There seem to be a variety of references to the kiss RNG.

That kiss monster is a new one to me, although I have heard of

the cookie monster. There seem to be two kinds of

RNGs in question: 1) variations on KISS, a random generator

that combines three simple generators, and 2) RNG's with

"monster" period, which arise from r-lag multiply-with-carry RNG's.

Here is a history and clarification:

The idea behind the kiss RNG goes back to "Super-Duper",

a widely used RNG that I developed at McGill, circa 1970.

Super-Duper combined the congruential sequence

x(n)=69609\*x(n-1)+12345 mod 2^32

(any odd replacing 12345), with the 2-shift generator

based on (using C notation):

y^=(y<<15); y^=(y>>17);

When I developed multiply-with-carry RNG's, I changed

from 2-shift to 3-shift for the y's (because some 2-shift

seeds yield a period around 2^21 rather than 2^32-1), then

added a third 1-lag MWC component, and called the result KISS,

based on Keep It Simple Stupid, a phrase popular in the

media at the time, either to support or deride the

early Clinton administration's economic policy.

So the name was partly---but not entirely--in jest, because

I think very good RNG's can be made by combining simple ones.

There are several versions of KISS. All of them seem to pass

the tests in DIEHARD, have a period around 2^124, (depending

on the choice of the MWC component). Versions are used by

gaming companies (some with, some without, license) because

the operations are particularly well-suited for 32-bit

processors in an electronic gaming machine.

The first version of KISS adjoined two 1-lag, 16-bit MWC sequences,

because Fortran did not provide ready access to the 64-bit

result of multiplying two 32-bit integers. Early C versions

merely converted the Fortran instructions, until the time

when most C implementations provided for that 64-bit access

via unsigned long long's. Thus the latest C version of KISS:

unsigned long KISS(void){

static unsigned long x=123456789,y=362436,z=521288629,c=7654321;

unsigned long long t, a=698769069LL;

x=69069\*x+12345;

y^=(y<<13); y^=(y>>17); y^=(y<<5);

t=a\*z+c; c=(t>>32);

return x+y+(z=t);

}

Four random seeds are required,

0<=x<2^32, 0<y<2^32, 0<=z<2^32, 0<=c<698769069.

If the static x,y,z,c is placed outside the KISS proc, a seed-set

routine may be added to allow the calling program to set the seeds.

In gaming machines these would presumably be set by clocks or

registers based on cumulative previous results.

The period is 2^32\*(2^32-1)\*(698769069\*2^31-1)> 2^124 or 10^37.

For variations: In the congruential part, 69069 may be replaced

by any multiplier that is 3 or 5 mod 8; for 12345, any odd constant.

For the 3-shifts, there are 161 triples besides (13,17,5) that

provide maximal period (if interested, send for article), and

for the multiply-with-carry sequence, choose any multiplier 'a'

such as 698769069 for which both a\*2^32-1 and a\*2^31-1 are primes.

A period for KISS, some 2^124, cannot be considered a "monster"

when compared to the periods that can be obtained by multiply-with-carry

or complimentary-multiply-with-carry sequences based on a circular table

of the r most recent x's :

x(n)=a\*x(n-r)+carry mod b, b=2^32 (MWC)

x(n)=(b-1)-[a\*x(n-r)+carry mod b], b=2^32-1, (CMWC)

In a recent posting to math/cs groups, I gave an example of a CMWC RNG,

based on a few simple C instructions. It has period 10^33458 times as

long as that of the Mersenne twister, an excellent RNG with an elaborate

program, touted for its long period, (the Mersenne prime 2^19937-1).

Here is a MWC example with period 3056868392^33216-1, a mere

10^4005 times as long as that of the Mersenne twister, yet faster,

far simpler, and seemingly at least as well-performing in tests

of randomness:

static unsigned long Q[1038],c=362436;

unsigned long MWC1038(void){

static unsigned long i=1037;

unsigned long long t, a=611373678LL;

t=a\*Q[i]+c; c=(t>>32);

if(--i) return(Q[i]=t);

i=1037; return(Q[0]=t);

}

You need to assign random 32-bits seeds to the static array Q[1038]

and to the initial carry c, with 0<=c<61137367.

In response to your request for free versions, the above are,

except for commercial purposes, free C versions.

I expect they will work for C++.

One is a table-free kiss , the other a kiss-free monster,

period > 10^10007.