Tempering

The new very long period Twisted GFSR can have not so good statistical properties.
Matsumoto and Kurita developed a shuffling of the bits that can help with this.

For T800 they resubmitted a TT800 version (Tempered Twisted GFSR).
The Marsenne Twister MT19337 is instead already equipped with a similar pattern.

T800 twisting :

```
#include <stdio.h>
#include <unistd.h>



int main(int argc, char* argv[])
{
unsigned int x,y,z;
int s = 7, t=15;
unsigned int a = 0x8ebfd028 ,b = 0x2b5b2500 ,c = 0xdb8b0000;

  while (1) {
    if (read(0,&x,4) != 4) _exit(1);
    y = x ^ ((x<<s) & b);
    z = y ^ ((y<<t)& c);
    write(1,&z,4);
  }
}
```

MT19337 twisting :

```
#include <stdio.h>
#include <unistd.h>



int main(int argc, char* argv[])
{
unsigned int x,y,z;
int u = 11, s = 7, t=15, l = 18;
unsigned int a = 0x9908b0df ,b = 0x9d2c5680 ,c = 0xefc60000;

  while (1) {
    if (read(0,&x,4) != 4) _exit(1);
    y = x ^ (x>>u) ;
    y = y ^ ((y<<s)& b);
    y = y ^ ((y<<t)& c);
    z = y ^ (y>>l) ;
    write(1,&z,4);
  }
}
```

In [ ]: