(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 542 471**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **84 03371**

(51) Int Cl³ : G 06 F 13/00; G 06 K 7/01.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 5 mars 1984.

(30) Priorité : US, 7 mars 1983, n° 472.609.

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 37 du 14 septembre 1984.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *ATALLA CORPORATION.* — US.

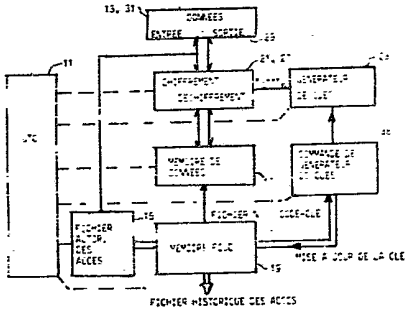
(72) Inventeur(s) : Martin M. Atalla.

(73) Titulaire(s) :

(74) Mandataire(s) : Regimbeau, Corre, Martin, Schrimpf, Warcoin, Ahner.

(54) Procédé et appareil pour assurer la sécurité de l'accès à des fichiers.

(57) L'invention concerne un procédé et un appareil pour assurer le contrôle de l'accès à des fichiers de données protégés suivant lequel et au moyen duquel les données sont enregistrées dans une mémoire 17 sous une forme chiffrée au moyen d'une première clé K_o... K_n et, après qu'elles ont été lues et éventuellement modifiées par un utilisateur autorisé, sont remises en mémoire sous une forme chiffrée au moyen d'une autre clé, un fichier 19 de contrôle d'utilisation des clés enregistrant continuellement, pour chaque fichier, les accès qui ont été effectués et indiquant la clé au moyen de laquelle il est chiffré au moment où un nouvel accès est demandé, ce fichier pouvant également servir pour effectuer une analyse rétrospective des utilisateurs qui ont eu accès aux fichiers.



FR 2 542 471 - A1

De nombreuses opérations connues commandées par ordinateur sur des fichiers de données protégées nécessitent la vérification de l'identité d'un individu qui cherche à avoir accès à un fichier avant que les données (habituellement, sous une forme chiffrée)puissent être accédées (voir, par exemple, les brevets US n° 3.938.091, n° 3.587.051, n° 3.611.293 et n° 4.198.619). En outre, de nombreux systèmes connus conçus pour assurer la sécurité des enregistrements,notamment,ceux utilisés en combinaison avec les cartes de crédit,nécessitent la vérification à la fois du droit d'usage de l'individu utilisateur et de l'authenticité des données contenues dans l'enregistrement pour assurer une protection contre les utilisateurs non autorisés et contre les enregistrements contrefaits ou copiés. Des systèmes de ce type sont décrits dans les brevets US n° 4.304.990, n° 4.328.414 et n° 4.357.423.

Un inconvénient lié aux systèmes de sécurité commandés par ordinateur de ces types est qu'il n'y a typiquement aucune indication laissée dans le fichier en ce qui concerne l'identité de la personne qui a eu accès à un enregistrement protégé.

Conformément au mode de réalisation préféré de la présente invention, on crée un enregistrement dynamique des clés de commande de chiffrement utilisées pour avoir accès initialement et à toutes les occasions suivantes à des fichiers chiffrés protégés à la fois en tant qu'élément actif du système d'accès et en tant qu'enregistrement historique protégé à des fins d'analyse rétrospective de tous les accès aux fichiers chiffrés. En outre, les substitutions de fichiers périmés sont empêchées une fois qu'un fichier est accédé, même pour affichage sans altération, de sorte que, lorsque le fichier accédé et que, par conséquent, sa sécurité a été compromise, il peut être rendu à nouveau protégé contre une copie, une substitution et une réutilisation. Des systèmes de ce type sont particulièrement utiles dans les opérations de banque et de transfert de fonds dans lesquelles un accès initialement correct à un fichier de compte bancaire, par

exemple, pour effectuer un retrait de fonds, doit être ensuite soigneusement contrôlé afin d'éviter des pratiques aussi désastreuses que la réalisation de multiples reproductions de la même opération associée à la substitution du solde d'origine dans le fichier. En outre, l'enregistrement historique des accès au fichier,produit par la présente invention,constitue un enregistrement d'analyse rétrospective sous forme chiffrée de tels accès.

