

Software CRC

Gomez Lacchini, Lihuel Joaquin

Aritmética modular

$$5 \bmod 2 = 1$$

Propiedad:

$$(a*b) \bmod c = ((a \bmod c) * (b \bmod c)) \bmod c$$

Ejemplo con $a=5$, $b=3$ y $c=2$

- $(5*3) \bmod 2 = 15 \bmod 2 = 1$
- $((5 \bmod 2) * (3 \bmod 2)) \bmod 2 = (1*1) \bmod 2 = 1$

Ejemplo con mas factores:

$$(7 * 8 * 4 * 2) \bmod 3$$
$$448 \bmod 3 = 1$$

$$((7 \bmod 3) * (8 \bmod 3) * (4 \bmod 3) * (2 \bmod 3)) \bmod 3$$
$$(1 * 2 * 1 * 2) \bmod 3$$
$$4 \bmod 3 = 1$$

Aritmética modular

$$5 \bmod 2 = 1$$

Propiedad:

$$(a*b) \bmod c = ((a \bmod c) * (b \bmod c)) \bmod c$$

Ejemplo con $a=5$, $b=3$ y $c=2$

- $(5*3) \bmod 2 = 15 \bmod 2 = 1$
- $((5 \bmod 2) * (3 \bmod 2)) \bmod 2 = (1*1) \bmod 2 = 1$

Entonces:

$$(a*b) \bmod c = ((a \bmod c) * b) \bmod c$$

$$((5 \bmod 2) * 3) \bmod 2 = ((1)*3) \bmod 2 = 3 \bmod 2 = 1$$

Ejemplo con mas factores:

$$(7 * 8 * 4 * 2) \bmod 3 \\ 448 \bmod 3 = 1$$

$$((7 \bmod 3) * (8 \bmod 3) * (4 \bmod 3) * (2 \bmod 3)) \bmod 3 \\ (1 * 2 * 1 * 2) \bmod 3 \\ 4 \bmod 3 = 1$$

$$((((7 \bmod 3) * 8) \bmod 3) * 4 \bmod 3) * 2 \bmod 3 \\ (((1 * 8) \bmod 3) * 4 \bmod 3) * 2 \bmod 3 \\ ((8 \bmod 3) * 4 \bmod 3) * 2 \bmod 3 \\ ((2) * 4 \bmod 3) * 2 \bmod 3 \\ ((8 \bmod 3) * 2 \bmod 3) \\ (2) * 2 \bmod 3 \\ 4 \bmod 3 \\ 1$$

Trabaja para una empresa que utiliza muchos ordenadores personales.

Su jefe, el Dr. Penny Pincher, ha querido vincular las computadoras durante algún tiempo, pero no ha estado dispuesto a gastar dinero en las tarjetas Ethernet que ha recomendado. Usted, sin saberlo, ha señalado que cada uno de los PCs provienen del proveedor con un puerto serie asíncrono sin costo adicional. Dr. Pincher, de Por supuesto, reconoce su oportunidad y le asigna la tarea de escribir el software necesario para permitir comunicación entre PCs. Ha leído un poco sobre comunicaciones y sabe que cada transmisión está sujeta a errores y que la solución típica a este problema es agregar alguna información de verificación de errores al final de cada mensaje. Esta información permite al programa receptor detectar cuándo se ha producido un error de transmisión. ocurrido (en la mayoría de los casos). Entonces, vaya a la biblioteca, tome prestado el libro más grande sobre comunicaciones que puede encontrar y pasar su fin de semana (horas extras no pagadas) leyendo sobre la verificación de errores. Finalmente, decide que CRC (verificación de redundancia cíclica) es la mejor verificación de errores para su situación y escriba una nota al Dr. Pincher detallando el mecanismo de verificación de errores propuesto que se indica a continuación.

