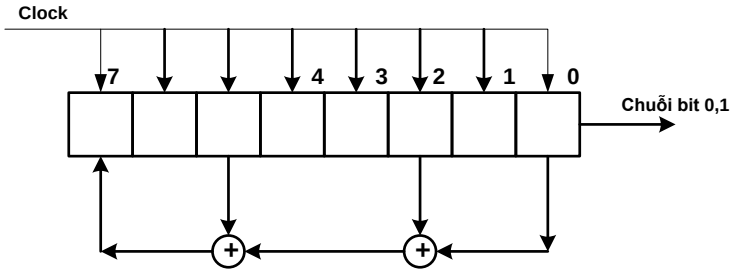
Bài 1 (30 điểm)

Chuỗi mã giả ngẫu nhiên là chuỗi giá trị bít {0,1} rất dài được phát ra theo quy luật có sẵn. Cho khối phần cứng tạo mã giả ngẫu nhiên theo hình vẽ sau:

Các ô vuông là các D Flip-flop, Đầu ra của flip-flop thứ i nối vào đầu vào của flip-flop thứ i-1. Các mũi tên cũng chỉ các đầu vào,ra của các flip-flop và được nối với bộ cộng modulo (XOR).



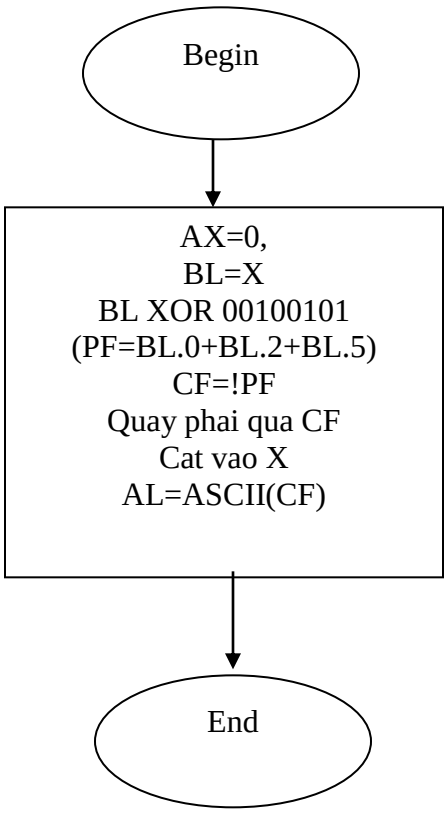
Viết chương trình con tạo mã giả ngẫu nhiên theo mô tả trên.

Mỗi lần gọi chương trình con là một lần có xung nhịp đồng hồ. Đầu ra là các giá trị 0, 1 và được ghi vào thanh ghi AL (thanh ghi AL chứa 2 giá trị 0,1). Nội dung của 8 flip-flop được lưu tại biến toàn cục X (1 byte). Không cần khởi tạo biến toàn cục.

Nội dung chấm điểm:

a) Vẽ lưu đồ thuật toán (10 điểm)

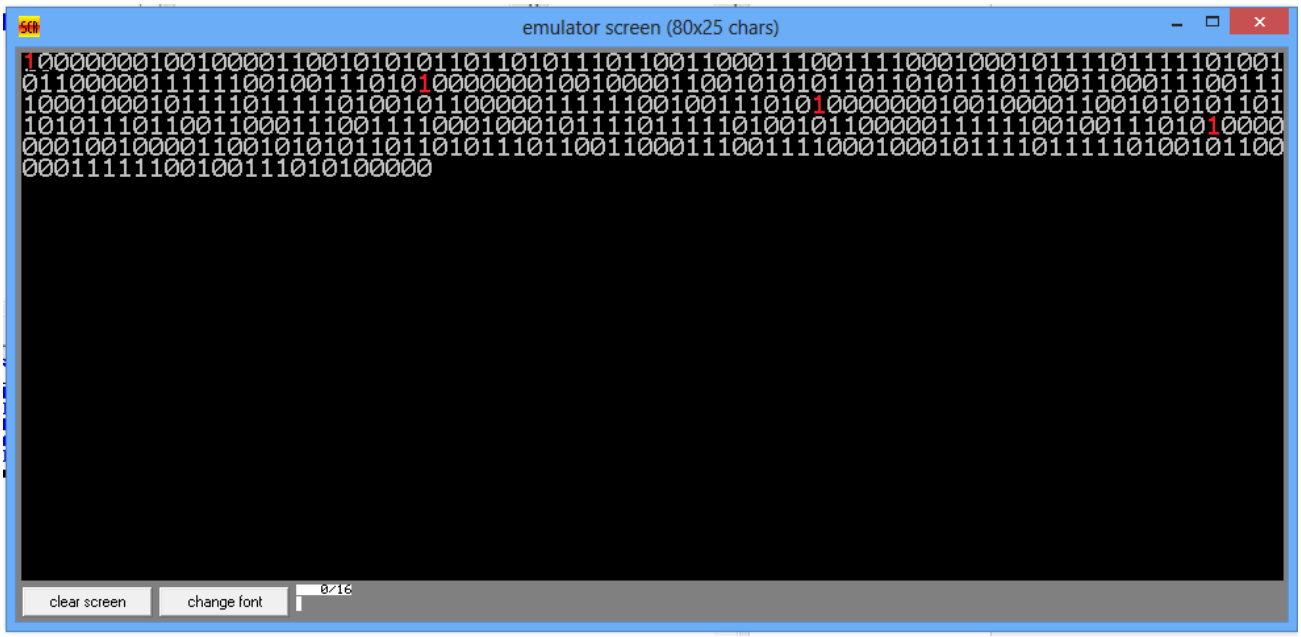
Có nhiều thuật toán khác nhau: thuật toán này dựa trên cơ sở parity là bit có liên quan tới phép cộng modulo (XOR) của các bit trong 1 thanh ghi.



