

| CPC Cifiado (PC (Perto Cifiar, R) i = 0 j = 0 IV = generar vector de Inicolización regetir hasta que se telinne la codena texa cifiar regetir hasta que se telinne la codena texa cifiar regetir hasta que se telinne la codena texa cifiar prijIII] = texto cifiar III Sina congeta las 64 bits de texacifiar cepetir hasta que no hayo bloques de bits i=0 i=0 regetir hasta que no hayo bloques de bits i=0 i=0 regetir hasta que la codena se terrine si IVII es igual a no IIII anonces varxor III = 0 sina varxor III = 1 CLIJ = cifiar 30cs a varxor con la lique k IV = CLIJ regiesor c e IV Cifiado CTR (texto Cifiar, k) i=0 regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se terrine la codena texto cifiar regetir hasta que se de la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que se de l'unite la codena texto cifiar regetir hasta que no hayo bloques de bits recetir hasta que la codena se terrine regetir hasta que no hayo bloques de bits recetir | eseudo código pora cificdo de los modos de operacio |
|--|--|
| Citiado (PC (texto Ciriar, K) i=0 j=0 1 | |
| i=0 j=0 IV= general vector de hipolización regetir hasta que se telnine la adena texa cificar regetir hasta que se telnine la adena texa cificar regetir hasta que se telnine la adena texa cificar regetir hasta que no hasa bloques de bits concerta enneros 64 bits de texacificar regetir hasta que no hasa bloques de bits i=0 regetir hasta que la adena se telnine si IVII es 1941 al rIIIII entonces Var Xor III=1 clid= cifica 3Des a var Xor can la lique k IV=CLII regiesar c e IV Cificado CTR (texto Cificar, k) i=0 regetir hasta que se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 | CPC |
| i=0 j=0 IV= general vector de hipolización regetir hasta que se telnine la adena texa cificar regetir hasta que se telnine la adena texa cificar regetir hasta que se telnine la adena texa cificar regetir hasta que no hasa bloques de bits concerta enneros 64 bits de texacificar regetir hasta que no hasa bloques de bits i=0 regetir hasta que la adena se telnine si IVII es 1941 al rIIIII entonces Var Xor III=1 clid= cifica 3Des a var Xor can la lique k IV=CLII regiesar c e IV Cificado CTR (texto Cificar, k) i=0 regetir hasta que se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 maili i=1 regiesar la cue se telnine la codena texto affor regetir hasta i=64 | Citizano CDC (Herio Circos H) |
| JEO 1 U = generar vector de Inicolización repetir hasta que de telnine la codena texto cifiar repetir hasta que de telnine la codena texto cifiar repetir hasta que las 64 bits celicor padaina recentar prineras 64 bits de textocifiar je ji i repetir hasta que no hasto bioques de bits i to i to i to repetir hasta que no hasto bioques de bits i to i to repetir hasta que la codena se terrine si lutil es igual a nijilij entonces var Xor Lij - 0 sino var Xor Lij - 1 clij = refor 3Des a var Xor can la lique k i u = CLij j = j + 1 regiesor c e lu cifiado CTR (textocifiar) k) i to repetir hasta i = 84 mijilij = textocifiar Lij i to repetir hasta i = 84 mijilij = textocifiar Lij i to repetir hasta i = 84 mijilij = textocifiar Lij | STETADO CALCITATA |
