

# CRYPTO

**Si vos disquettes contiennent des données confidentielles (fichiers ASCII, écrans, programmes...) CRYPTO permet de les mettre à l'abri des regards indiscrets. CRYPTO est un programme de codage d'une face complète de disquette : il rend totalement illisible celle-ci, catalogue compris. Ecrit en langage machine, il est rapide (moins de deux minutes pour coder / décoder 178 ko) et accepte les formats DATA ou SYSTEM.**

## Le principe du codage

Le programme lit une piste de la disquette et l'écrit dans un tampon en mémoire ; puis il code chacun des octets de ce tampon et recopie ensuite la piste sur le disque. Quand les quarante pistes ont été traitées, les données initiales ont été remplacées par

des codes incohérents. Seul un décodage adéquat permet de retrouver les données initiales. Le codage de chaque octet du tampon utilise la fonction logique XOR. Par exemple, pour coder l'octet &41 (correspondant à la lettre A en ASCII) avec la valeur &E6, on calcule : &41 XOR &E6 = &A7. Pour vérifier ce résultat, taper au clavier en mode direct : ? HEX\$ (&41 XOR &E6) puis « ENTER », l'ordinateur répond : A7. Pour retrouver l'octet initial il faut savoir que celui-ci a été codé avec la valeur &E6 ; on calcule : &A7 XOR &E6 = &41. (Vérifiez-le !). Ainsi, le même procédé qui a servi au codage sert au décodage.

Naturellement, si on codait tous les octets avec la même valeur &E6 le secret serait bien mal gardé ! Pour durcir le code on change cette valeur à chaque octet codé suivant une loi complexe. L'idéal serait d'utiliser une séquence aléatoire (système dit « à clé aléatoire une fois »). Le résultat serait alors totalement inviolable, mais la séquence à retenir pour le décodage aurait même longueur que le message à coder (ici 182 272 caractères !). Pour palier cet inconvénient on utilise un générateur pseudo-aléatoire qui, une fois initialisé par l'utilisateur, va

produire une suite de valeurs pour le codage. Le générateur utilisé par CRYPTO est du type à congruence linéaire. Sans être le meilleur au point de vue « imprévisibilité », il a l'avantage d'être rapide et d'avoir une période suffisamment longue pour empêcher une attaque statistique du code.

## Le programme BASIC

Pour permettre l'écriture du programme par des lecteurs ne possédant pas d'assembleur, celui-ci est proposé en DATA dans un programme BASIC qui le chargera en mémoire. Le programme vérifie chaque ligne de DATA grâce à une somme de contrôle. Si une erreur est détectée, le programme s'arrête et le numéro de la ligne fautive est affiché. Il faut la corriger avec la commande EDIT puis relancer le programme. Quand tout se déroule bien, le programme demande si l'ordinateur est un CPC 464 ou un 664-6128. Répondre suivant le cas. Le programme crée alors sur disque le fichier CRYPTO.BIN.

Le disque contenant CRYPTO étant dans le lecteur, on le lance par : RUN''CRYPTO « ENTER ». Le programme demande alors la clé de codage / décodage. C'est une chaîne de caractères

alphanumériques (dont il faudra impérativement se souvenir !) qui sert à initialiser le générateur aléatoire. Ensuite, on place dans le lecteur le disque à coder et on appuie sur (ENTER). Le codage commence alors et le numéro de la piste en cours de traitement est affiché. En cas d'erreur le programme affiche un message : suivre alors les indications données. Quand le codage est terminé on retourne sous BASIC. On peut alors demander un catalogue de la disquette ; on obtient généralement n'importe quoi : la disquette est illisible. Pour décoder il suffit de relancer CRYPTO avec exactement la même clé de codage. L'opération terminée, on doit retrouver le catalogue initial et la disquette doit être à nouveau lisible.

## Mise en garde

CRYPTO modifiant directement les données sur la disquette, les données initiales figurant sur celle-ci sont effacées. L'auteur ne connaît aucun moyen simple pour retrouver ces données si on a oublié la clé ! Amnésiques, abstenez-vous ! En particulier, il est prudent de conserver une disquette « claire » contenant CRYPTO. Pour bien initialiser le générateur aléatoire, il est préférable d'utiliser une clé





d'au moins huit caractères. Noter que le programme distingue les majuscules des minuscules et que tous les caractères dont le code ASCII est compris entre 32 et 127 sont valides. Sans être indécryptable par un gros système, CRYPTO permet

de protéger efficacement et rapidement vos disquettes. Pour les lecteurs intéressés par la cryptographie signalons les ouvrages suivants :

\* David KAHN, « La guerre des codes secrets » 1980 InterEdition Paris. (Une étude historique

passionnante, des hiéroglyphes à l'ordinateur...)

