Números aleatorios en ensamblador usando el coprocesador

En los proyectos de “brute force” es bueno tener una generación rápida de números aleatorios. A continuación muestro mi implementación usando el coprocesador. Inicializaremos nuestro proyecto con los siguientes variables:

```
.const

Multiplicador       dd 16807
NumeroMaximo        dd 07FFFFFFFh

.data

Semilla             dd 0
NumeroAzar          real8 0.0
```

Al iniciar el programa debe tomarse una semilla “al azar”:

```
    rdtsc                   ; inicialización
    and eax, NumeroMaximo   ; de la semilla de
    mov Semilla, eax        ; numeros aleatorios
    finit                   ; y de la FPU
```

Recordemos cambiar la directiva **.386** por **.586** para que compile sin error la instrucción rdtsc. Para generar un número decimal al azar (NumeroAzar) entre 0 y 1 (sin alcanzar el 1) incluiremos el siguiente código:

```
    fild  NumeroMaximo
    fild  Semilla
    fimul Multiplicador
    fprem
    fist  Semilla
    fdivr
    fstp  NumeroAzar
```

Si queremos un número entero entre 0 y Nelementos-1 (por ejemplo, un índice al azar de una tabla de Nelementos) incluiremos:

```
    fild NumeroMaximo
    fild Semilla
    fimul Multiplicador
    fprem
    ffree st(1)
    fistp Semilla

    mov eax, Semilla
    cdq
    div Nelementos
```

Quedando en el registro **edx** un número entero al azar entre 0 y Nelementos-1.

Agradecimientos a Ricardo, RedH@wk, stzwei, y a todos los Crackslatinos.