D'autres caractéristiques de l'invention apparaitront à la lecture de la description qui va suivre et à l'examen des dessins annexés dans lesquels:

la Fig. 1 est un schéma-bloc montrant une application de l'appareil de la présente invention;

la Fig. 2 est un organigramme illustrant le fonctionnement de l'appareil de la Fig. 1;

la Fig. 3 est un schéma-bloc du mode de réalisation de la présente invention choisi à titre d'exemple; et

la Fig. 4 est un tableau qui illustre la formation et le fonctionnement du fichier de contrôle d'utilisation des clés selon la présente invention.

Sur la Fig. 1 à laquelle on se référera maintenant, on a représenté un schéma-bloc de la présente invention montrant l'addition d'un module 9 assurant la sécurité de l'accès à un système d'ordinateur typique qui comprend une unité de traitement centrale (UTC) 11, un contrôleur 13 de clavier et des moyens de mémoire 15, 17 pour mettre en mémoire les fichiers. Les moyens de mémoire 15, 17 peuvent utiliser une forme classique quelconque de technologie d'appareils de mémoire,tels que les mémoires à semi-conducteur, les mémoires magnétiques à tores, à cristal, à disque, à tambour ou à bande ou toute combinaison de tels appareils pour mettre en mémoire (mémoire 17) les données dont l'accès doit être contrôlé et pour mettre en mémoire (mémoire 15) les informations d'autorisation d'accès au sujet des individus et entités qui peuvent avoir accès aux données mémorisées 17. Le clavier 13 permet un accès, au moyen d'une entrée manuelle, au système d'ordinateur d'une manière classique et

il est représentatif d'autres systèmes d'accès à un ordinateur, tel que celui par un autre système d'ordinateur et analogue.

Conformément à la présente invention, on modifie un tel système d'ordinateur typique de façon à y incorporer un module 9 assurant la sécurité de l'accès qui fonctionne en combinaison avec le système d'ordinateur pour rechiffrer progressivement les données contenues dans les moyens de mémoire 17 chaque fois qu'un fichier est accédé et,facultativement, pour mettre à jour les informations d'autorisation d'accès contenues dans les moyens de mémoire 15 en réponse à des autorisations accordées et pour engendrer des fichiers historiques sous une forme chiffrée des clés de chiffrement utilisées pour déchiffrer et rechiffrer chaque fichier accédé dans les moyens de mémoire 17. En outre, le module 9 fonctionne dans un mode de réinitialisation commandé pour reconstruire tous les fichiers contenus dans les moyens de mémoire 17 avec une nouvelle clé de chiffrement normalisée après que de nombreux accès aux fichiers contenus dans la mémoire 17 ont été autorisés. Le nombre d'accès qui doivent être effectués avant qu'une réinitalisation soit nécessaire est déterminé par la capacité de la mémoire du module 9.

Sur les Fig. 2 et 3 auxquelles on se référera également maintenant, tout en continuant de se référer à la Fig. 1, on a représenté respectivement un organigramme et un schéma-bloc illustrant le fonctionnement du système de la Fig. 1 sous la commande d'une unité de traitement centrale 11. En fonctionnement, une personne ou entité, R, demandant l'accès à un fichier particulier peut entrer des numéros d'identification personnels, des informations relatives au fichier particulier et analogues, au moyen du clavier 13. Facultativement, une routine 21 de vérification d'identité personnelle peut être effectué d'une manière classique (comme décrit, par exemple, dans le brevet US n° 3.938.091 ou dans le brevet US n° 4.198.619) et une recherche peut être effectuée dans les fichiers d'autorisation d'accès pour déterminer s'il existe une autorisation d'accès au fichier demandé.

Tous ces fichiers contenus dans les moyens de mémoire 17 sont initialement chiffrés avec un code-clé initial K_0, d'une manière classique (par exemple, en utilisant le module de Chiffrement de Données Normalisé qui peut être obtenu du Bureau National des Normes des EUA) en chiffrant les données du fichier dans le module de chiffrement 21 au moyen du code-clé, K_0, fourni par le générateur 23 de codes-clés.