Generación de CRC

El mensaje que se va a transmitir se ve como un número binario positivo largo. El primer byte del mensaje se trata como el byte más significativo del número binario. El segundo byte es el siguiente más significativo, etc. Este número binario se llamará "m" (para el mensaje). En lugar de transmitir "m", transmitirá un mensaje, "m2", que consta de "m" seguido por un valor CRC de dos bytes. El valor CRC se elige de modo que "m2" cuando se divide por un cierto valor de 16 bits "g" deja un resto de 0. Esto facilita que el programa receptor determine si el mensaje ha sido dañado por errores de transmisión. Simplemente divide cualquier mensaje recibido por "g". Si el resto de la división es cero, se supone que no se ha producido ningún error. Observa que la mayoría de los valores sugeridos de "g" en el libro son extraños, pero no ve cualquier otra similitud, por lo que selecciona el valor 34943 para "g" (el valor del generador). Debe idear un algoritmo para calcular el valor CRC correspondiente a cualquier mensaje que podría ser enviado.

- Para probar este algoritmo, escribirá un programa que lee líneas de la entrada estándar y escribe en la salida estándar.

Input

Cada línea de entrada no contendrá más de 1024 caracteres ASCII (cada línea contiene todos los caracteres hasta, pero sin incluir el carácter de final de línea) como entrada. La entrada termina con una línea que contiene un "#" en la columna 1.

Output

Para cada línea de entrada calcula el valor CRC para el mensaje contenido en la línea y escribe el valor numérico de los bytes CRC (en notación hexadecimal) en una línea de salida. Tenga en cuenta que cada CRC impreso debe estar en el rango de 0 a 34942 (decimal).

Sample Input

this is a test

A

#

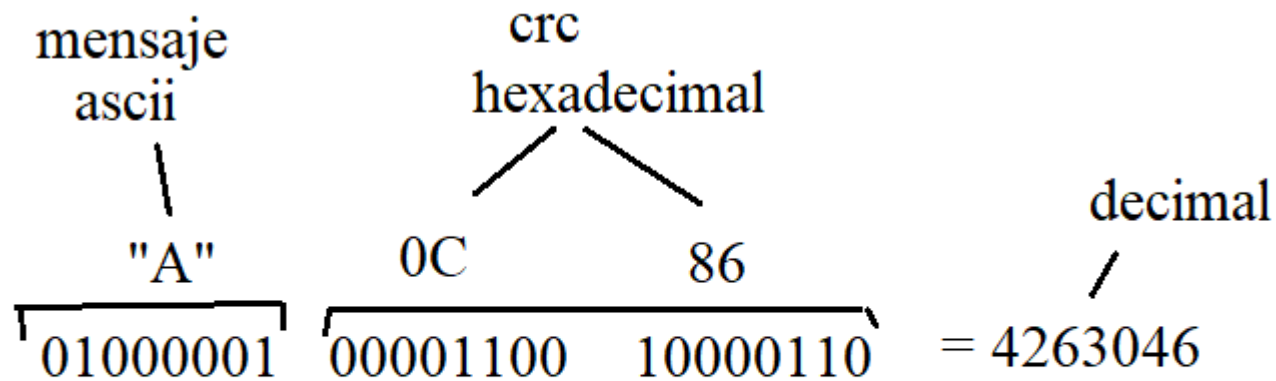
Sample Output

77 FD

00 00

0C 86

AB4 → ?



$$4263046 \bmod 34943 = 0$$



¿Como se puede llegar a eso?

$$\begin{array}{c} \text{"A"} \\ 01000001 \end{array} \overbrace{\begin{array}{cc} \text{CRC} \\ \text{????????} & \text{????????} \end{array}} \text{ mod } 34943 = 0$$