| JEO 1 U = generar vector de Inicolización repetir hasta que de telnine la codena texto cifiar repetir hasta que de telnine la codena texto cifiar repetir hasta que las 64 bits celicor padaina recentar prineras 64 bits de textocifiar je ji i repetir hasta que no hasto bioques de bits i to i to i to repetir hasta que no hasto bioques de bits i to i to repetir hasta que la codena se terrine si lutil es igual a nijilij entonces var Xor Lij - 0 sino var Xor Lij - 1 clij = refor 3Des a var Xor can la lique k i u = CLij j = j + 1 regiesor c e lu cifiado CTR (textocifiar) k) i to repetir hasta i = 84 mijilij = textocifiar Lij i to repetir hasta i = 84 mijilij = textocifiar Lij i to repetir hasta i = 84 mijilij = textocifiar Lij | 120 10000000000000000000000000000000000 |
| The general vector de Indologoción regetir hasta que se telnine la codella texa cifiar regetir hasta que se telnine la codella texa cifiar regetir hasta lesta si itil sina congeta los 64 bits aplicar padding recentar prineras 64 bits de texaccifiar repetir hasta que no hayo bioques de bits i o jeo regetir hasta que la codena se telnine si lutil es igual a nijilij entonces var Xor Lijeo sino var Xor Lije 1 clije riflor 3Des a var Xor can la lique k ive CIJI regiesor c e lu cifiado CTR (texto Citiar ; k) i o jeo resetir hasta i esta repetir hasta i esta repetir hasta i esta repetir hasta i esta repetir hasta i esta recentar hasta cificar Lij | is a supply set of the |
| regetir hasta que se ternine la codella reso cirial regetir hasta 1=64 mr.j.[1] = texto afror [i] \$1.00 congeta los 64 bits centar enneros 64 bits de textocifior jejti regetir hasta que no hago bioques de bits 1=0 regetir hasta que lo codeno se ternine \$1.10 til es gual a n. [i] [i] entonces var Xor [i] = 0 \$1.00 wor Xor [i] = 1 [clj] = (i fior 3 Des a var Xor can lo lique k 1V = C[i] [egiesor c e lv citiado CTR (textocifiar, k) i=0 jeo regetir hasta que se ternine la codena texto cifior regetir hasta i=64 mr.j.[i] = textocifiar [i] | 111- 900 ppc 11200 00 111001120000 |
| repetir hosta 1=84 mr.j[1] = texto afror [i] sino congeta los 64 bits copicor Rodoling recentar princios 64 bits de textocifior j=j+1 repetir hosta que no hogo bioques de bits i=0 j=0 repetir hosta que 10 codeno se terrine si IVII es igual a n. [i] [i] entonces Var Xor [i] = 0 sino vor Xor [i] = 1 [clj] = (i Fior 3 Des a var Xor can lo lique k 1V = C[i] regiesor C e IV citiado CTR (textocifiar, k) i=0 j=0 repetir hosta que se terrine la codena texto cifior repetir hosta i=84 mr.j[i] = textocifiar [i] | reaptir hasta que se telnine la codena rexo cirial |
| Sinc congete los 64 bits aplicor Radding recentar princies 64 bits de textocifiar jejti repetir tosta que no hayo bioques de bits i=0 repetir tosta que la codeno se terrine si IVIII es Igual ai nIJIII entonces var Xor III=0 sino vor Xor III=1 clij=cifior 3Des a var Xor can lo lique k IV=CIII regiesor c e IV cifiado CTR (textocifiar, k) i=0 j=0 repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior repetir hosto que se terrine la codena texto cifior | TPOPLIT NOTO 1=64 |
| recentar enneros 64 bits de textocifiar recentar enneros 64 bits de textocifiar recetir hasta que no hayo bioques de bits i=0 recetir hasta que la codena se terrine si IVIII es Igual a nIJJIII entonces var Xor IIJ = 0 sino var Xor IIJ = 1 cli] = cifiar 3Des a var Xor can la lique k IV = CLJI regetir hasta que se terrine la codena texto afiar refetir hasta que se terrine la codena texto afiar refetir hasta i = 64 maijii j = textocifiar Lij | mi juli = texto cirror L'i |