L'autorisation ayant été établie, à l'étape 25, le fichier particulier n° X peut être accédé mais le déchiffrement du fichier n° X nécessite l'emploi du code-clé correct. A cette fin, une recherche est effectuée dans le fichier de contrôle d'utilisation des clés (FCUC) 19,que l'on décrira plus en détail ultérieurement, pour déterminer si le dossier n° X a été précédemment accédé. Les conditions d'accès antérieur,à savoir que le fichier a ou non déjà fait l'objet d'un accès,sont toutes deux possibles. S'il n'y a pas eu d'accès antérieur, le fichier n° X n'apparait pas dans le fichier de contrôle d'utilisation des clés, ce qui constitue une indication qu'il se trouve dans la mémoire 17,chiffré avec le code-clé initial K_0. Le générateur 23 de clés est capable d'engendrer une séquence de codes-clés différents K_0, K_1, K_2, K_3, ... K_n et il est alors réglé pour fournir le code-clé K_0 au module de déchiffrement 27 (qui peut être un module CDN du même type que le module de chiffrement 21 ou peut être ce même module). Le fichier demandé n° X peut, par conséquent, être déchiffré d'une manière classique à l'aide du code-clé K_0 pour fournir les données accédées en texte en clair. Les données sont alors retournées dans la mémoire avec ou sans de nouvelles modifications des données 31 qui reflètent une transaction orientée vers les données, telle qu'une vente, un dépôt, un retrait ou analogue et ces données sont remises en mémoire en utilisant un nouveau code-clé K_1. Ceci est fait en modifiant, à l'étape 38, le réglage du générateur 23 de codes-clés pour qu'il fournisse les données 33 avec ou sans modifications afin qu'elles soient chiffrées dans le module 21 avec le code-clé K_1. En outre, le fichier 19 de contrôle d'utilisation des clés est mis à jour

pour contenir l'indication que le fichier n° X a été accédé et se trouve maintenant en mémoire sous une forme nouvellement chiffrée avec le nouveau code-clé K_1 de la séquence. En outre, les fichiers 15 d'autorisation d'accès peuvent être facultativement mis à jour pour empêcher tout nouvel accès de l'utilisateur R au fichier n° X, par exemple, pour empêcher l'accès de R jusqu'à une "nouvelle date" ou jusqu'à ce que le fichier ait été accédé par un autre utilisateur ou autre condition analogue. L'accès suivant au fichier n° X pour l'utilisateur R, s'il est continuellement autorisé, ou par tout autre utilisateur doit être effectué au moyen d'un déchiffrement avec le code-clé K_1.

Si le fichier n° X a été précédemment accédé, le fichier de contrôle d'utilisation des clés (FCUC) 19 contient l'entrée du fichier n° X indiquant qu'il a été précédemment accédé et retourné à la mémoire chiffré avec un nouveau code-clé K_1, K_2, ... K_n, selon le nombre d'accès précédents au fichier n° X. Ainsi, comme représenté dans la table de la Fig. 4 qui représente les entrées typiques du fichier 19 de contrôle d'utilisation des clés, si le fichier n° X est le fichier n° 00100, les accès précédents à ce fichier ont eu pour résultat qu'il a été remis en mémoire sous une forme chiffrée au moyen du code-clé K_2 (élément 37). La recherche effectuée dans le fichier 19 de contrôle d'utilisation des clés indique ainsi que le fichier n° 00100 a été précédemment accédé deux fois et doit maintenant être déchiffré avec le code-clé K_2. Si l'autorisation de l'utilisateur demandeur est encore valide, à la suite de l'étape 39, le générateur 23 de codes-clés est réglé de manière à fournir le code-clé K_2 au module de déchiffrement 27 afin de fournir, à l'étape 29, les données de ce fichier en texte en clair. La remise en mémoire des données de ce fichier sous une forme modifiée ou non modifiée est effectuée en modifiant le réglage du générateur 23 de codes-clés pour qu'il fournisse le code-clé K_3 (élément 41 sur la Fig. 4) au module de chiffrement 21 afin de chiffrer les données retournées avec le nouveau code-clé K_3. Toutes les sorties de données de la mémoire 17 peuvent

être effectuées avec lecture destructive des informations dans le fichier adressé de sorte que les données qui y sont ré-enregistrées peuvent être écrites sous la forme nouvellement chiffrée. Après de nombreux accès aux fichiers contenus dans la mémoire 17, le fichier 19 de contrôle d'utilisation des clés comprendra typiquement des indications semblables à celles indiquées sur la Fig. 4. Un tel fichier peut facilitativement comporter des codes pour identifier les utilisateurs particuliers qui ont eu accès à chaque fichier. Le fichier 19 fournit ainsi un enregistrement d'analyse rétrospective des accès aux fichiers contenus dans la mémoire 17. En outre, le fichier 19 de contrôle d'utilisation des clés est sous une forme chiffrée étant donné qu'il ne révèle ni les données contenues dans la mémoire 17 ni les codes-clés effectifs K_1-K_n (qui ne sont engendrés que par le générateur 23) requis pour déchiffrer les données de la mémoire 17.En outre, les codes-clés K_0 ... K_n qui servent de codes de protection des fichiers peuvent être engendrés intérieurement d'une manière classique, par exemple par un générateur 23 de nombres aléatoires,et n'ont pas, par conséquent, besoin d'être connus de quiconque.