$$01000001 \quad 00000000 \quad 00000000 \quad \text{mod } 34943 = ?$$

$$((65 \times 256) + 0) \times 256 + 0 \quad \text{mod } 34943 = ?$$

$$4.259.840 \quad \text{mod } 34943 = 31737$$

$$34943 - 31737 = 3206$$

sumando lo que le
falta al resto para
llegar a g, va a ser
multiplo de este

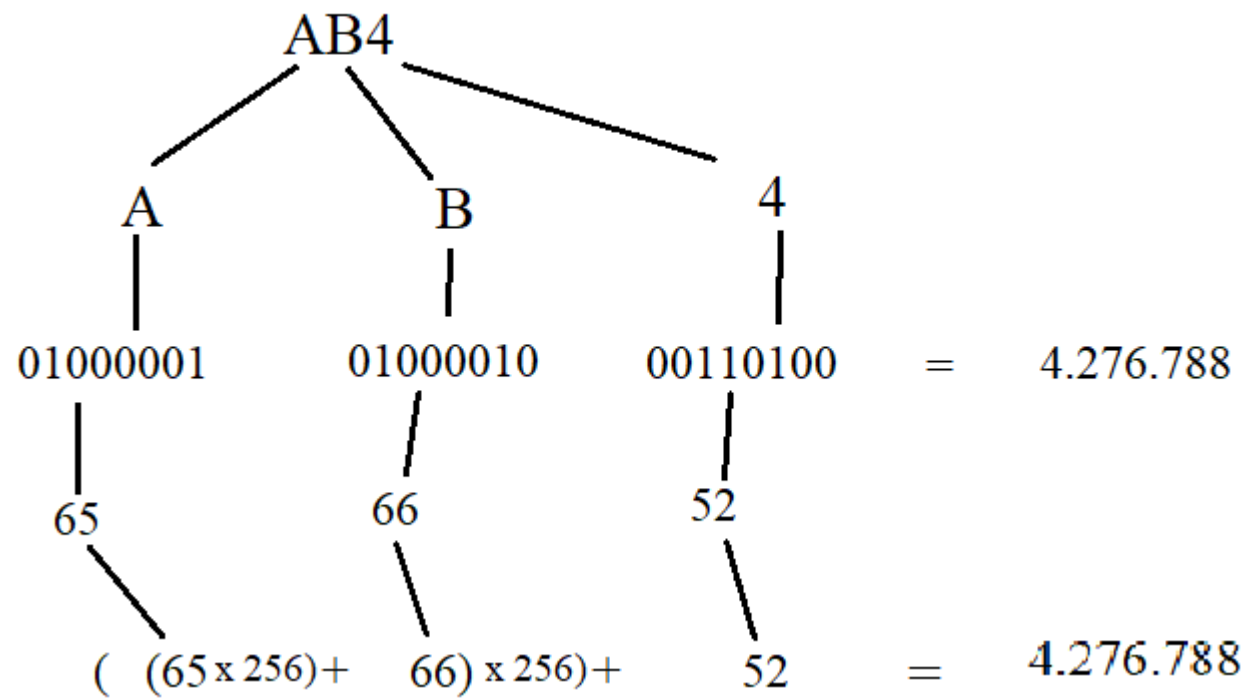
$$3206 = 110010000110 = \text{C } 86$$

/
decimal

|
binario

\
hexadecimal

AB4 \longrightarrow ?



01000001 01000010 00110100 ???????? ???????? mod 34943 = 0

A	B	4	<div style="display: inline-block; text-align: center;"> <div style="border-top: 1px solid black; width: 150px; margin: 0 auto;"></div> <div style="margin: -10px 0 0 0;">CRC</div> </div>
01000001	01000010	00110100	???????? ???????? mod 34943 = 0

$$((((65 \times 256) + 66) \times 256) + 52) \times 256 + ?? \times 256 + ?? \mod 34943 = 0$$

$$((((65 \times 256) + 66) \times 256) + 52) \times 256 + 0 \times 256 + 0 = 280.283.578.368$$

$$01000001 \ 01000010 \ 00110100 \ 00000000 \ 00000000 = 280.283.578.368$$

$$((((65 \times 256) + 66) \times 256) + 52) \times 256 + 0 = 280.283.578.368$$

$$280.283.578.368 \% 34943 = 8.021.165,2796...$$

$$280.283.578.368 \bmod 34943 = 9773$$

$$34943 - 9773 = 25170 \longrightarrow \text{CRC}$$

Demostración

$$280.283.578.368 + 25.170 = 280.283.603.538$$

$$280.283.603.538 \% 34943 = 8.021.166$$

$$280.283.603.538 \bmod 34943 = 0$$

¿Cómo hacer que los números no se vuelvan exponencialmente mas grandes con mensajes mas largos?