\* Romain ROUBATY, « ABC de cryptographie avec programmes en basic ». 1984 Masson. (Tous les codes classiques, avec des programmes de décryptement).

\* Evangelos KRANAKIS, « Primality and Cryptography ». 1986 Wiley-Teubner Series in Computer Science. (Le point actuel sur la question, en anglais dans le texte, pour ceux que les mathématiques n'effraient pas !).

J.-L. Morel

```

100 '***** [1543]
*****
110 '*          CRYPTO          [533]
    *
120 '*          [175]
    *
130 '* Programme de cryptage disqu [2169]
ette *
140 '*          [175]
    *
150 '* Auteur : J.-L. MOREL      [1211]
    *
160 '*          [175]
    *
170 '* C.1986 Amstrad-magazine & l' [2720]
auteur *
180 '*          [175]
    *
190 '***** [1543]
*****
200 '          [117]
210 MODE 2:MEMORY &7FFF:RESTORE [2507]
220 PRINT TAB(12) CHR$(24)+" * GENE [3798]
RATEUR -> CRYPTO * "+CHR$(24)
230 LOCATE 1,5:PRINT "> Ligne coura [4166]
nte : ";ad = &8000:S=0
240 FOR lg=1000 TO 2290 STEP 10    [1443]
250 LOCATE 20,5:PRINT lg          [982]
260 FOR I=0 TO 7                  [486]
270 READ A$:oct=VAL("&"+A$):S=S+oct [1532]
280 POKE ad,oct:ad=ad+1            [317]
290 NEXT I                        [375]
300 READ A$:ctr=VAL("&"+A$):S=S MOD [2123]
    4096
310 IF ctr <> S THEN PRINT:PRINT: P [5249]
RINT CHR$(7)+ ">> Erreur de DATA ":
PRINT:END
320 NEXT lg                        [437]
330 PRINT:PRINT                    [743]
340 PRINT"Pour un CPC 464          p [2860]
ressez : 4"
350 PRINT"Pour un CPC 664 ou 6128 p [2964]
ressez : 6"
360 T$="":WHILE T$="":T$=INKEY$:WEN [1400]

```

```

D
370 IF T$="4" GOTO 400             [446]
380 IF T$="6" GOTO 420             [791]
390 GOTO 360                       [524]
400 POKE &8265,&85:POKE &8266,&B2 [1556]
410 POKE &8274,&85:POKE &8275,&B2 [962]
420 SAVE "CRYPTO.BIN",B,&8000,&408, [1741]
    &8000
430 PRINT:PRINT"> CRYPTO sur disque [1911]
    ."
440 END                            [110]
1000 DATA CD,03,BB,CD,51,BB,3E,02, [1631]
    3A4
1010 DATA CD,0E,BC,21,00,08,11,80, [1548]
    5F5
1020 DATA 82,CD,64,82,11,98,82,CD, [1824]
    A22
1030 DATA 61,82,21,0C,84,06,18,3E, [818]
    C12
1040 DATA 20,77,23,10,FC,21,05,00, [1617]
    DFE
1050 DATA 11,8F,82,CD,64,82,CD,81, [2200]
    221
1060 DATA BB,21,0C,84,06,00,CD,06, [1608]
    466
1070 DATA BB,FE,0D,28,33,FE,7F,28, [816]
    82C
1080 DATA 17,FE,20,38,F1,FE,7F,30, [2064]
    C37
1090 DATA ED,4F,78,FE,18,28,E7,79, [1007]
    089
1100 DATA 77,CD,5A,BB,04,23,18,DE, [2002]
    3FF
1110 DATA 78,B7,28,DA,2B,05,3E,08, [1333]
    6A6
1120 DATA CD,5A,BB,3E,20,77,CD,5A, [2146]
    A84
1130 DATA BB,3E,08,CD,5A,BB,18,C6, [2062]
    E45
1140 DATA CD,84,BB,21,24,84,06,08, [1209]
    128
1150 DATA 3E,00,77,23,10,FC,21,0C, [831]
    339