Après de nombreux accès aux données contenues dans la mémoire 17 qui s'approchent de la limite de la séquence de codes-clés pour un fichier particulier quelconque, ou sur une base périodique, la totalité des fichiers contenus dans la mémoire 17 peuvent être rechiffrés au moyen d'un nouveau code-clé initial K_0' d'une séquence de nouveaux codes-clés K_0',K_1' ... K_n' en utilisant l'appareil représenté sur la Fig. 3 sous la commande de l' unité de traitement centrale 11. Cependant, étant donné que les fichiers contenus dans la mémoire 17 ont été chiffrés avec différents codes-clés, le fichier 19 de contrôle d'utilisation des clés doit être consulté pour déterminer quel code-clé doit être utilisé pour déchiffrer les données de chaque fichier en vue de leur rechiffrement avec un nouveau code-clé initial K_0'. Après achèvement de ce mode de fonctionnement de réinitialisation, le fichier 19 de contrôle d'utilisation des clés pour la sé-

quence de codes-clés $K_0 \ldots K_1$ peut être retiré pour servir d'enregistrement historique de l'accès aux données contenues dans la mémoire 17 sans compromettre la sécurité du système ni des données contenues dans la mémoire 17 sous une forme chiffrée au moyen de nouveaux codes de chiffrement.

REVENDICATIONS

1 - Procédé pour commander l'accès à des fichiers de données mis en mémoire, caractérisé en ce qu'il consiste à chiffrer (21) les données de fichier sous forme d'une combinaison logique choisie desdites données avec un code-clé de chiffrement initial (K_0) d'une série de tels codes-clés (K_0-K_n) pour produire des données de fichier sous une forme chiffrée en vue de leur mise en mémoire dans des emplacements d'adresse de fichier choisis; à établir un enregistrement (19) des accès à chaque emplacement d'adresse de fichier et de celui de la série de codes-clés de chiffrement au moyen duquel les données de fichier qui se trouvent à l'emplacement d'adresse ont été chiffrées; à traiter une demande (13) d'accès aux données de fichier situées à un emplacement d'adresse de fichier choisi en déterminant, à partir de l'enregistrement, le nombre d'accès antérieurs à cet emplacement et le code-clé de chiffrement qui y est associé; à déchiffrer (27) les données de fichier qui se trouvent à l'emplacement d'adresse de fichier choisi en utilisant le code-clé de chiffrement associé; à rechiffrer (21) les données de fichier pour ledit emplacement d'adresse de fichier choisi en utilisant un nouveau code-clé de ladite série de codes-clés de chiffrement dans ladite combinaison logique choisie; à mettre les données de fichier nouvellement rechiffrées en mémoire dans l'emplacement d'adresse de fichier accédé; et à modifier l'enregistrement (19) pour indiquer un accès supplémentaire à l'emplacement d'adresse de fichier choisi et le nouveau code-clé de chiffrement qui lui est associé.

2 - Procédé selon la revendication 1, caractérisé en ce que les données de fichier qui se trouvent à l'emplacement d'adresse de fichier choisi sont déchiffrées (27) en utilisant le code-clé de chiffrement initial (K_0) en réponse à la détermination, à partir de l'enregistrement (19), que l'emplacement d'adresse du fichier choisi n'a pas été précédemment accédé.

3 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte un fichier (15) des autorisations d'accès des utilisateurs et en ce qu'avant d'accéder à un emplace-

ment d'adresse de fichier choisi, l'état d'autorisation d'un utilisateur à avoir accès à l'emplacement d'adresse de fichier choisi est déterminé à partir du fichier.

4 - Procédé selon la revendication 3, caractérisé en ce que l'autorisation d'accès d'un utilisateur pour avoir ultérieurement accès à l'emplacement d'adresse de fichier choisi est sélectivement modifiée (39) en réponse au rechiffrement des données de fichier en vue de leur mise en mémoire à l'emplacement d'adresse de fichier choisi.

5 - Procédé selon la revendication 1, caractérisé en ce qu'il comporte l'étape qui consiste à ré-initialiser toutes les données de fichier en déchiffrant (27) les données de fichier qui se trouvent à chaque emplacement d'adresse de fichier choisi en utilisant le code-clé de chiffrement de ces données déterminé à partir de l'enregistrement (19); et à rechiffrer (21) les données de fichier à chacun de ces emplacements d'adresse de fichier en utilisant un nouveau code-clé initial (K_0') choisi parmi une série de tels codes-clés ($K_0' \ldots K_n'$).

