Generación de números aleatorios

Los números aleatorios son muy útiles en muchas aplicaciones. Aunque existen muchas maneras de generar números aleatorios, siempre es deseable construir una secuencia que sea de máxima longitud antes de que se repita (una secuencia pseudoaleatoria) . Para números de 16 bits es evidente que la longitud de dicha secuencia es 2 elevado a la 16, es decir 65536 números. McCraken describe un algoritmo y tiene la siguiente forma:

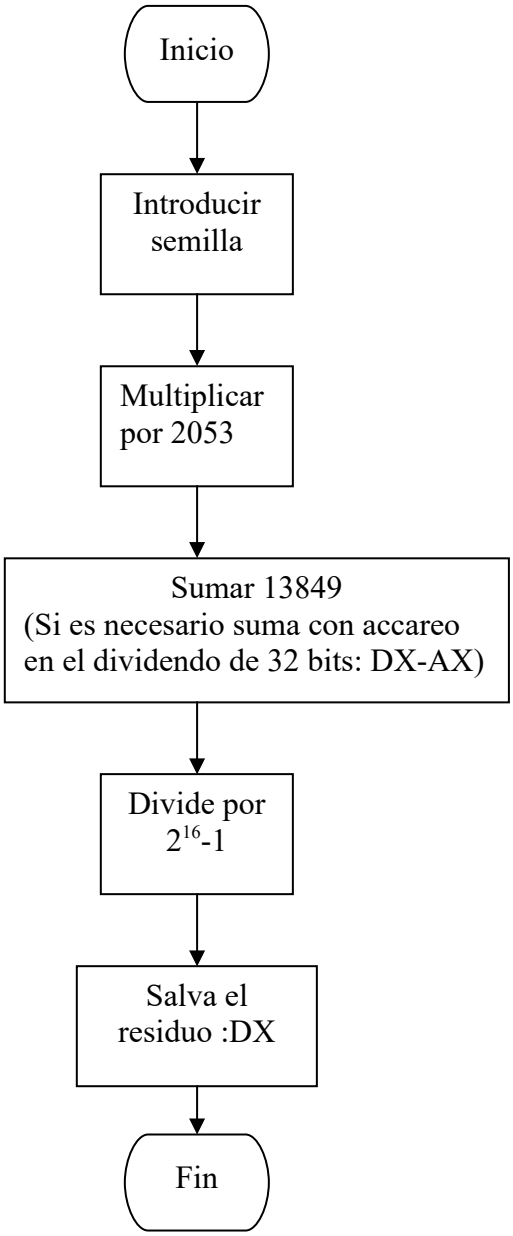
$X_{n+1} = (2053_d X_n + 13849_d) \bmod 2_d^{16} - 1$

Donde :

X_n es un número de entrada aleatoria
X_{n+1} es el resultado de la operación

$2053_d = 805_h$
$13849_{d=} 3619_h$

Diagrama de flujo del procedimiento ALAETORIO



Ejemplo: Desplegar 10 números aleatorios entre 0 y 9

```
;programa para tasm QUE OBTIENE UN NUMERO ALEATORIO
   ; ESTE PROGRAMA CALCULA UN NUMERO ALEATORIO BASADO
   ; EN OTRO NUMERO ALEATORIO PREVIO O SEMILLA, COLOCADO EN DX
   ;Y LA SALIDA SE OBTIENE EN AX, EL NUMERO ALEATORIO ES DE 16 BITS

; Definicion de stack
STACKSG segment para stack 'stack'
        DB 20 DUP (0)
STACKSG ENDS

;DEFINICION DE AREAS DE TRABAJO
DATASG SEGMENT PARA 'DATA'
MEN1 DB 'SEMILLA PARA EL NUMERO$'
MEN2 DB 'ADIOS$'
DATASG ENDS

CODESG SEGMENT PARA 'CODE'
PRINCI PROC FAR
   ASSUME SS:STACKSG, DS:DATASG,CS:CODESG
   ;PROTOCOLO
   PUSH DS
   SUB AX,AX
   PUSH AX
   MOV AX,SEG DATASG
   MOV DS,AX

   ;INICIA PROGRAMA
   MOV CX,10
OTRO:   PUSH CX
   CALL SEMILLA
   CALL ALEATORIO
   CALL ESCALANDO
   CALL LEE
   POP CX
   LOOP OTRO
   CALL SALIR_DOS
PRINCI ENDP


ALEATORIO PROC
; XN+1=(2053*XN + 13849)MOD 2**16
; RETORNA EL NUMERO PSEUDOALEATORIO EN AX
MOV AX,DX ;CARGANDO A AX EL NUMERO SEMILLA tomado de la int 21 serv
           2CH
MOV DX,0  ;CARGANDO CERO EN LA POSICION MAS SIGNIFICATIVA DEL
           MULTIPLICANDO
MOV BX,2053 ; MULTIPLICADOR
MUL BX
MOV BX,13849 ;CARGA EN BX LA CONSTANTE ADITIVA
CLC
ADD AX,BX ; SUMA PARTES MENOS SIGNIFICATIVAS DEL RESULTADO
ADC DX,0 ; SUMA EL ACARREO SI ES NECESARIO
MOV BX,0FFFFH ; CARGAR LA CONSTANTE 2**16-1
DIV BX
MOV AX,DX ; MUEVE EL RESIDUO  AX
RET
```

```
ALEATORIO ENDP

SEMILLA PROC
PUSH AX
MOV AH,2CH
INT 21H  ; RETORNA CH=HORAS, EN FORMATO 00-23, MEDIANOCHE=0
         ; CL MINUTOS 00-59
         ;DH SEGUNDOS 00-59
         ;DL CENTESIMAS DE SEGUNDO 00-99
POP AX
RET
SEMILLA ENDP

ESCALANDO PROC
   ; ESCALANDO EL NUMERO PSEUDOALEATORIO OBTENIDO
   MOV DX,0
   MOV BX,0AH ;NUMEROS ALEATORIOS ENTRE 0 Y 9
   DIV BX
   MOV AX,DX
   ADD AX,3030H ; CONVIRTIENDO EL DATO BINARIO A ASCII
   MOV DL,AH
   MOV DH,AL
   CALL ESCRIBE
   MOV DL,DH
   CALL ESCRIBE
   RET
ESCALANDO ENDP

ESCRIBE PROC
   MOV AH,02
   INT 21H
 RET
ESCRIBE ENDP

SALIR_DOS PROC
   MOV AH,4CH
   INT 21H
RET
SALIR_DOS ENDP

LEE PROC
   MOV AH,01
   INT 21H
RET
LEE ENDP

CODESG ENDS
        END PRINCI
```

Notas:
CLC: Limpia la bandera de acarreo
ADC: Suma el contenido de la bandera de acarreo mas el 1er operando y posteriormente suma el primero con el 2º.

Suponga la semilla en Dx = FFFF

FFFF*805=804F7FB	DX=0804	AX=F7FB	CF=0
804F7FB+3619=8052E14	CF=1	BX=3619	
	DX=805	AX=2E14	