

L'ECHO DES OCTETS

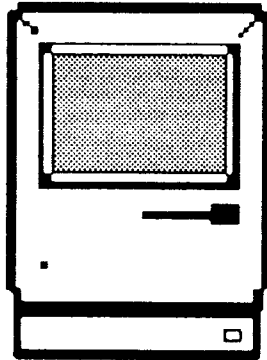
(LE JOURNAL DES ADHERENTS DU C.R.I.P.)

CRYPTOGRAPHIE

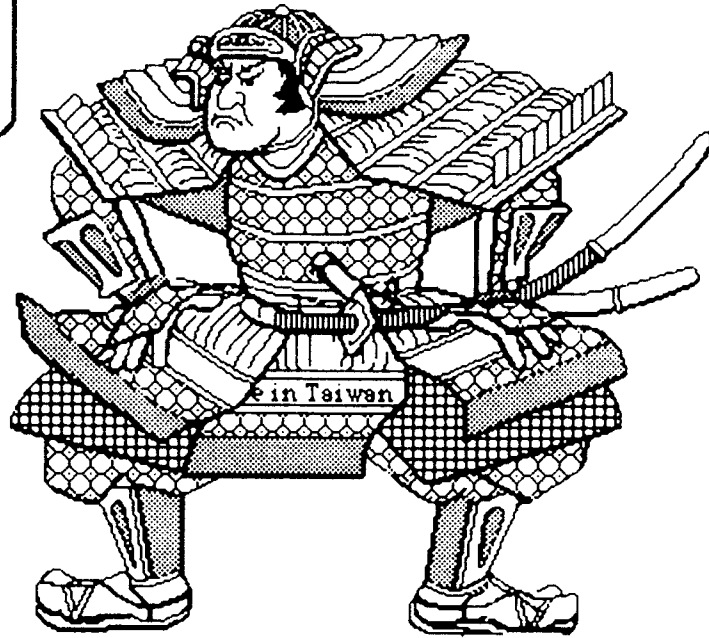
...
EDITO
...

BOITE A OUTIL

US. BUG ARMY, \$\$123#2
made in Honkong.



AMERICANUS MARINES MACUS



INFORMATICUS JAPONUS.

NUMERO : 7

« IN BUG WE TRUST ! »

C.R.I.P. : 51-36-14-90

2ème édition

CE JOURNAL EST BI-MESTRIEL, CELUI-CI CORRESPOND A AVRIL MAI 1987

1948

1948

1948

1948

1948

1948

1948

EDITO

Après le rêve Américain et son « American way of life », voici aujourd' hui le nouvel idéal des Kids, « The CRIP way of Computing ».

En effet, qui de nos jours ne rêve pas d'imiter Sir Breuilh, le seul Reporter International capable de commenter l'arrivée de la course autour du monde (Et vive la marine à voile et le Muscadet ! Hips !), en direct de Dompierre/yon . Et quand Sir Sire , mes godasses (-sic-) et son TestMaker, en français dans le texte, en compagnie du preux Sir Bouchet, qui débouche du virage en tête devant Jean-Paul II, alors que Bernard Hinault toque Truc à cacaque Bidule apparaît sur la place Saint Pierre, on entend les mêmes Hurler dans les cuisines de France et de Saint Pierre et Miquelon (-37,2°C le matin), « Maman, quand je serai grand j'irai au CRIP ». Et lorsque trois Mousquetaires Inventeurs disent devant les Belges, « Nous on est au CRIP ! » on voit des regards de jalousie tomber dans les frites et s'empourprer de Ketchup (Beurk); Et quand (- une fois de plus -) Sir Leterme, Sir Vrignaud, et les autres, saisissent leurs clavier à deux mains on voit Cupertino trembler, IBM frémir, Microsoft déposer son Bilan...

Alors ô toi lecteur, non adhérent, maintenant tu sais que faire pour « devenir qui tu es », laisse toi guider par ton computing-moi !!

PHILIPPE

CRYP(TOGRAPHIE) AU CRIP !!