6 - Procédé selon la revendication 5, caractérisé en ce que les données de fichier à tout emplacement d'adresse de fichier qui n'est pas indiqué dans l'enregistrement (19) comme ayant été précédemment accédé sont déchiffrées en utilisant le code-clé de chiffrement initial.

7 - Un appareil utilisable conformément au procédé de la revendication 1 pour assurer la sécurité de données à l'encontre d'un accès non autorisé, dans lequel les données de fichier sont mises en mémoire sous une forme chiffrée dans des moyens de mémoire (17) ayant des emplacements d'adresse de fichier sélectionnables et dans lequel des moyens de chiffrement (21) chiffrent les données de fichier en réponse à des signaux de clé de chiffrement; caractérisé en ce que les moyens de chiffrement produisent les données de fichier chiffrées à un emplacement d'adresse de fichier choisi sous forme de la combinaison de codage logique des données de fichier et d'un signal de clé de chiffrement qui y est appliqué par des moyens (23) générateurs de signaux de clé de chiffrement; en

ce que des moyens d'enregistrement(19) produisent une indication d'emplacements d'adresse de fichier choisis et de signaux de code-clé associés au chiffrement des données de fichier qui y sont mis en mémoire; en ce qu'un premier circuit (38) fonctionne en réponse à l'identification d'un emplacement d'adresse de fichier choisi pour déterminer, à partir des moyens d'enregistrement, le signal de clé de chiffrement qui y est associé afin de régler les moyens générateurs (23) pour qu'ils fournissent le signal de clé de chiffrement associé; en ce que des moyens de déchiffrement (27) sont disposés de façon à recevoir les signaux de clé de chiffrement des moyens générateurs et les données de fichier chiffrées des moyens de mémoire (17) et fonctionnent conformément à ladite combinaison de codage logique pour déchiffrer les données de fichier qui se trouvent audit emplacement d'adresse de fichier choisi; et en ce qu'un second circuit (38) est actionné après déchiffrement des données de fichier pour modifier le réglage des moyens générateurs afin qu'ils fournissent un nouveau signal de clé de chiffrement utilisé pour remettre en mémoire à l'emplacement d'adresse de fichier choisi les données de fichier nouvellement chiffrées avec le nouveau signal de clé de chiffrement et pour modifier les moyens d'enregistrement afin de produire une indication du nouveau signal de clé de chiffrement associé aux données de fichier qui se trouvent dans l'emplacement d'adresse de fichier choisi.

8 - Appareil selon la revendication 7, caractérisé en ce que le premier circuit (38) fonctionne en réponse à l'indication par les moyens d'enregistrement (19) qu'un emplacement d'adresse de fichier choisi n'a pas été précédemment accédé pour régler les moyens générateurs (23) de façon qu'ils fournissent le signal de clé de chiffrement initial (K_0) aux moyens de déchiffrement (27).

9 - Appareil selon la revendication 7, caractérisé en ce qu'il comporte des moyens (15) d'enregistrement d'accès pour mettre en mémoire des données représentatives de l'autorisation donnée à des utilisateurs d'accéder sélectivement aux données de fichier contenues dans les moyens de mémoire (17);

et des moyens d'interdiction qui sont disposés de manière à recevoir les données d'identification d'un utilisateur et qui sont couplés auxdits circuits (38) pour empêcher les moyens générateurs (23) de fournir un signal de clé de chiffrement aux moyens de déchiffrement (27) pour un utilisateur identifié non autorisé.

10 - Appareil selon la revendication 9, caractérisé en ce que le second circuit (39) fonctionne en réponse à la remise en mémoire à l'emplacement d'adresse de fichier choisi des données de fichier nouvellement chiffrées avec un nouveau signal de clé de chiffrement pour modifier l'autorisation de l'utilisateur identifié d'accéder audit emplacement d'adresse de fichier choisi dans les moyens (15) d'enregistrement d'accès.

11 - Appareil selon la revendication 7, caractérisé en ce qu'il comporte des moyens d'initialisation couplés aux moyens générateurs (23), aux moyens de chiffrement (21), aux moyens dé déchiffrement (27) et aux moyens d'enregistrement (19) pour régler les moyens générateurs de façon à déchiffrer sélectivement les données de fichier dans chaque emplacement d'adresse de fichier en utilisant les signaux de clé de chiffrement fournis par les moyens générateurs et établis à partir des moyens d'enregistrement (19) pour chacun de ces emplacements d'adresse de fichier et pour rechiffrer les données de fichier déchiffrées pour chaque emplacement d'adresse de fichier en utilisant un nouveau signal de clé de chiffrement initial (K_0') pour la remise en mémoire à l'emplacement d'adresse de fichier respectif.

