same sequence on
// two different machines.

// the following platforms probably use this random number generator:
// FreeBSD, Linux, Solaris, IBM–AIX, possible even more OS–es based on
UNIX/POSIX ;)

static unsigned long POSIX_next = 1;

/* RAND_MAX assumed to be 32767 */
int POSIX_rand(void)
{
    POSIX_next = POSIX_next * 1103515245 + 12345;
    return((unsigned)(POSIX_next/65536) % 32768);
}

void POSIX_srand(unsigned seed)
{
    POSIX_next = seed;
}

int main()
{
    int seed;

    // use same seed for all srand functions to find same implementations ;)
    etc ;)
    seed = 12345;

    // visual c/c++ 6.0 srand and rand:
    printf("visual c/c++ 6.0 \n" );

    srand( seed );
}
```

Re: Hunt for rand and srand implementations ;)

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

```
printf("rand1: %d \n", rand() );
printf("rand2: %d \n", rand() );
printf("rand3: %d \n", rand() );

// visual c/c++ 6.0 rand output for srand seed 12345
// rand1: 7584
// rand2: 19164
// rand3: 25795

// IBM AIX srand and rand:
printf("IBM AIX \n" );

IBM_AIX_srand( seed );

printf("rand1: %d \n", IBM_AIX_rand() );
printf("rand2: %d \n", IBM_AIX_rand() );
printf("rand3: %d \n", IBM_AIX_rand() );

// IBM AIX rand output for srand seed 12345
// rand1: 21468
// rand2: 9988
// rand3: 22117

// POSIX srand and rand:
printf("POSIX \n" );

POSIX_srand( seed );

printf("rand1: %d \n", POSIX_rand() );
printf("rand2: %d \n", POSIX_rand() );
printf("rand3: %d \n", POSIX_rand() );

// POSIX rand output for srand seed 12345
// rand1: 21468
// rand2: 9988
// rand3: 22117

return 0;
}
```

Bye,
Skybuck

Re: Hunt for rand and srand implementations ;)