Un adhérent du CRIP a réalisé un logiciel dit cryptographique ou " protecticiel". Ce genre de programme est très utile pour la protection des documents confidentiels ou secrets des entreprises. Gérard Vrignaud, responsable du Verrou Informatique, qui est passé par la dure école du "Chiffre" de l' Armée Française vous parle ici de l'art difficile du cryptage.

Stéphane .

La cryptographie est connue depuis l'antiquité. Phéniciens, Egyptiens, Grecs et Romains l'utilisèrent pour écrire, suivant les époques, sur des tablettes de pierre, du papyrus, du parchemin, etc. à destination des diplomates ou des militaires. Il s'agissait, jusqu'au début du XXème siècle de systèmes simples, manuels. En 1925 sont apparues des machines à chiffrer : plus rapides, moins sujettes à erreur, elles permettent aussi d'employer des procédés plus perfectionnés. Et comme à chaque siècle ses moyens, au XX ème les siens, Les " Protecticiels " !!

**POURQUOI DES
« PROTECTICIELS » ?**

Parce qu'un fichier de clients, une liste de dernières

commandes, un brevet en cours de dépôt intéressent toujours les concurrents; parce qu'une comptabilité parallèle intéresse le Fisc. En un mot, parce qu'il existe des documents confidentiels dans toutes les Entreprises. Et parce que la protection par mot de passe n'est pas toujours suffisante, car aisément contournable par tout professionnel.

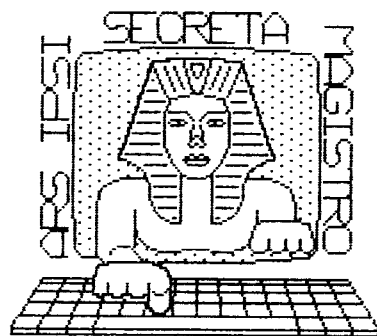
**DIS,
COMMENT CA MARCHE ??**

L'utilisateur commence par entrer le nom du fichier à protéger ou à récupérer, puis les 2 clés (chacune de 3 à 6 lettres) qu'il a choisies. Ensuite, le "protecticiel" réalise une substitution, c'est à dire que, pour chaque caractère, il extrait le code ASCII, lui ajoute (chiffrement) un nombre, appelé décalage, puis écrit à cette place un autre caractère dont le code ASCII est égal au résultat (code + décalage). Au déchiffrement le décalage est retranché et on retrouve le caractère d'origine. Entre temps le fichier reste accessible, mais c'est une suite de caractères inintelligibles.

(suite en page 3)

La valeur d'un système de chiffrement se mesure à la qualité du décalage. Jules César employait un décalage constant, de 3 (il remplaçait toujours A par D). Dans le cas des "protecticiels", le décalage varie à chaque caractère, et il est tel que, sur tout document chiffré assez long tous les caractères ont le même pourcentage de présence (il y a $1/256=0,39\%$ de A ou de m ou de f ...). Cette suite de décalages différents constitue une chaîne cryptographique. La longueur de cette chaîne (important critère de qualité) varie, selon les modèles de "protecticiels" et les clés choisies par l'utilisateur, de 250000 à quelques milliards de maillons.

Bien entendu, chaque "protecticiel" est unique, c'est à dire que ses caractéristiques internes sont différentes de



tous les autres. On peut donc comparer cela à un coffre-fort perfectionné muni d'une clé et d'une combinaison modifiable à chaque manœuvre.

Un "protecticiel" est un coffre-fort logique.

Et pour ceux qui ne

croiraient pas à l'intérêt du cryptage, qu'ils évitent de regarder CANAL+.

"Le Verrou Informatique" et "protecticiel" sont des marques de la SARL LE VERRU INFORMATIQUE, 123 cité A. Paré, Bld Rouillé, La Roche Sur Yon, Tél 51.36.27.18 ..

Gérard Vrignaud.

*IL PARAÎT
QUE*

Un ordinateur en Arséniure de Gallium .