b) Viết chương trình con (20 điểm)

```
.model small
.stack
.data
   X DB 1
.code
MAIN proc
   MOV AX,@Data
   MOV DS,AX
  Lap:
   MOV CX,100
   call PseudoRandom1
   mov AH,2
   MOV DL,AL
   ADD DL,'0'
   INT 21h
   LOOP Lap
   ;Thoat ra DOS
   mov ax, 4c00h
   int 21h
MAIN endp

PseudoRandom1 PROC
       XOR AL,AL    ;xoa AX
       MOV BL,X     ;dung BL
       AND BL,00100101b    ; lay cac bit co lien quan
       ;dem so bit 1 hoac check parity hoac dung XOR 3 lan
       JNP SET_CF
       CLC
       JMP END_IF
    SET_CF:
       STC
    END_IF:
       MOV BL,X      ;truoc do BL da bi thay doi nen phai reload
       RCR BL,1      ;dich bit LSB ra CF, CF-> MSB
       MOV X,BL
       ADC AL,0     ; AL=AL+0+CF
       RET
PseudoRandom1 ENDP
```

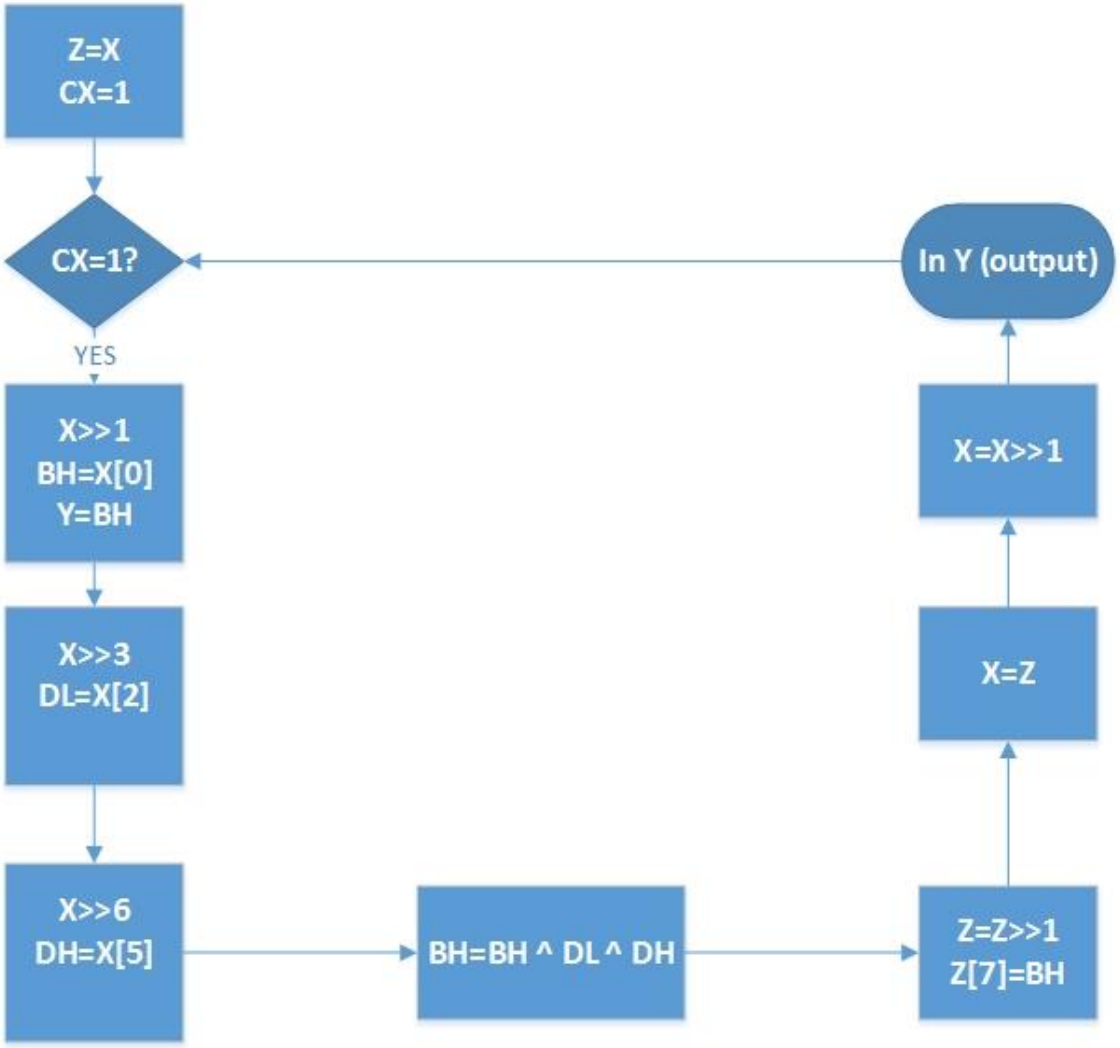


c) Điểm cộng: sau bao nhiêu chu kỳ thì chuỗi lặp lại. (5 điểm)

Sau tối đa 2^8-1 lần dịch thì chuỗi lặp lại. Số lần lặp lại này phụ thuộc vào giá trị khởi tạo. Nếu X=1 thì số lần lặp là 105.
Xem thêm:
http://en.wikipedia.org/wiki/Pseudorandom_number_generator
Sau đây là 1 bài giải của một bạn trong lớp. Tuy rằng kết quả không giống với kết quả của thầy nhưng chương trình cũng tạo được ra chuỗi mã giả ngẫu nhiên. Bài này có thể được điểm tối đa.