| recentar enneros 64 bits de textocifiar recentar enneros 64 bits de textocifiar recetir hasta que no hayo bioques de bits i=0 recetir hasta que la codena se terrine si IVIII es Igual a nIJJIII entonces var Xor IIJ = 0 sino var Xor IIJ = 1 cli] = cifiar 3Des a var Xor can la lique k IV = CLJI regetir hasta que se terrine la codena texto afiar refetir hasta que se terrine la codena texto afiar refetir hasta i = 64 maijii j = textocifiar Lij | C 00 200010 100 (4 b) 4 |
| receitar prineros 64 bits de texhocitror j = j + 1 repetir tosta que no hayo boques de bits j = 0 repetir hosta que la codena se terrine si lutil es ignal a risilia entonces var xor [i] = 0 sino vor xor [i] = 1 i = j + 1 cli] = rifior 3 Des a var xor can la lique k iv = CLi] regiesor c c IV cifica CTR (textocitrar, k) i = 0 resetir hosta que se terrine la codena texto afior resetir hosta que se terrine la codena texto afior resetir hosta que se terrine la codena texto afior resetir hosta i = 64 maijilij = textocitrar Lii | Gelicot goding |
| repetir hosts que no hayo bloques de bits i=0 j=0 repetir hosts que la codeno se terrine si lutil es ignal a mijlij entonces var xor [i]=0 sino vor xor [i]=1 clij=citor 3Des a varxor can la lique k iv=clij regiesor c c iv cifiqoo CTR (texto citrar, th) i=0 j=0 repetir hosts que se terrine la codena texto afior repetir hosts i=64 mijlij=texto cifiar Lij i=1+1 | recentor primeros 64 bits de textocifiar |
| repetir hosts que no hogo bloques de bits j=0 repetir hosts que la codena se termne si IVII es Igual a mijili entonces var xor [i]=0 sino vor xor [i]=1 i=i+1 cli]= rifior 3Des a var xor can la lique k IV=CLI] regiesor c c IV citiado CTR (texto Citiar, k) i=0 j=0 repetir hosts que se termne la codena texto afior repetir hosts i=64 mijilij=texto Cifior Li] | |
| repetur hosta que la codeno se terrine si IVI il es Igual a mISILIJ entonces Var Xor IIJ=0 sino vor Xor IIJ=1 i=i+1 clij=cifior 3Des a vor Xor con la lique k IV=CIJI j=i+1 regiesor c e IV cifiado CTR (texto citiar, k) i=0 j=0 refetir hosta que se terrine la codena texto cifior refetir hosta i=64 mLjILiJ=texto cifior Li] | repetir hosta que no hayo bloques de bits |
| repetir hosto que la codeno se terrine si IVII es Igual al mIJII entonces Var Xor IIJ = 0 sino vor Xor IIJ = 1 i=i+1 cljl = cifior 3Des a vorxor can lo lique k IV = CLJI regiesor c e IV cifiado CTR (texto Cifiar, k) i=0 resetir hosto que se terrine lo codeno texto cifior refetir hosto i=64 mcjjIij = texto Cifiar Lij | 1:0 |
| SINTI ES 1941 a MEJLIJ ENTONCES VAR XOR EIJ = 0 SINO WOR XOR EIJ = 1 I = i + 1 CLIJ = CIFIOR 3DES A VORXOR CON 10 LIQUE K 1V = CEJJ J = j + 1 CIFIADO CTR (+exto CIFIAR, K) i = 0 i = 0 i = 0 resetir hosto que se termine lo coderio texto cifior resetir hosto i = 64 MEJJE iJ = texto CIFIAR LIJ | |
| Sino Var Xor [i] = 0 Sino Var Xor [i] = 1 i = i + 1 cli] = cifier 3Des a var Xor can la lique k IV = CLi] j = i + 1 regiesor C e IV Cifiqua CTR (texto Cifiar, k) i = 0 j = 0 refetir hasta e ve se te mine la codina texto afior refetir hasta i = 64 majilij = texto cifiar Lij | repetir hosis que 19 codeño se terrine |