McDonnell Douglas a construit une puce en arséniure de gallium qui selon celui-ci est la première à avoir été testée avec succès en tant que microprocesseur. La MD2901 (c'est son nom !) possède tous les éléments pour traiter, stocker et manipuler l'information selon Bill Geideman le responsable du programme microprocesseur chez McDonnell Douglas. Celle-ci servirait à constituer le cœur d'un ordinateur en arséniure de gallium (AsGa) qui est caractérisée par sa grande vitesse, sa résistance aux radiations et sa faible consommation électrique. Cette nouvelle puce microprocesseur qui émule l'AMD 2901 et pourrait utiliser les mêmes logiciels est une puce 4 bits de 4,5 cm de côté

contenant 1860 transistors et consommant seulement 135 milliwatts. McDonnell Douglas prépare d'ailleurs un ordinateur 16 bits utilisant cette nouvelle technologie.

**Trouvé dans la
TITRÉS grande,
revue Américaine
«Byte».**

**Traduit par
Stephane & Eric...**

*ET AU
PASSAGE*

NSI Logic Inc. a intégré cinq standards graphiques différents sur une seule puce. L'EVC-315 (Enhanced Video Controller ou si vous préférez le contrôleur vidéo étendu) peut émuler* l'adaptateur graphique couleur (CGA), l'adaptateur graphique étendu (EGA), l'adaptateur monochrome, Hercules et l'adaptateur graphique professionnel .

Au moment où le conseil des ministres s'apprête à nommer B. Pivot, monsieur Langue, Le PDG de chez Bull, le grand Français de l'informatique, se pose des questions sur le nom de sa marque....

Ps : écrit le 1er avril.

BOITE A OUTILS

Afficher l'état des touches NUM LOCK et CAPS LOCK sur IBM PC....

Le programme assembleur ci-dessous est destiné à palier à une lacune du clavier de l'IBM PC puisqu'il a pour but d'afficher dans le coin supérieur droit de l'écran l'état des touches

Num Lock et Caps Lock.

Il affichera :

- M si l'on est en majuscule
- m si l'on est en minuscule
- N si l'on utilise le pavé numérique
- D si l'on utilise le pavé curseur

Listing du programme CLAYIER.ASM :

```
code SEGMENT                ; les registres de segments
    ASSUME CS:code; DS:code; ES:code ; pointent sur notre
                                ; programme.
    ORG 100h                ; nécessaire pour convertir en .com.

attribut RECORD clig:1,ArrPlan:3,Intens:1,PremPlan:3 ; Cf variable Utilisées
affiche EQU 0B800h
ici: JMP installation
    STI
    PUSH AX
    PUSH BX                ; on sauvegarde (empile) sur la pile tous les
    PUSH CX                ; registres du microprocesseur qui pourraient
    PUSH DX                ; être modifiés afin de les lui restituer à
    PUSH SI                ; la fin.
    PUSH DI
    PUSH DS
    PUSH ES
    MOV AX,40h              ; DS:BX pointera sur l'adresse contenant
    MOV DS,AX              ; l'état des touches NUM et CAPS.
    MOV AX,affiche         ; ES:BX pointera sur l'adresse de la mémoire
    MOV ES,AX              ; écran où afficher les données.
; ---- Ici commence vraiment notre routine -----
    MOV BX,17h             ; on regarde si le 3ème bit de DS:BX est à 0
    MOV AL,[BX]            ; s'il est à 0 alors on est en déplacement et
    MOV BX,92h             ; l'on va l'afficher (D), sinon on affiche N.
    AND AL,20h             ; on met dans BX la colonne (92h) où afficher
    JZ deplace             ; le message
    MOV AH,attribut<0,001b,1,110b> ; on affiche
    MOV AL,'N'
    MOV ES:[BX]AX          ; N
    JMP encore
    MOV AH,attribut<0,001b,1,110b> ; on affiche
deplace : MOV AL,'D'
    MOV ES:[BX]AX          ; D
encore : MOV BX,17h        ; on regarde si le 2ème bit de DS:BX est à
    MOV AL,[BX]            ; 0, si c'est le cas on est en minuscule et
    MOV BX,94h             ; l'on va afficher m sinon on affiche M
    AND AL,40h             ; on charge BX avec la colonne où afficher
```