BÀI GIẢI:

a) Lưu đồ thuật toán:



b) Chương trình

```
.model small
.stack 100h
.data
   X DB ?,
   Y DB ?,
   Z DB ?,
   s1 DB 10,13,"Ma gia ngau nhien voi X = 22h: $"
```

```
.code
mov AX,@data
mov DS,AX

mov DX, OFFSET s1
mov AH,9
int 21h

xor AX,AX
xor BX,BX
xor CX,CX
xor DX,DX

mov X,22h    ;Khoi tao X

mov CX,42d   ;Khoi tao CX=8
mov AL,X
mov Z,AL
jmp XUNG

XUNG:        ;tao clock
cmp CX,1h
ja DICH
cmp CX,1h
je THOAT
LOOP XUNG
DICH:

xor AX,AX
xor BX,BX
xor DX,DX

mov BL,Z   ;gan lai BL=Z
shr BL,1    ;CF= X[0]
rcl BH,1    ;BH= CF= X[0]

mov Y,BH    ;chuoi 0,1 dau ra
```

```
mov BL,X    ;gan lai BL=X
shr BL,1    ;CF= X[0]
rcl BH,1    ;BH= CF= X[0]

mov BL,X
shr BL,3   ;CF= X[2]
rcl DL,1   ;DL= CF= X[2]

mov BL,X
shr BL,6   ;CF=X[5]
rcl DH,1   ;DH= CF= X[5]

xor BH,DL
xor BH,DH   ;BH= X[0] xor X[2] xor X[5]

sar BH,1    ; CF=BH =X[7]
mov AL,Z    ; Z = trang thai truoc do cua X
rcr AL,1    ; AL= X_sau khi dich va tinh lai bit X[7]= X[0] ^ X[2] ^
X[5]
mov X,AL

mov BL,X    ; gan gia tri X cho Z
mov Z,BL
shr BL,1    ; dich gia tri X sang trai roi lai gan cho X
mov X,BL

jmp INKETQUA

INKETQUA:
mov DL,Y    ;DL=Y
add DL,30h  ;ung voi ki tu so
mov AH,2
int 21h
dec CX
jmp XUNG

THOAT:
mov AH,4Ch
```

```
int 21h
end
```