A	B	4	CRC			
01000001	01000010	00110100	????????	????????	%	34943 = 0

$$((((65 \times 256) + 66) \times 256) + 52) \times 256 + 0) \times 256 + 0 \% 34943 = 0$$

"A"

$$65 \bmod 34943 = 65$$

"B"

$$(65 \times 256 + 66) \bmod 34943 =$$
$$(16640 + 66) \bmod 34943 = 16706$$

"4"

$$(16.706 \times 256 + 52) \bmod 34943 =$$
$$(4.276.736 + 52) \bmod 34943 = 13742$$

0

$$(13.742 \times 256 + 0) \bmod 34943 =$$
$$(3.517.952 + 0) \bmod 34943 = 23.652$$

0

$$(23.052 \times 256 + 0) \bmod 34943 = 5942.112$$

$$(6.054.912 + 0) \bmod 34943 = 9773$$

$$34943 - 9773 = 25170 \longrightarrow \text{CRC}$$

```
g= 34943
```

```
mensaje = input()
```

```
while mensaje != "#": #Termina cuando entra #
```

```
    #Calculo CRC
```

```
    #Lo imprimo en Hexadecimal
```

```
mensaje = input() #Leo otro mensaje
```

```
g= 34943
mensaje = input()
✓ while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    ✓ for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
        #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
        resto= (resto*256*256)%g
        #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
        #El %g es por si resto da 0, que devuelva 0 y no g
        CRCdecimal=(g-resto)%g

        #Lo imprimo en Hexadecimal

    mensaje = input() #Leo otro mensaje
```

```

g= 34943
mensaje = input()
✓ while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    ✓ for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    ✓ while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print([CRChex[:2]+" "+CRChex[2:]])

    mensaje = input() #Leo otro mensaje

```


g= 34943

mensaje = input()

AB4

while mensaje != "#": #Termina cuando entra #

 resto=0

resto=0

 #Calculo el resto del valor del mensaje dividido g

 for caracter in mensaje:

caracter A

 resto= ((resto*256) + ord(caracter))% g

$resto = ((0 * 256) + 65) \bmod 34943$

 #Calculo el resto del valor del mensaje con dos bytes vacios dividido g

 resto= (resto*256*256)%g

$resto = 65 \bmod 34943$

 #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)

 #El %g es por si resto da 0, que devuelva 0 y no g

$resto = 65$

 CRCdecimal=(g-resto)%g

 #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora

 #hay que presentarlo como pide el output

 #Se convierte a decimal:

 CRChex= hex(CRCdecimal)

 #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":

 CRChex=CRChex[2:(len(CRChex)+1)]

 #Convierto las letras a mayuscula:

 CRChex=CRChex.upper()

 #Si es menor de 4 digitos, entonces lo relleno con ceros delante:

 while len(CRChex)!=4:

 CRChex="0"+CRChex

 #Al imprimir pongo un espacio entre el primer byte y el segundo:

 print([CRChex[:2]+" "+CRChex[2:]])

mensaje = input() #Leo otro mensaje

"A"
65 mod 34943= 65

```

g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print([CRChex[:2]+" "+CRChex[2:]])

mensaje = input() #Leo otro mensaje

```

AB4

resto = 65

caracter ~~A~~ B

resto = ((65*256)+66 mod 34943

resto = (16640+66) mod 34943

resto = 16706



"B"

$(65 \times 256 + 66) \bmod 34943 =$
 $(16640 + 66) \bmod 34943 = 16706$

```

while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje

```

resto = 16706

caracter ~~A~~ ~~B~~ 4

resto = ((16706*256) + 52) mod 34943

resto = (4376736+52) mod 34943

resto = 13742

"4"
 $(16.706 \times 256 + 52) \bmod 34943 =$
 $(4.276.736 + 52) \bmod 34943 = 13742$

```

g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje

```

AB4

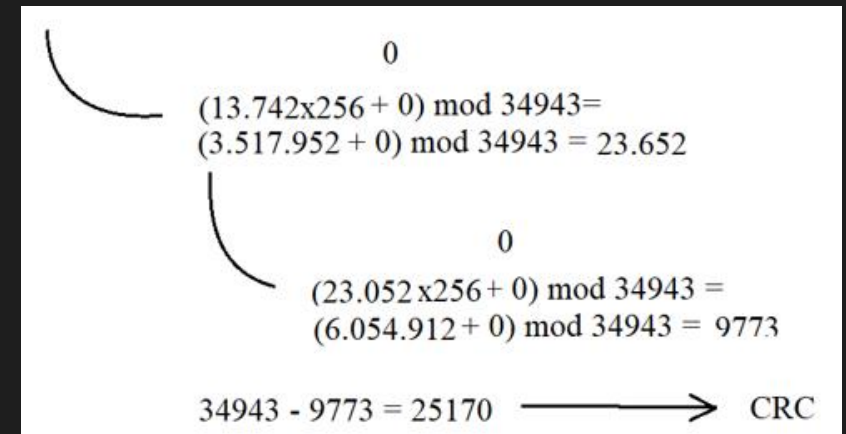
resto = 13742

resto= (13742x256x256) mod 34943

resto = 9773

CRCdecimal= (34943-9773) mod 34943

CRCdecimal = 25170



g= 34943

mensaje = input()