Ce petit miracle est réalisé par la modification de l'interruption* Bios 9 (Int 9h) appelée par le système à chaque fois qu'une touche est enfoncée ou relâchée. En effet notre programme Clavier.Com remplace l'interruption 9 par une routine qui vérifie l'état de CAPS et NUM et l'affiche avant de rendre la main à l'ancienne interruption 9 toujours présente en mémoire.

Une fois le programme ci-dessous saisi sous n'importe quel éditeur de texte et sauve en ASCII* (Clavier.asm) il ne vous reste plus qu'à assembler celui-ci à l'aide de n'importe quel assembleur en faisant :

A>ASM Clavier.asm ;
Lors de cette phase ne tenez pas compte du message d'erreur indiquant l'absence de Stack Segment (Segment de pile) en effet les programmes en .com n'ont pas de segment de pile.

A>LINK Clavier.obj ;
Le ; vous évite d'avoir à répondre à toute sorte de questions bêtes (nom de fichiers

intermédiaires

```

JZ pasmajuscules ;le message
MOV AL,'M' ; on affiche
MOV ES:[BX],AX ; M
JMP fin
pasmajuscules: MOV AL,'m' ; on affiche
MOV ES:[BX],AX ; m
fin: PUSHF ; on sauvegarde le registre d'état avant d'appeler
CALL DWORD PTR CS:sauvedep ;l'ancienne int 9h
CLI
POP ES
POP DS
POP DI ; on restitue (dépile) tous les registres afin que
POP SI ; le microprocesseur se retrouve dans la même
POP DX ; situation qu'avant l'appelle de notre nouvelle
POP CX ; int 9h.
POP BX
POP AX
IRET ; sortie de notre nouvelle int 9h.

;===== A PARTIR D'ICI COMMENCE LA PROCEDURE DE =====
;===== MISE EN MEMOIRE DE NOTRE NOUVELLE INT9h =====
;PS:toute cette partie n'est pas sauvegardée en mémoire

sauvedep dw ? ; Cf Variables utilisées.
sauveseg dw ?

installation: Nop
MOV AX,CS
MOV DS,AX
MOV AX,3509h ; on récupère l'adresse de
INT 21h ; l'ancienne INT9h que l'on
MOV AX,BX ; met dans Sauveseg:Sauvedep
MOV WORD PTR DS:sauvedep,AX
MOV AX,ES
MOV WORD PTR DS:sauveseg,AX
MOV AX,OFFSET ici ; on met l'adresse de notre
MOV DX,AX ; nouvelle int9h (DX:DS)
MOV AX,CS ; dans la table des
MOV DS,AX ; interruptions
MOV AX,2509h
INT 21h
CLI
MOV BX,OFFSET ici ; on change le JMP initial
INC BX ;(JMP 1 au lieu de
MOV WORD PTR CS:[BX],1 ;JMP installation).
STI
MOV DX,OFFSET installation ; on termine le programme
INC DX ; en le laissant résident
INT 27h ; en mémoire.
code ENDS
END ici

```

intermédiaires comme le LST ou MAP).

A>EXE2BIN Clavier CLAVIER.COM

EXE2BIN transforme Clavier.exe en Clavier.com.

Variables utilisées :

Affiche : segment de la mémoire vidéo pour affichage des messages

(B800h pour un moniteur couleur, B000h pour un moniteur monochrome)

Attribut : attribut vidéo du message (M-m) à afficher (Couleur du fond, du texte, etc...).

Sauvedep : Offset de l'ancienne interruption 9 (pour pouvoir la rappeler à la fin de notre routine)

Sauveseg : Segment de l'ancienne int 9.