12 - Appareil selon la revendication 11, caractérisé en ce que les moyens d'initialisation fonctionnent en réponse à une indication des moyens d'enregistrement qu'aucun accès précédent n'a été effectué à un emplacement d'adresse de fichier choisi pour déchiffrer les données de fichier qui s'y trouvent en utilisant un signal de clé de chiffrement initial et pour rechiffrer les données de fichier déchiffrées en utilisant un nouveau signal de clé de chiffrement initial en vue de la remise en mémoire des données de fichier nouvellement chiffrées à l'emplacement d'adresse de

fichier respectif.

13 - Procédé selon la revendication 1 pour produire un enregistrement des accès à des fichiers, caractérisé en ce que les données de fichier qui sont chiffrées sous la forme de la combinaison logique des données de fichier et de signaux de clé de chiffrement choisis parmi une série de tels signaux sont mises en mémoire à des emplacements d'adresse de fichier choisis; en ce que les données de fichier qui se trouvent à un emplacement d'adresse de fichier choisi sont déchiffrées au moyen du signal de clé de chiffrement qui leur est associé conformément à ladite combinaison logique; en ce que les données de fichier déchiffrées sont rechiffrées sous forme d'une combinaison logique de ces données avec un nouveau signal de clé de chiffrement en vue de leur remise en mémoire à l'emplacement d'adressede fichier correspondant; et en ce qu'un enregistrement des accès aux fichiers est produit sous forme de la compilation d'au moins le nombre de fois que chaque emplacement d'adresse de fichier choisi a été déchiffré et des informations indicatives des signaux de clé de chiffrement avec lesquels les données de fichier qui se trouvent à chaque emplacement d'adresse de fichier choisi y ont été rechiffrées et remises en mémoire.

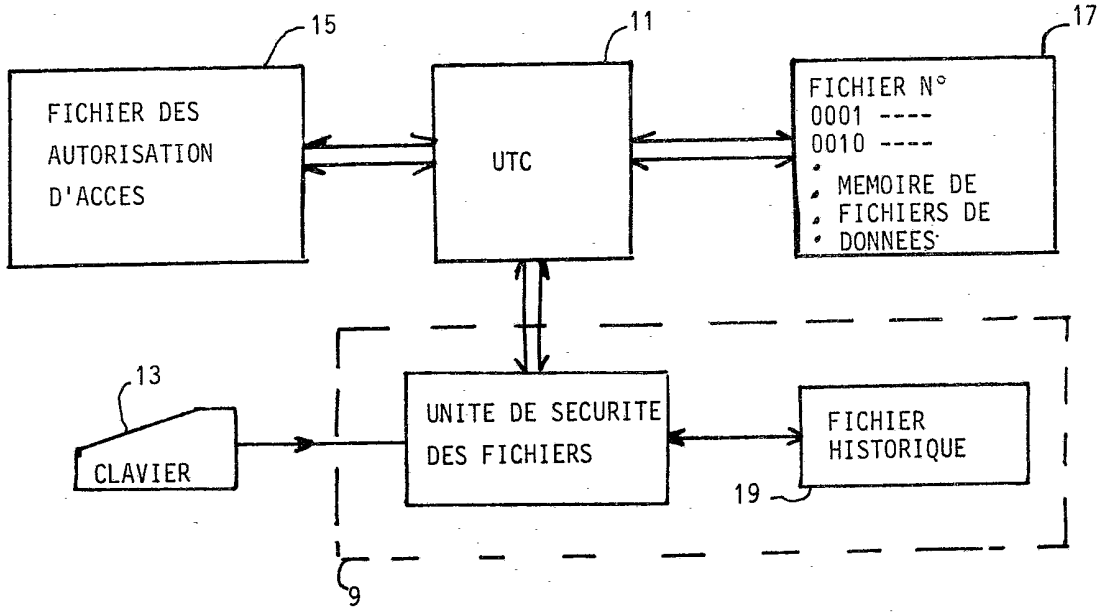

15
11
17
FICHIER DES AUTORISATION D'ACCES
UTC
FICHIER N°
0001 ----
0010 ----
MEMOIRE DE FICHIERS DE DONNEES
13
CLAVIER
UNITE DE SECURITE DES FICHIERS
FICHIER HISTORIQUE
19
9