```



1160 DATA 84,06,03,48,11,24,84,06, [1107]  
4CD  
1170 DATA 08,1A,86,12,13,23,10,F9, [1129]  
6C6  
1180 DATA 41,10,F0,21,25,84,06,04, [1756]  
8DB  
1190 DATA 34,28,FD,23,23,10,F9,21, [1636]  
BA4  
1200 DATA 24,84,06,04,CB,C6,23,23, [1917]  
E2D  
1210 DATA 10,FA,0E,07,CD,0F,B9,C5, [1035]  
1A6  
1220 DATA 3E,FF,32,78,BE,CD,70,82, [1852]  
60A  
1230 DATA 11,DB,82,CD,61,82,CD,5C, [1319]  
A4E  
1240 DATA 82,CD,06,BB,CD,70,82,3E, [957]  
E5B  
1250 DATA 00,CD,30,C6,38,0E,11,F1, [964]  
166  
1260 DATA 82,CD,61,82,CD,5C,82,CD, [1872]  
610  
1270 DATA 06,BB,18,D9,21,2C,84,11, [728]  
BA4  
1280 DATA 00,00,0E,C1,CD,66,C6,3E, [2150]  
BAA  
1290 DATA C1,11,9F,83,38,17,21,2C, [1948]  
E3A  
1300 DATA 84,11,00,00,0E,41,CD,66, [985]  
051  
1310 DATA C6,3E,41,11,AE,83,38,05, [1978]  
315  
1320 DATA 11,19,83,18,CC,32,09,84, [1081]  
565  
1330 DATA 21,08,00,CD,64,82,11,BF, [1262]  
811  
1340 DATA 83,21,0B,00,CD,64,82,21, [1740]  
A94  
1350 DATA 30,30,22,0A,84,11,00,00, [1641]  
BB5  
1360 DATA 21,0B,12,22,26,B7,3E,18, [1123]  
D48  
1370 DATA CD,5A,BB,2A,0A,84,7C,CD, [1145]  
12B  
1380 DATA 5A,BB,7D,CD,5A,BB,3E,18, [2484]  
4F5  
1390 DATA CD,5A,BB,2C,7D,FE,3A,20, [1686]  
8DB  
1400 DATA 03,2E,30,24,22,0A,84,21, [1676]  
A2E  
1410 DATA 2C,84,3A,09,84,4F,D5,C5, [2000]  
DBE  
1420 DATA CD,66,C6,D2,CA,81,01,00, [1106]  
1A5  
1430 DATA 02,09,C1,D1,0C,79,E6,0F, [1672]  
4BC  
1440 DATA FE,0A,20,EA,D5,CD,E7,81, [691]

9DB  
1450 DATA D1,21,2C,84,3A,09,84,4F, [2228]  
C90  
1460 DATA D5,C5,CD,4E,C6,D2,CA,81, [1553]  
228  
1470 DATA 01,00,02,09,C1,D1,0C,79, [883]  
44B  
1480 DATA E6,0F,FE,0A,20,EA,14,3E, [1281]  
7A4  
1490 DATA 28,BA,20,94,11,D5,83,21, [1193]  
AC4  
1500 DATA 0E,00,CD,64,82,C1,CD,18, [2806]  
E2B  
1510 DATA B9,11,71,83,CD,61,82,CD, [1834]  
266  
1520 DATA 4E,82,D0,CD,70,82,21,0E, [1339]  
5F4  
1530 DATA 00,CD,73,82,21,0B,00,CD, [1597]  
BAF  
1540 DATA 73,82,21,0B,00,CD,73,82, [2023]  
B8F  
1550 DATA 11,8A,83,CD,61,82,CD,4E, [2496]  
F78  
1560 DATA 82,CD,70,82,DA,70,80,C3, [964]  
446  
1570 DATA 06,80,C1,D1,21,0E,00,11, [1762]  
69E  
1580 DATA EE,83,CD,64,82,11,34,83, [890]  
ABA  
1590 DATA CD,61,82,CD,5C,82,CD,06, [1306]  
EB8  
1600 DATA BB,CD,70,82,C3,95,81,21, [1139]  
32C  
1610 DATA 2C,84,11,80,04,D5,E5,ED, [1237]  
718  
1620 DATA 4B,24,84,11,7D,87,CD,38, [2511]  
A25  
1630 DATA 82,22,24,84,ED,4B,26,84, [1282]  
D53  
1640 DATA 11,D5,D2,CD,38,82,22,26, [1008]  
ODA  
1650 DATA 84,ED,4B,28,84,11,9D,56, [1338]  
446  
1660 DATA CD,38,82,22,28,84,ED,4B, [1438]  
7D3  
1670 DATA 2A,84,11,F5,6D,CD,38,82, [1738]  
B7B  
1680 DATA 22,2A,84,E1,11,25,84,06, [2071]  
DEC  
1690 DATA 04,1A,AE,77,23,13,13,10, [1701]  
F88  
1700 DATA FB,D1,1B,7A,B3,20,B6,C9, [1806]  
438  
1710 DATA 21,00,00,3E,10,CB,1A,CB, [1315]  
657  
1720 DATA 1B,30,03,09,37,3F,CB,11, [2052]  
800