Adresses Utilisées :

40h:17h = octet indiquant l'état des touches spéciales du clavier. Le 2ème bit indique l'état de CAPS Lock, si = 1 alors M (instruction AND AL,20h car 40H=01000000). Le 3ème bit indique l'état de NUM Lock, si = 1 alors N (instruction AND AL,20h car 20H=00100000).

Interruptions Utilisées :

Fonction 35 de l'interruption 21h :

Récupère l'adresse d'une interruption donnée (ici l'adresse de l'ancienne int 9 pour pouvoir la rappeler à la fin de notre routine).

Au départ : AL=n° de l'interruption dont on veut récupérer l'adresse

(suite de la page 5)

AH=35 (n° de la fonction appelée)
Au retour : BX=adresse de l'interruption.

Fonction 25 de l'interruption 21h :

Installe une interruption en mémoire (inscrit son adresse dans la table des interruptions en début de mémoire).

Au départ : AL=n° de l'interruption à installer. DS=segment de l'interruption. DX=offset de l'interruption.

Interruption 27 :

Termine le programme en le laissant résident en mémoire (uniquement pour les .com).

Au départ : DX=offset de la dernière instruction du programme à sauvegarder+1.

Instructions utilisées :

JMP étiquette : saute à la première instruction suivant étiquette.

CLI : Clear Interruption; suspend toutes les interruptions masquables (comme CTRL break ...); permet d'éviter que la séquence d'instructions qui suit ne soit interrompue.

STI : annule CLI, toutes les interruptions seront prises en compte par le microprocesseur.

NB : si vous saisissez le listing ci-joint ne tapez tous les commentaires suivants les ; ce symbole indiquant à l'assembleur qu'il ne doit pas tenir compte de ce qui suit (REM du Basic).

Stéphane .

LEXIQUINFO

INTERRUPTION (Une) :

C'est un sous programme en mémoire. Lorsque le MicroProcesseur reçoit un signal lui demandant d'exécuter une interruption (Signal venant d'un périphérique transmettant des données à l'ordinateur), le Microprocesseur sauvegarde l'adresse où " il se trouve " sur la pile puis exécute les instructions se situant à l'adresse mémoire de l'interruption. Lorsque l'exécution de celle-ci est fini le Microprocesseur dépile l'adresse où il se trouvait et continue là où il en était rendu.

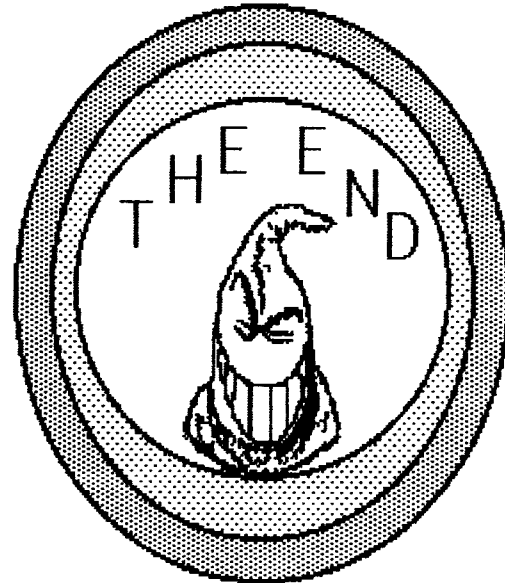
ASCII (CODE) :

L'ordinateur ne comprenant

que des chiffres, le code ASCII (American Standard Code for Information Interchange) est codification des caractères, à un nombre est affecté un caractères (Ex : A = 65). Ce code est utilisé pour stocker des données, en mémoire, sur disquette ou cassette, ou bien pour transférer des données vers un périphérique (Clavier, Imprimante, Ecran,).

EMULER : Imiter.

MOT : Nombre binaire de 16 Bits .



A METRO GOLDWIN BUG MAYER PRODUCTION

Conçu et Réalisé
 par

LE BERRE PHILIPPE
 SIRE STEPHANE
 ANGELIN OLIVIER
 BOUCHET ERIC