| SINO VOR XOR [i]=1 i=i+1 cLj]= (iFIOR 3DES Q VORXOR CON 10 HOUR K IV=CLJ] regiesor C e IV Cifiquo CTR (+exto Cifiq C, K) i=0 j=0 resptir hosto que se teinine lo codeno texto cifior respetir hosto i=64 mcj][i]= texto Cifiar Li] | 51 1/4 13 es 19091 9 11 1332 13 en tonces |
| cli] = 1+1 cli] = cifior 3Des a varxor can la lique k iv = CLI] i = i+1 regiesor c e iv cifiado CTR (texto Cifiar, k) i = 0 j = 0 resetir hosto que se ternine la codena texto cifiar resetir hasto i = 64 mcji[i] = texto cifiar Li] | |
| CLJ] = CIFIOR 3DES Q VORXOR CON 10 HOUR K 1V = CLJ] J = j +1 regiesor C e IV CIFIODO CTR (+exto CIFIQA, H) i = 0 j = 0 refetir hosto que se termine lo codeno texto cifior refetir hosto i = 64 mcjj[i] = texto CiFIOR Li] | vor Xor [i] =1 |
| regiesor c e IV cifiado CTR (texto Cifiar, k) i=0 j=0 resetir hosto que se termine lo codeno texto cifior resetir hosto i=64 mcjjrij=texto cifiar Lij | 1=1+1 1 1+1=1 |
| regiesor c e IV cifiado CTR (texto Cifiar, k) i=0 j=0 resetir hosto que se termine lo codeno texto cifior resetir hosto i=64 mcjjrij=texto cifiar Lij | CLIL = CIFIOT 3DES 9 varxor can la lique K |
| Cifiado CTR (texto Cifiar, th) i=0 j=0 refetir hosto que se termine la codena texto afior refetir hasto i=64 mLijIcij = texto cifiar [i] | in = de22 |
| Cifiado CTR (texto Cifiar, th) i=0 j=0 refetir hosto que se termine la codena texto afior refetir hasto i=64 mLijIcij = texto cifiar [i] | |
| Cifiquo CTR (texto Cifiqr, th) i=0 j=0 respetir hosto, que se termine la codena texto affor respetir hosto i=64 MLJILIJ = texto Cifiqr LIJ | |
| i=0 j=0 resptir hosts are se ternine to codens texto after respetir hosts i=64 majjrij = textocifier [i] | |
| i=0 j=0 resptir hosts are se ternine to codens texto after respetir hosts i=64 majjrij = textocifier [i] | Cifigdo CTR (texto Cifigr, H) |
| resetir hosto que se termine la codena texto assor resetir hosto i = 64 mcjjcij = texto associfiar [i] | UDD CHAN DISMINISTED CONTRACTOR |
| resptir hosto que se termine la codena texto assor resette hosto i = 64 mcjjcij = textocisior [] | |
| MEDILID = JexIOCIFIOF [] | 0200112 1001 |
| MCJJCiJ = texto CiPior [1] | recept hasto is the mine to codence texto after |
| | mc it it terro Ci Sing [] |
| si no completa los 64 bits aplicor padoling | |
| aplicor podding | Si no completo los 64 bito |
| | aplicor podding |
| | |

```
recortor erineros 64 bits de texto Pescifior
            1= 1+1
       J=0
      repetir hosto que no hogo bbques de bits
x=bloque contodor
            Cont = cifior 3DES q x con lo llove k

Repetir hosto que la codena se terrine cent
si cont cijes igual a nijjij entances

CLIJLIJ = 0
                   SINO
                        CLIDCIJ=1
                   1=1+1
           j=j+1
           X = X + 1
     regiesor C
cificdo CFB (textocifior, k)
     i = 3
     J=0
     14= generos vector de Iniciolización
     repetir hosto que se teinne la codenc texto citror
          repetir bosto 1=64

M L J L i ] = texto CiFror [i]
                1= 1+1
          Sino completo los 64 bits
                appror podding
          recortor prineros 64 bits de texto cifico