AB4

while mensaje != "#": #Termina cuando entra #

resto=0

#Calculo el resto del valor del mensaje dividido g

for caracter in mensaje:

 resto= ((resto*256) + ord(caracter))% g

#Calculo el resto del valor del mensaje con dos bytes vacios dividido g

resto= (resto*256*256)%g

#En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)

#El %g es por si resto da 0, que devuelva 0 y no g

CRCdecimal=(g-resto)%g

CRCdecimal = 25170

#En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora

#hay que presentarlo como pide el output

#Se convierte a decimal:

CRChex= hex(CRCdecimal)

CRChex= 0x6252

#Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":

CRChex=CRChex[2:(len(CRChex)+1)]

CRChex= 6252

#Convierto las letras a mayuscula:

CRChex=CRChex.upper()

CRChex= 6252

#Si es menor de 4 digitos, entonces lo relleno con ceros delante:

while len(CRChex)!=4:

 CRChex="0"+CRChex

#Al imprimir pongo un espacio entre el primer byte y el segundo:

print([CRChex[:2]+" "+CRChex[2:]])

Output= 62 52

mensaje = input() #Leo otro mensaje

```

g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
  
```



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
```

mensaje = "A"

resto = 0

~~A~~ resto = ((0*256) + 65) mod 34943

resto = 65 mod 34943 = 65

resto = (65*256*256) mod 34943

resto = 31737



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
```

mensaje = "A"

resto = 0

~~A~~

resto= ((0*256) +65) mod 34943

resto = 65 mod 34943 = 65

resto = (65*256*256) mod 34943

resto = 31737

CRCdecimal = (34943-31737)mod 34943

CRCdecimal = 3206



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g
    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])
    mensaje = input() #Leo otro mensaje
```

mensaje = "A"

resto = 0

A

resto= ((0*256) +65) mod 34943

resto = 65 mod 34943 = 65

resto = (65*256*256) mod 34943

resto = 31737

CRCdecimal = (34943-31737)mod 34943

CRCdecimal = 3206

CRChex= 0xc96

CRChex= c96

CRChex = C96

CRChex = 0C96

Output = 0C 96



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
```



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
```

mensaje = ""

resto = 0

$resto = (0 * 256 * 256) \bmod 34943$

$resto = 0 \bmod 34943 = 0$

$CRCdecimal = (34943 - 0) \bmod 34943$

$CRCdecimal = 0$

Si CRCdecimal en vez de $(g - resto) \% g$ hubiera sido solamente $g - resto$, hubiese quedado igual a 34943 que es incorrecto



```
g= 34943
mensaje = input()
while mensaje != "#": #Termina cuando entra #
    resto=0
    #Calculo el resto del valor del mensaje dividido g
    for caracter in mensaje:
        resto= ( (resto*256) + ord(caracter) )% g
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
    resto= (resto*256*256)%g
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
    #El %g es por si resto da 0, que devuelva 0 y no g
    CRCdecimal=(g-resto)%g

    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
    #hay que presentarlo como pide el output
    #Se convierte a decimal:
    CRChex= hex(CRCdecimal)
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
    CRChex=CRChex[2:(len(CRChex)+1)]
    #Convierto las letras a mayuscula:
    CRChex=CRChex.upper()
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
    while len(CRChex)!=4:
        CRChex="0"+CRChex
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
    print(CRChex[:2]+" "+CRChex[2:])

    mensaje = input() #Leo otro mensaje
```

mensaje = ""

resto = 0

$\text{resto} = (0 * 256 * 256) \bmod 34943$

$\text{resto} = 0 \bmod 34943 = 0$

$\text{CRCdecimal} = (34943 - 0) \bmod 34943$

$\text{CRCdecimal} = 0$

$\text{CRChex} = 0x0$

$\text{CRChex} = 0$

$\text{CRChex} = 0$

$\text{CRChex} = 0000$

Output = 00 00

