Subject: How to re-initialize random generator?
Posted by Mindtraveller on Wed, 09 Sep 2009 15:30:33 GMT
View Forum Message <> Reply to Message

It looks like Core has some advanced version of random numbers generator adopted from Makoto Matsumoto works (Core/Random.cpp).
My question is how to reinitialize this generator each time program start for it to generate different values on each start? (I mean, something like Randomize()).

Subject: Re: How to re-initialize random generator?
Posted by mirek on Thu, 10 Sep 2009 12:28:31 GMT
View Forum Message <> Reply to Message

Mindtraveller wrote on Wed, 09 September 2009 11:30It looks like Core has some advanced version of random numbers generator adopted from Makoto Matsumoto works (Core/Random.cpp).
My question is how to reinitialize this generator each time program start for it to generate different values on each start? (I mean, something like Randomize()).

Well, it is seeding automatically:

```
MTrand::MTrand()
{
 mti = N + 1;
 mag01[0] = 0;
 mag01[1] = MATRIX_A;
 dword seed[1024];
#ifdef PLATFORM_POSIX
 int fd = open("/dev/urandom", O_RDONLY);
 read(fd, seed, sizeof(seed));
#else
 for(int i = 0; i < 1024; i++) {
  Uuid uuid;
  CoCreateGuid((GUID *)&uuid);
  seed[i] = GetHashValue(uuid);
 }
#endif
 init_by_array(seed, 1024);
}
```

Subject: Re: How to re-initialize random generator?

Posted by Mindtraveller on Thu, 10 Sep 2009 16:05:13 GMT
View Forum Message <> Reply to Message

Thanks for the reply, Mirek. Could you please tell if this random generator can be used to generate initial seed value for any cryptographically secure pseudo-random number generator (i.e. the one from OpenSSL which I consider using for next project).

Subject: Re: How to re-initialize random generator?
Posted by mirek on Thu, 10 Sep 2009 23:53:50 GMT
View Forum Message <> Reply to Message

http://en.wikipedia.org/wiki/Mersenne_twister