          1= 1+1
    reget in hoste que no haye bloques de bits
          1=0
         aux IV= cifior 3DES a IV con a llove & repetir hosto que se termine la codena aux IV si qux IV si qual q n I j I si T en tonces
                    O = 70X 70V
               SINC
                  1= 10x 10V
               1=1+1
         clid = ver xor
         IV = CEST
         0=1+1
   regie gor Ce
```

Norma

CIFIODO OFP CHEX to CIFIOT , K) i = 0 5=0 1 v = generor vector de l'inicia lización repetir hosts que se termine 10 adens repetir hosta 1=64 n [] [] = texto cifiar [] 1=1+1 Sino congleto los 64 bits apheor padoding recorder princios 64 bits de texto Cifior J= 1+1 1=0 repetir hosto que no hogo bloques de bits QUXIV = CIFIAT 3DES Q IV can la lidue k 10 = GUXIV Begetir hosto que la codena auxIV ternine SI GUXIVE ; J es Igual a mejilij en tonces (E33E17=1 1=41 j=j+10000 regiesor ce iv escudo ródigo poro descifiado de las modas de operación descifiedo CBC (texto Descifior, K, IV) i, C J=0 repetir hosto que se temme la codena repetir hosto 1=64 CLIBEIJ = HEATO DESCIPIOTEIJ 1=1+1 recortor princios 64 bit de texto Descifique 11 J= 1 +1 = 1 re petir hoste que no hoyo bloques de bits 1=0 aux c = descrition 3 Des 9 CEIT con 19 110 ve to reactir hosts are gux c termine

```
es 1909 9 GUXO [1] entonces
                mc 37513=0
             SINO
                mLJIII=1
             1= 1+1
         1U = CE 17
         1=1+1
    regiesor m
desafiodo CTR (texto Descifiar, k)
    17G
    j=0
     repetir hosto que se termine la codenc texto Desation
        repetir hosta 1 = 64
            CLIJLIJ = texto pescifior [i]
             1=1+1
        recordor picheros 64 bits de lextocition
         1=1+1
    1=0
    repetir hoste que no hojo bloques de bits
        x = blogge contecor
        1=0
        cont = cifior 3DES a x con la llove h
        repetir hosto que se termine la codena cont
si CEII es igual a cont CII entances
               0= [1][1]m
    No SINO
               MESJEIJ=1
            1=1+1
        X = X +1
          = 1+1
   regresor
             M
descitiodo CFB (texto Descition, H, IV)
   i = G
   1=0
   repetir hosto que se ternine la codena textoDescifror
       repetir hosto 1=64
           CEJIE 1] = texto Descripor [1]
       recortor emperos 64 bits de textocifrat
       1=1+1
   1=0
```

```
repetir hosta que no hogo bloques de bits
        1=0
        auxIV = CIFIOT 3 DES q IV con la llove k
        Repetit hosts que la codens se terrine
            SI CEUJEIJ es Igual a guxIVCIJ enfonces
               MEIJEIJ=0
            5100
                mcj][i]=1
            1=1+1
        14 = CC17
        1=1+1
   regiesor m
desafiodo OFB ( texto pesafior, k, lu)
    i=0
    J=0
    repetir hosto que se terme la codena texto Descirror
            CEJJEIJ = texto Descifior [i]
            1=1+1
        recortor princios 64 bits de texto Descifror
        1=1+1
    repetir hosts no hogo bloques de bits
       gux IV = CIFIOT 3DES 9 IV CON 19 11008 K
       1V = QUX 1V
       Repetit hosto que la codena se temme
Si C[j][i] es igual a cux lu entances
M[j][i]=0
            SINO
               MED CIJ=1
           i = 1 +1
       J=1+1
   regresor M
```