1730 DATA CB,10,3D,CB,18,EF,CD,06, [1675]  
BBA  
1740 DATA BB,CB,EF,FE,6F,37,CB,FE, [1562]  
199  
1750 DATA 6E,CB,18,F2,11,57,83,18, [1727]  
4DC  
1760 DATA 06,21,14,00,22,26,B7,1A, [1432]  
630  
1770 DATA 13,B7,CB,CD,5A,BB,18,F7, [1991]  
AB3  
1780 DATA 21,14,00,22,26,B7,06,50, [1585]  
C3D  
1790 DATA 3E,20,CD,5A,BB,10,FB,C9, [1235]  
051  
1800 DATA 18,20,2A,20,43,52,59,50, [1391]  
211  
1810 DATA 54,4F,20,2A,20,18,00,3E, [2051]  
374  
1820 DATA 20,43,6C,65,20,3A,20,00, [1333]  
522  
1830 DATA 18,20,45,6E,74,72,65,7A, [1358]  
7D2  
1840 DATA 20,6C,61,20,63,6C,65,20, [998]  
A33  
1850 DATA 64,65,20,63,6F,64,61,67, [658]  
D1A  
1860 DATA 65,20,28,32,34,20,63,61, [1516]  
F11  
1870 DATA 72,2E,20,6D,61,78,29,2E, [1090]  
16E  
1880 DATA 20,56,61,6C,69,64,65,7A, [1453]  
45D  
1890 DATA 20,70,61,72,20,28,45,4E, [899]  
69B  
1900 DATA 54,45,52,29,2E,20,18,00, [1078]  
815  
1910 DATA 18,20,49,6E,74,72,6F,64, [1585]  
ABD  
1920 DATA 75,69,73,65,7A,20,6C,65, [1293]  
DDE  
1930 DATA 20,64,69,73,71,75,65,2E, [2042]  
0B7  
1940 DATA 00,18,20,44,69,73,71,75, [1358]  
2F5  
1950 DATA 65,20,61,62,73,65,6E,74, [658]  
5F7  
1960 DATA 20,6F,75,20,70,72,6F,74, [1875]  
8E0  
1970 DATA 65,67,65,20,65,6E,20,65, [1660]  
B89  
1980 DATA 63,72,69,74,75,72,65,2E, [1073]  
EB5  
1990 DATA 00,18,20,45,72,72,65,75, [1385]  
0F0  
2000 DATA 72,20,64,65,20,66,6F,72, [1831]  
3B2  
2010 DATA 6D,61,74,20,64,69,73,71, [1807]

6C5  
2020 DATA 75,65,2E,00,18,20,45,72, [984]  
8BC  
2030 DATA 72,65,75,72,20,6C,65,63, [2605]  
BCE  
2040 DATA 74,75,72,65,2F,65,63,72, [1778]  
EF7  
2050 DATA 69,74,75,72,65,20,73,65, [1782]  
218  
2060 DATA 63,74,65,75,72,2E,00,20, [1536]  
489  
2070 DATA 3E,3E,20,50,72,65,73,73, [1480]  
732  
2080 DATA 65,7A,20,75,6E,65,20,74, [1656]  
A0D  
2090 DATA 6F,75,63,68,65,2E,20,18, [1290]  
C87  
2100 DATA 00,18,20,41,75,74,72,65, [1830]  
EC0  
2110 DATA 20,64,69,73,71,75,65,20, [1803]  
18B  
2120 DATA 28,4F,2F,4E,29,20,3F,20, [1343]  
327  
2130 DATA 18,00,18,20,4D,65,6D,65, [1359]  
4FB  
2140 DATA 20,63,6C,65,20,28,4F,2F, [1241]  
715  
2150 DATA 4E,29,20,3F,20,18,00,3E, [1427]  
861  
2160 DATA 20,44,61,74,61,20,66,6F, [1284]  
AF0  
2170 DATA 72,6D,61,74,2E,00,3E,20, [1408]  
D30  
2180 DATA 53,79,73,74,65,6D,20,66, [1476]  
03B  
2190 DATA 6F,72,6D,61,74,2E,00,3E, [2234]  
2CA  
2200 DATA 20,43,6F,64,61,67,65,20, [1749]  
54D  
2210 DATA 70,69,73,74,65,20,3A,20, [902]  
7EC  
2220 DATA 8F,8F,8F,8F,00,3E,20,43, [1230]  
AC9  
2230 DATA 6F,64,61,67,65,20,64,69, [1850]  
DB6  
2240 DATA 73,71,75,65,20,63,6F,6D, [1529]  
0D3  
2250 DATA 70,6C,65,74,2E,00,3E,20, [1507]  
314  
2260 DATA 43,6F,64,61,67,65,20,64, [1370]  
5DB  
2270 DATA 69,73,71,75,65,20,69,6E, [434]  
8F9  
2280 DATA 63,6F,6D,70,6C,65,74,2E, [1364]  
C1B  
2290 DATA 00,00,00,00,00,00,00,00, [1237]  
C1B