Fig.1

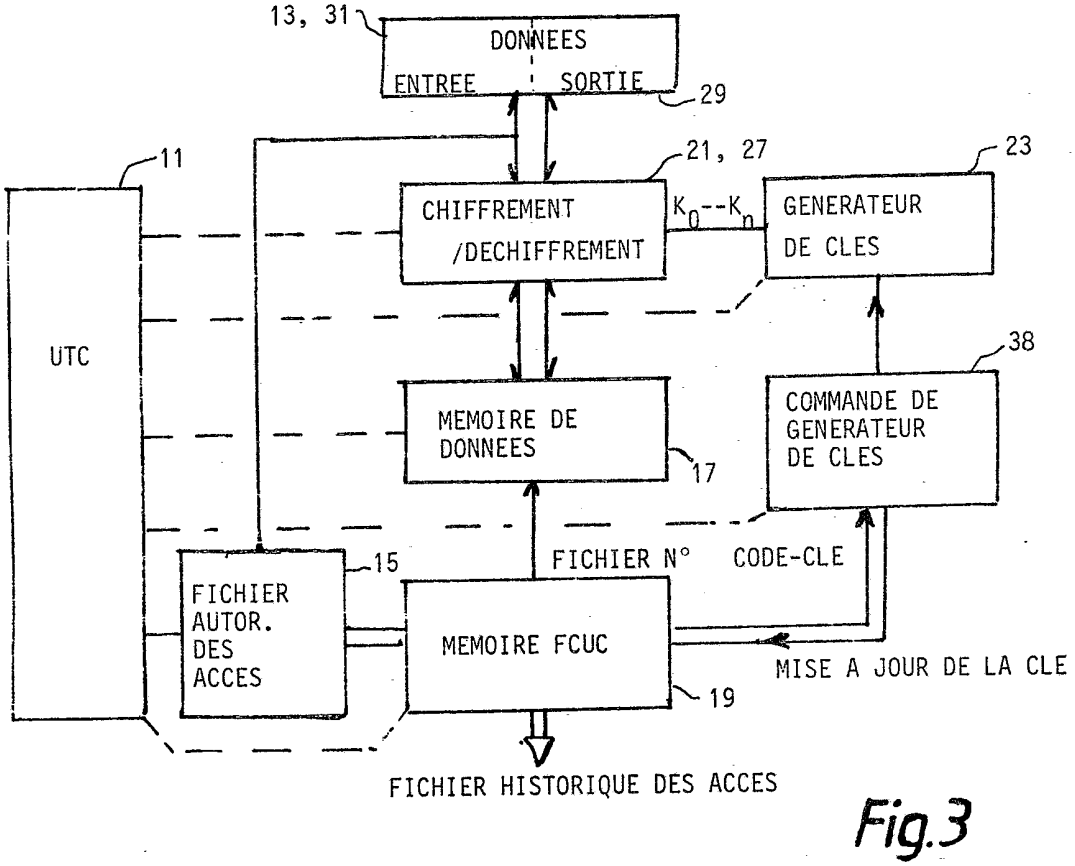
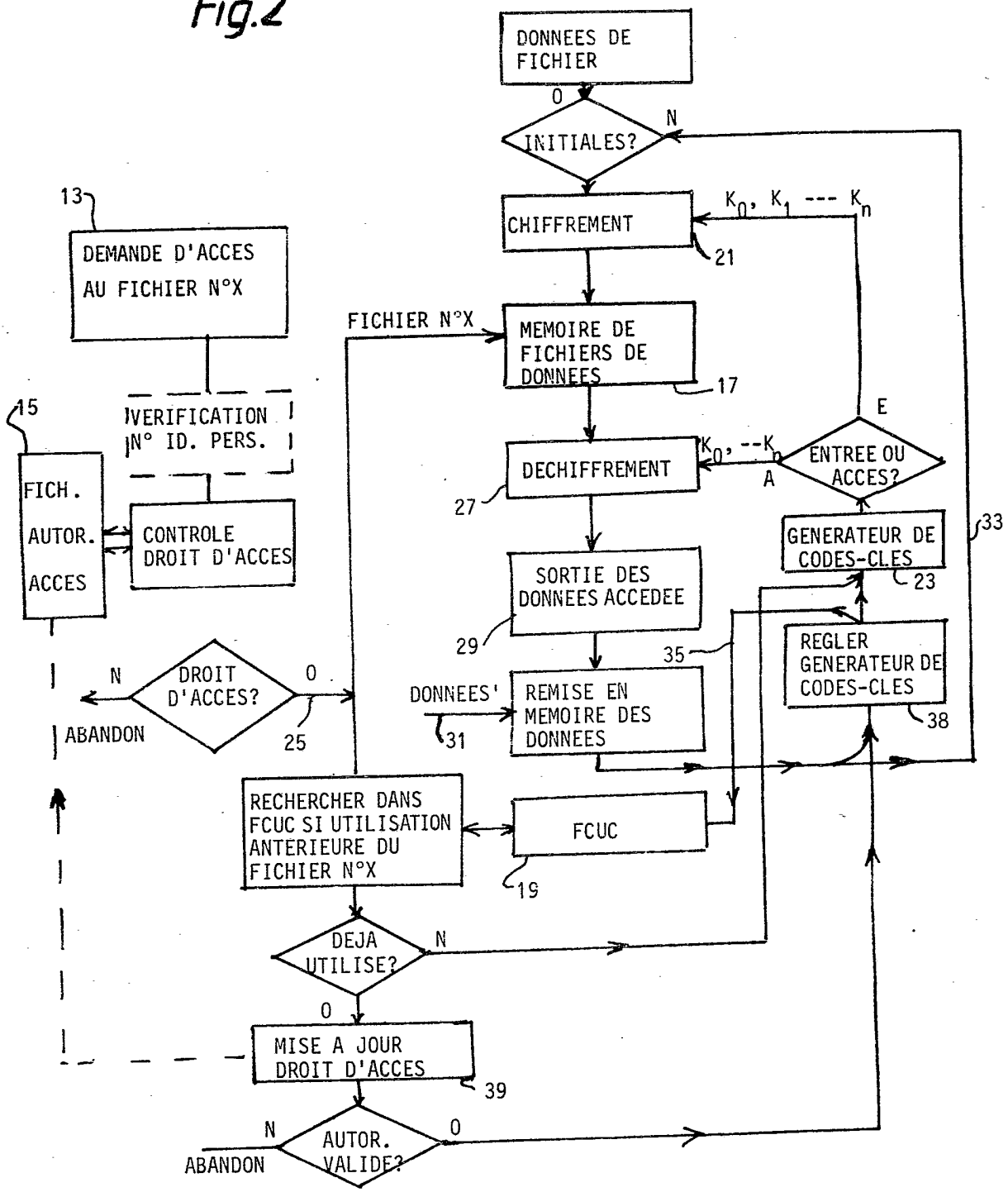
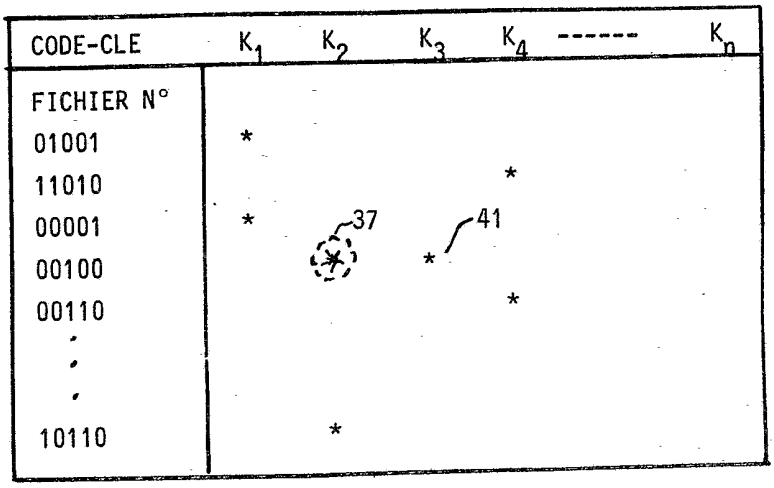

13, 31
DONNEES
ENTREE
SORTIE
29
11
21, 27
23
CHIFFREMENT /DECHIFFREMENT
K_0--K_n
GENERATEUR DE CLES
UTC
38
MEMOIRE DE DONNEES
17
COMMANDE DE GENERATEUR DE CLES
15
FICHIER N°
CODE-CLE
FICHIER AUTOR. DES ACCES
MEMOIRE FCUC
MISE A JOUR DE LA CLE
19
FICHIER HISTORIQUE DES ACCES

Fig.3

2542471

Fig.2




CODE-CLE
K1
K2
K3
K4

Kn
FICHIER N°
01001
11010
00001
00100
00110
10110
37
41

Fig.4