```
g= 34943
```

```
mensaje = input()
```

```
mensaje = "tron"
```

```
while mensaje != "#": #Termina cuando entra #
```

```
    resto=0
```

```
    resto = 0
```

```
    #Calculo el resto del valor del mensaje dividido g
```

```
    for caracter in mensaje:
```

```
        resto= ( (resto*256) + ord(caracter) )% g
```

```
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
```

```
    resto= (resto*256*256)%g
```

```
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
```

```
    #El %g es por si resto da 0, que devuelva 0 y no g
```

```
    CRCdecimal=(g-resto)%g
```

```
    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
```

```
    #hay que presentarlo como pide el output
```

```
    #Se convierte a decimal:
```

```
    CRChex= hex(CRCdecimal)
```

```
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
```

```
    CRChex=CRChex[2:(len(CRChex)+1)]
```

```
    #Convierto las letras a mayuscula:
```

```
    CRChex=CRChex.upper()
```

```
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
```

```
    while len(CRChex)!=4:
```

```
        CRChex="0"+CRChex
```

```
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
```

```
    print(CRChex[:2]+" "+CRChex[2:])
```

```
mensaje = input() #Leo otro mensaje
```



```
g= 34943
```

```
mensaje = input() mensaje = "tron"
```

```
while mensaje != "#": #Termina cuando entra #
```

```
    resto=0 resto = 0
```

```
    #Calculo el resto del valor del mensaje dividido g
```

```
    for caracter in mensaje: resto = ((0*256) + 116) mod 34943
```

```
        resto= ( (resto*256) + ord(caracter) )% g resto = 116
```

```
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
```

```
    resto= (resto*256*256)%g
```

```
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
```

```
    #El %g es por si resto da 0, que devuelva 0 y no g
```

```
    CRCdecimal=(g-resto)%g
```

```
    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
```

```
    #hay que presentarlo como pide el output
```

```
    #Se convierte a decimal:
```

```
    CRChex= hex(CRCdecimal)
```

```
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
```

```
    CRChex=CRChex[2:(len(CRChex)+1)]
```

```
    #Convierto las letras a mayuscula:
```

```
    CRChex=CRChex.upper()
```

```
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
```

```
    while len(CRChex)!=4:
```

```
        CRChex="0"+CRChex
```

```
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
```

```
    print(CRChex[:2]+" "+CRChex[2:])
```

```
mensaje = input() #Leo otro mensaje
```

```
g= 34943
```

```
mensaje = input()
```

```
mensaje = "tron"
```

```
while mensaje != "#": #Termina cuando entra #
```

```
    resto=0
```

```
    resto = 116 r
```

```
    #Calculo el resto del valor del mensaje dividido g
```

```
    for caracter in mensaje:
```

```
    resto = ((116*256)+114) mod 34943
```

```
        resto= ( (resto*256) + ord(caracter) )% g
```

```
    resto = (29696+114) mod 34943
```

```
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
```

```
    resto = 29810
```

```
    resto= (resto*256*256)%g
```

```
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
```

```
    #El %g es por si resto da 0, que devuelva 0 y no g
```

```
    CRCdecimal=(g-resto)%g
```

```
    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
```

```
    #hay que presentarlo como pide el output
```

```
    #Se convierte a decimal:
```

```
    CRChex= hex(CRCdecimal)
```

```
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
```

```
    CRChex=CRChex[2:(len(CRChex)+1)]
```

```
    #Convierto las letras a mayuscula:
```

```
    CRChex=CRChex.upper()
```

```
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
```

```
    while len(CRChex)!=4:
```

```
        CRChex="0"+CRChex
```

```
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
```

```
    print(CRChex[:2]+" "+CRChex[2:])
```

```
mensaje = input() #Leo otro mensaje
```

```
g= 34943
```

```
mensaje = input()
```

```
mensaje = "tron"
```

```
while mensaje != "#": #Termina cuando entra #
```

```
    resto=0
```

```
    resto = 29810 no
```

```
    #Calculo el resto del valor del mensaje dividido g
```

```
    for caracter in mensaje:
```

```
    resto = ((29810*256)+111) mod 34943
```

```
        resto= ( (resto*256) + ord(caracter) )% g
```

```
    resto = (7631360+111)mod 34943
```

```
    #Calculo el resto del valor del mensaje con dos bytes vacios dividido g
```

```
    resto = 13897
```

```
    resto= (resto*256*256)%g
```

```
    #En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)
```

```
    #El %g es por si resto da 0, que devuelva 0 y no g
```

```
    CRCdecimal=(g-resto)%g
```

```
    #En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora
```

```
    #hay que presentarlo como pide el output
```

```
    #Se convierte a decimal:
```

```
    CRChex= hex(CRCdecimal)
```

```
    #Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":
```

```
    CRChex=CRChex[2:(len(CRChex)+1)]
```

```
    #Convierto las letras a mayuscula:
```

```
    CRChex=CRChex.upper()
```

```
    #Si es menor de 4 digitos, entonces lo relleno con ceros delante:
```

```
    while len(CRChex)!=4:
```

```
        CRChex="0"+CRChex
```

```
    #Al imprimir pongo un espacio entre el primer byte y el segundo:
```

```
    print(CRChex[:2]+" "+CRChex[2:])
```

```
    mensaje = input() #Leo otro mensaje
```


g= 34943	
mensaje = input()	mensaje = "tron"
while mensaje != "#": #Termina cuando entra #	
resto=0	resto = 13897 110 n
#Calculo el resto del valor del mensaje dividido g	
for caracter in mensaje:	resto = ((13897*256)+110) mod 34943
resto= ((resto*256) + ord(caracter))% g	resto = (3557632+110)mod 34943
#Calculo el resto del valor del mensaje con dos bytes vacios dividido g	resto = 28499
resto= (resto*256*256)%g	
#En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)	resto= (28499*256*256)mod 34943
#El %g es por si resto da 0, que devuelva 0 y no g	resto = 1867710464 mod 34943
CRCdecimal=(g-resto)%g	resto = 7114
	CRCdecimal = (34943-7114)mod 34943
#En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora	CRCdecimal=27829
#hay que presentarlo como pide el output	
#Se convierte a decimal:	
CRChex= hex(CRCdecimal)	
#Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":	
CRChex=CRChex[2:(len(CRChex)+1)]	
#Convierto las letras a mayuscula:	
CRChex=CRChex.upper()	
#Si es menor de 4 digitos, entonces lo relleno con ceros delante:	
while len(CRChex)!=4:	
CRChex="0"+CRChex	
#Al imprimir pongo un espacio entre el primer byte y el segundo:	
print(CRChex[:2]+" "+CRChex[2:])	
mensaje = input() #Leo otro mensaje	

g= 34943

mensaje = input()

mensaje = "tron"

while mensaje != "#": #Termina cuando entra #

resto=0

resto = 13897 ~~110~~ n

#Calculo el resto del valor del mensaje dividido g

for caracter in mensaje:

resto = ((13897*256)+110) mod 34943

resto= ((resto*256) + ord(caracter))% g

resto = (3557632+110)mod 34943

#Calculo el resto del valor del mensaje con dos bytes vacios dividido g

resto = 28499

resto= (resto*256*256)%g

#En CRCdecimal calculo cuanto falta para llegar a un multiplo de g (g-resto)

resto= (28499*256*256)mod 34943

#El %g es por si resto da 0, que devuelva 0 y no g

resto = 1867710464 mod 34943

CRCdecimal=(g-resto)%g

resto = 7114

#En CRCdecimal ya tengo el resultado del CRC de ese mensaje, ahora

CRCdecimal = (34943-7114)mod 34943

#hay que presentarlo como pide el output

#Se convierte a decimal:

CRCdecimal=27829

CRChex= hex(CRCdecimal)

CRChex=0x6cb5

#Al convertir a decimal se genera en modo 0xaaa, entonces le quito el "0x":

CRChex=6cb5

CRChex=CRChex[2:(len(CRChex)+1)]

#Convierto las letras a mayuscula:

CRChex=6CB5

CRChex=CRChex.upper()

#Si es menor de 4 digitos, entonces lo relleno con ceros delante:

while len(CRChex)!=4:

CRChex="0"+CRChex

#Al imprimir pongo un espacio entre el primer byte y el segundo:

Output = 6C B5

print(CRChex[:2]+" "+CRChex[2:])

mensaje = input() #Leo otro mensaje